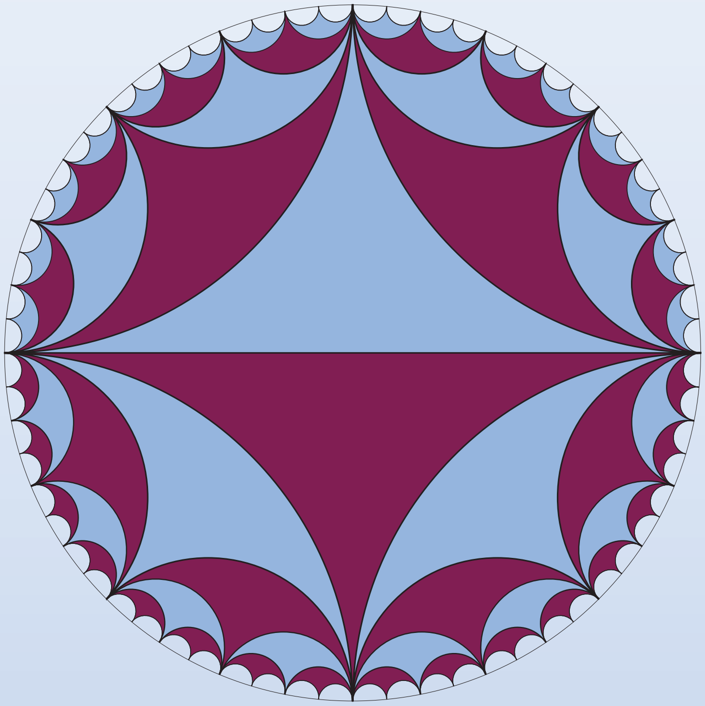
Topology of Numbers

Allen Hatcher



Topology of Numbers

Allen Hatcher

Preface

This book provides an introduction to Number Theory from a point of view that is more geometric than is usual for the subject, inspired by the idea that pictures are often a great aid to understanding. The title of the book *Topology of Numbers* is intended to express this visual slant, where we are using the term “Topology" with its general meaning of “the spatial arrangement and interlinking of the components of a system" rather than its standard mathematical meaning involving open sets, etc.

The principal geometric theme is a certain two-dimensional figure known as the Farey diagram, discovered by Adolf Hurwitz in 1894, which displays certain relationships between rational numbers beyond just their usual distribution along the one-dimensional real number line. Among the many things the diagram elucidates that will be explored in this book are Pythagorean triples, the Euclidean algorithm, Pell’s equation, continued fractions, Farey sequences (of course!), two-by-two matrices with integer entries and determinant ± 1, and best of all, quadratic forms in two variables with integer coefficients, thanks to John Conway’s marvelous idea of the topograph of such a form. A good part of the book is devoted to this last topic, and in fact an alternative title for the book might have been “The Topography of Numbers".

Besides the goal of making the Farey diagram more widely known, our second aim is to make the elementary theory of two-variable quadratic forms more accessible to students. The origins of this wonderfully subtle theory can be traced back to ancient times, and a big boost was provided in the 1600s by Fermat, but it was only in the period 1750-1800 that Euler, Legendre, Lagrange, and especially Gauss were able to uncover the main features of the theory. The later chapters of the book provide an introduction to this material.

Prerequisites for reading the book are fairly minimal, hardly going beyond high school mathematics for the most part. One topic that often forms a significant part of elementary number theory courses is congruences modulo an integer n. It would be helpful if the reader has already seen and used these a little, but we will not develop congruence theory as a separate topic and will instead just use congruences as the need arises, proving whatever nontrivial facts are required including several of the basic ones that form part of a standard introductory number theory course. Among these is quadratic reciprocity, where we give Eisenstein’s classical proof since it involves some geometry.

Chapter 0: A Preview

Pythagorean Triples

As an introduction to the sorts of questions that we will be studying, let us consider right triangles whose sides all have integer lengths. The most familiar example is the $(3,4,5)$ right triangle, but there are many others as well, such as the $(5,12,13)$ right triangle. Thus we are looking for triples (a,b,c) of positive integers such that $a^2 + b^2 = c^2$. Such triples are called *Pythagorean triples* because of the connection with the Pythagorean Theorem. Our goal will be a formula that gives them all. The ancient Greeks knew such a formula, and even before the Greeks the ancient Babylonians must have known a lot about Pythagorean triples because one of their clay tablets from nearly 4000 years ago has been found which gives a list of 15 different Pythagorean triples, the largest of which is $(12709, 13500, 18541)$. (Actually the tablet only gives the numbers a and c from each triple (a,b,c) for some unknown reason, but it is easy to compute b from a and c.)

There is an easy way to create infinitely many Pythagorean triples from a given one just by multiplying each of its three numbers by an arbitrary number n. For example, from $(3,4,5)$ we get $(6,8,10)$, $(9,12,15)$, $(12,16,20)$, and so on. This process produces right triangles that are all similar to each other, so in a sense they are not essentially different triples. In our search for Pythagorean triples there is thus no harm in restricting our attention to triples (a,b,c) whose three numbers have no common factor. Such triples are called *primitive*. The large Babylonian triple mentioned above is primitive, since the prime factorization of 13500 is $2^2 3^3 5^3$ but the other two numbers in the triple are not divisible by 2, 3, or 5.

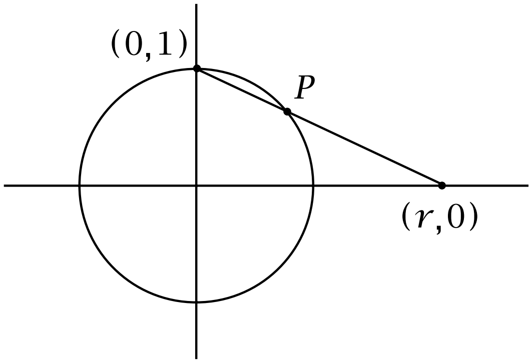
A fact worth noting in passing is that if two of the three numbers in a Pythagorean triple (a,b,c) have a common factor n, then n is also a factor of the third number. This follows easily from the equation $a^2 + b^2 = c^2$, since for example if n divides a and b then n^2 divides a^2 and b^2, so n^2 divides their sum c^2, hence n divides c. Another case is that n divides a and c. Then n^2 divides a^2 and c^2 so n^2 divides their difference $c^2 - a^2 = b^2$, hence n divides b. In the remaining case that n divides b and c the argument is similar.

A consequence of this divisibility fact is that primitive Pythagorean triples can also be characterized as the ones for which no two of the three numbers have a common factor.

If (a,b,c) is a Pythagorean triple, then we can divide the equation $a^2 + b^2 = c^2$ by c^2 to get an equivalent equation $(\frac{a}{c})^2 + (\frac{b}{c})^2 = 1$. This equation is saying that the point $(x,y) = (\frac{a}{c}, \frac{b}{c})$ is on the unit circle $x^2 + y^2 = 1$ in the xy-plane. The coordinates $\frac{a}{c}$ and $\frac{b}{c}$ are rational numbers, so each Pythagorean triple gives a *rational point* on the circle, i.e., a point whose coordinates are both rational. Notice that multiplying each of a, b, and c by the same integer n yields the same point (x,y) on the circle. Going in the other direction, given a rational point on the circle, we can find a common denominator for its two coordinates so that it has the form $(\frac{a}{c},\frac{b}{c})$ and hence gives a Pythagorean triple (a,b,c). We can assume this triple is primitive by canceling any common factor of a, b, and c, and this doesn't change the point $(\frac{a}{c},\frac{b}{c})$. The two fractions $\frac{a}{c}$ and $\frac{b}{c}$ must then be in lowest terms since we observed earlier that if two of a, b, c have a common factor, then all three have a common factor.

From the preceding observations we can conclude that the problem of finding all Pythagorean triples is equivalent to finding all rational points on the unit circle $x^2+y^2=1$. More specifically, there is an exact one-to-one correspondence between primitive Pythagorean triples and rational points on the unit circle that lie in the interior of the first quadrant (since we want all of a,b,c,x,y to be positive).

In order to find all the rational points on the circle $x^2+y^2=1$ we will use a construction that starts with one rational point and creates many more rational points from this one starting point. The four obvious rational points on the circle are the intersections of the circle with the coordinate axes, which are the points $(\pm1,0)$ and $(0,\pm1)$. It doesn't really matter which one we choose as the starting point, so let's choose $(0,1)$. Now consider a line which intersects the circle in this point $(0,1)$ and some other point P, as in the figure at the right. If the line has slope m, its equation will be $y=mx+1$. If we denote the point where the line intersects the x-axis by $(r,0)$, then $m=-1/r$ so the equation for the line can be rewritten as $y=1-\frac{x}{r}$. To find the coordinates of the point P in terms of r we substitute $y=1-\frac{x}{r}$ into the equation $x^2+y^2=1$ and solve for x:



$$\begin{aligned} x^2+\left(1-\frac{x}{r}\right)^2 &= 1 \\ x^2+1-\frac{2x}{r}+\frac{x^2}{r^2} &= 1 \\ \left(1+\frac{1}{r^2}\right)x^2-\frac{2x}{r} &= 0 \\ \left(\frac{r^2+1}{r^2}\right)x^2 &= \frac{2x}{r} \\ x &= \frac{2r}{r^2+1} \quad \text{or} \quad x=0 \end{aligned}$$

Now we plug $x=\dfrac{2r}{r^2+1}$ into the formula $y=1-\frac{x}{r}$. This gives:

$$y=1-\frac{x}{r}=-\frac{1}{r}\left(\frac{2r}{r^2+1}\right)+1=\frac{-2}{r^2+1}+1=\frac{r^2-1}{r^2+1}$$

Summarizing, the coordinates (x, y) of the point P are given by the following formula:

$$(x, y) = \left(\frac{2r}{r^2+1}, \frac{r^2-1}{r^2+1}\right)$$

Note that when $x = 0$ there are two points $(0, \pm 1)$ on the circle. The point $(0, -1)$ comes from the value $r = 0$, while if we let r approach $\pm\infty$ then the point P approaches $(0, 1)$, as we can see either from the picture or from the formula for (x, y).

If r is a rational number, then the formula for (x, y) shows that both x and y are rational, so we have a rational point on the circle. Conversely, if both coordinates x and y of the point P on the circle are rational, then the slope m of the line must be rational, hence r must also be rational since $r = -1/m$. We could also solve the equation $y = 1 - \frac{x}{r}$ for r to get $r = \frac{x}{1-y}$, showing again that r will be rational if x and y are rational (and y is not 1). The conclusion of all this is that, starting from the initial rational point $(0, 1)$ we have found formulas that give all the other rational points on the circle.

Since there are infinitely many choices for the rational number r, there are infinitely many rational points on the circle. But we can say something much stronger than this: Every arc of the circle, no matter how small, contains infinitely many rational points. This is because every arc on the circle corresponds to an interval of r-values on the x-axis, and every interval in the x-axis contains infinitely many rational numbers. Since every arc on the circle contains infinitely many rational points, we can say that the rational points are *dense* in the circle, meaning that for every point on the circle there is an infinite sequence of rational points approaching the given point.

Now we can go back and find formulas for Pythagorean triples. If we set the rational number r equal to p/q with p and q integers having no common factor, then the formulas for x and y become:

$$x = \frac{2(\frac{p}{q})}{\frac{p^2}{q^2}+1} = \frac{2pq}{p^2+q^2}$$

$$y = \frac{\frac{p^2}{q^2}-1}{\frac{p^2}{q^2}+1} = \frac{p^2-q^2}{p^2+q^2}$$

Our final formulas for Pythagorean triples are then:

$$(a, b, c) = (2pq, p^2-q^2, p^2+q^2)$$

Here are a few examples with small values of p and q:

(p,q)	(x,y)	(a,b,c)
$(2,1)$	$(4/5,3/5)$	$(4,3,5)$
$(3,1)^*$	$(6/10,8/10)^*$	$(6,8,10)^*$
$(3,2)$	$(12/13,5/13)$	$(12,5,13)$
$(4,1)$	$(8/17,15/17)$	$(8,15,17)$
$(4,3)$	$(24/25,7/25)$	$(24,7,25)$
$(5,1)^*$	$(10/26,24/26)^*$	$(10,24,26)^*$
$(5,2)$	$(20/29,21/29)$	$(20,21,29)$
$(5,3)^*$	$(30/34,16/34)^*$	$(30,16,34)^*$
$(5,4)$	$(40/41,9/41)$	$(40,9,41)$
$(6,1)$	$(12/37,35/37)$	$(12,35,37)$
$(6,5)$	$(60/61,11/61)$	$(60,11,61)$
$(7,1)^*$	$(14/50,48/50)^*$	$(14,48,50)^*$
$(7,2)$	$(28/53,45/53)$	$(28,45,53)$
$(7,3)^*$	$(42/58,40/58)^*$	$(42,40,58)^*$
$(7,4)$	$(56/65,33/65)$	$(56,33,65)$
$(7,5)^*$	$(70/74,24/74)^*$	$(70,24,74)^*$
$(7,6)$	$(84/85,13/85)$	$(84,13,85)$

The starred entries are the ones with nonprimitive Pythagorean triples. Notice that this occurs only when p and q are both odd, so that not only is $2pq$ even, but also both p^2-q^2 and p^2+q^2 are even, so all three of a, b, and c are divisible by 2. The primitive versions of the nonprimitive entries in the table occur higher in the table, but with a and b switched. This is a general phenomenon, as we will see in the course of proving the following basic result:

Proposition. *Up to interchanging a and b, all primitive Pythagorean triples (a,b,c) are obtained from the formula $(a,b,c) = (2pq, p^2-q^2, p^2+q^2)$ where p and q are positive integers, $p > q$, such that p and q have no common factor and are of opposite parity (one even and the other odd).*

Proof: We need to investigate when the formula $(a,b,c) = (2pq, p^2-q^2, p^2+q^2)$ gives a primitive triple, assuming that p and q have no common divisor and $p > q$.

Case 1: Suppose p and q have opposite parity. If all three of $2pq$, p^2-q^2, and p^2+q^2 have a common divisor $d > 1$ then d would have to be odd since p^2-q^2 and p^2+q^2 are odd when p and q have opposite parity. Furthermore, since d is a divisor of both p^2-q^2 and p^2+q^2 it must divide their sum $(p^2+q^2)+(p^2-q^2) = 2p^2$ and also their difference $(p^2+q^2)-(p^2-q^2) = 2q^2$. However, since d is odd it would then have to divide p^2 and q^2, forcing p and q to have a common factor (since any prime factor of d would have to divide p and q). This contradicts the assumption that p and q had no common factors, so we conclude that $(2pq, p^2-q^2, p^2+q^2)$ is primitive if p and q have opposite parity.

Case 2: Suppose p and q have the same parity, hence they are both odd since if they were both even they would have the common factor of 2. Because p and q are both odd, their sum and difference are both even and we can write $p+q = 2P$ and

$p - q = 2Q$ for some integers P and Q. Any common factor of P and Q would have to divide $P + Q = \frac{p+q}{2} + \frac{p-q}{2} = p$ and $P - Q = \frac{p+q}{2} - \frac{p-q}{2} = q$, so P and Q have no common factors. In terms of P and Q our Pythagorean triple becomes

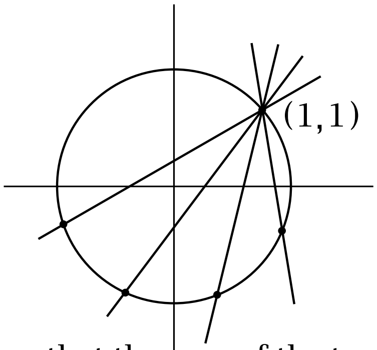
$$\begin{aligned}(a,b,c) &= (2pq, p^2 - q^2, p^2 + q^2)\\ &= (2(P+Q)(P-Q), (P+Q)^2 - (P-Q)^2, (P+Q)^2 + (P-Q)^2)\\ &= (2(P^2 - Q^2), 4PQ, 2(P^2 + Q^2))\\ &= 2(P^2 - Q^2, 2PQ, P^2 + Q^2)\end{aligned}$$

After canceling the factor of 2 we get a new Pythagorean triple, with the first two coordinates switched, and this one is primitive by Case 1 since P and Q can't both be odd, because if they were, then $p = P + Q$ and $q = P - Q$ would both be even, which is impossible since they have no common factor.

From Cases 1 and 2 we can conclude that if we allow ourselves to switch the first two coordinates, then we get all primitive Pythagorean triples from the formula by restricting p and q to be of opposite parity and to have no common factors. □

Rational Points on Other Quadratic Curves

The same technique we used to find the rational points on the circle $x^2 + y^2 = 1$ can also be used to find all the rational points on other quadratic curves $Ax^2 + Bxy + Cy^2 + Dx + Ey = F$ with integer or rational coefficients A, B, C, D, E, F, provided that we can find a single rational point (x_0, y_0) on the curve to start the process. For example, the circle $x^2 + y^2 = 2$ contains the rational points $(\pm 1, \pm 1)$ and we can use one of these as an initial point. Taking the point $(1,1)$, we would consider lines $y - 1 = m(x - 1)$ of slope m passing through this point. Solving this equation for y and plugging into the equation $x^2 + y^2 = 2$ would produce a quadratic equation $ax^2 + bx + c = 0$ whose coefficients are polynomials in the variable m, so these coefficients would be rational whenever m is rational. From the quadratic formula $x = (-b \pm \sqrt{b^2 - 4ac})/2a$ we see that the sum of the two roots is $-b/a$, a rational number if m is rational, so if one root is rational then the other root will be rational as well. The initial point $(1,1)$ on the curve $x^2+y^2 = 2$ gives $x = 1$ as one rational root of the equation $ax^2 + bx + c = 0$, so for each rational value of m the other root x will be rational as well. Then the equation $y - 1 = m(x - 1)$ implies that y will also be rational, and hence we obtain a rational point (x, y) on the curve for each rational value of m. Conversely, if x and y are both rational then obviously $m = (y - 1)/(x - 1)$ will be rational. Thus one obtains a dense set of rational points on the circle $x^2 + y^2 = 2$, since m can be any rational number. An exercise at the end of this chapter is to work out the formulas explicitly.



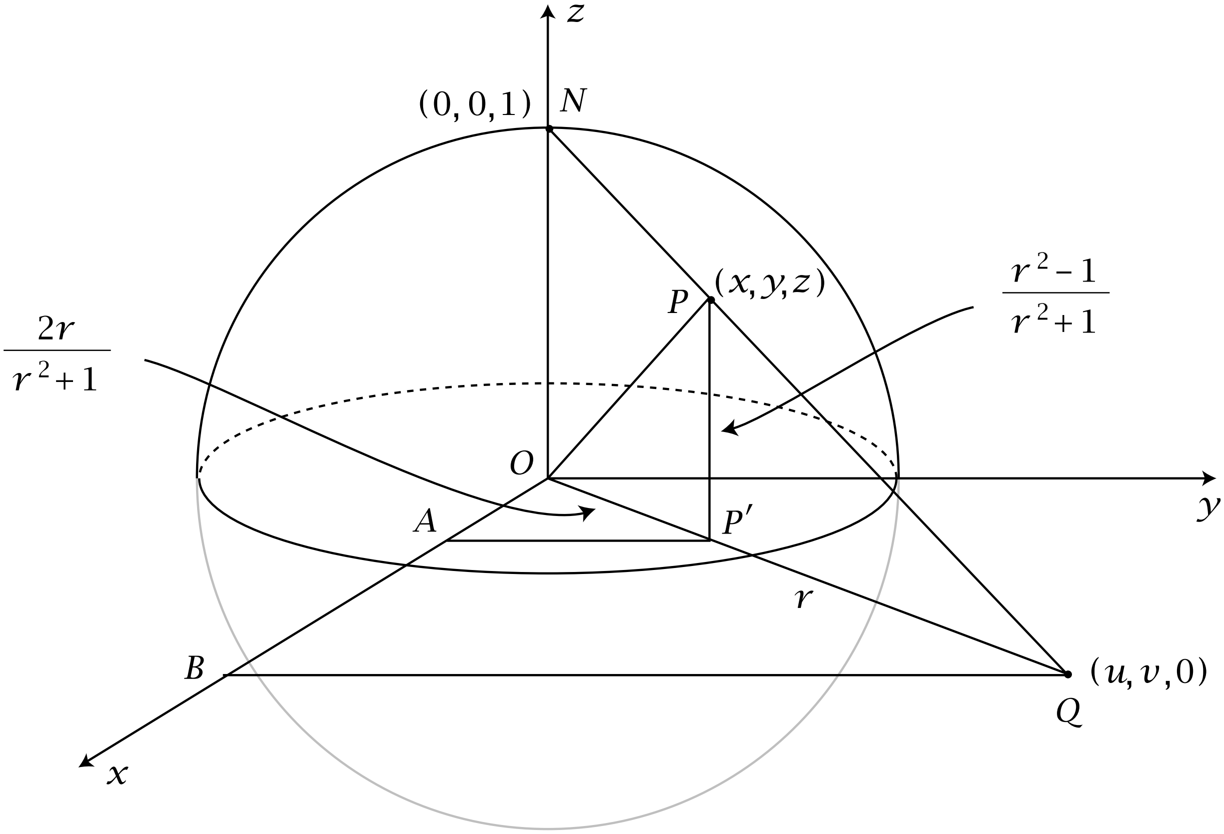
If instead of $x^2 + y^2 = 2$ we consider the circle $x^2 + y^2 = 3$ then there aren't any obvious rational points. In fact this circle contains no rational points at all. For if there were a rational point, this would yield a solution of the equation $a^2 + b^2 = 3c^2$ by integers a, b, and c. We can assume a, b, and c have no common factor. Then a and b can't both be even, otherwise the left side of the equation would be even, forcing c to be even, so a, b, and c would have a common factor of 2. To complete the argument we look at the equation modulo 4. (This means that we consider the remainders obtained after division by 4.) The square of an even number has the form $(2n)^2 = 4n^2$, which is 0 modulo 4, while the square of an odd number has the form $(2n + 1)^2 = 4n^2 + 4n + 1$, which is 1 modulo 4. Thus, modulo 4, the left side of the equation is either $0 + 1$, $1 + 0$, or $1 + 1$ since a and b are not both even. So the left side is either 1 or 2 modulo 4. However, the right side is either $3 \cdot 0$ or $3 \cdot 1$ modulo 4. We conclude that there can be no integer solutions of $a^2 + b^2 = 3c^2$.

The technique we just used to show that $a^2 + b^2 = 3c^2$ has no integer solutions can be used in many other situations as well. The underlying reasoning is that if an equation with integer coefficients has an integer solution, then this gives a solution modulo n for all numbers n. For solutions modulo n there are only a finite number of possibilities to check, although for large n this is a large finite number. If one can find a single value of n for which there is no solution modulo n, then the original equation has no integer solutions. However, this implication is not reversible, as it is possible for an equation to have solutions modulo n for every number n and still have no actual integer solutions. A concrete example is the equation $2x^2 + 7y^2 = 1$. This obviously has no integer solutions, yet it does have solutions modulo n for each n, although this is certainly not obvious. Note that the ellipse $2x^2 + 7y^2 = 1$ does contain rational points such as $(1/3, 1/3)$ and $(3/5, 1/5)$. These can in fact be used to show that $2x^2 + 7y^2 = 1$ has solutions modulo n for each n, as we will show in Chapter 6 when we study congruences in more detail.

In Chapter 6 we will also find a complete answer to the question of when the circle $x^2 + y^2 = n$ contains rational points. It turns out that there are rational points on this circle only when there are integer points on it, and we will see that the existence of integer solutions of $x^2 + y^2 = n$ depends heavily on the prime factorization of n. Namely, we will show that $x^2 + y^2 = n$ has integer solutions exactly when each prime factor of n of the form $4k + 3$ occurs to an even power in the prime factorization of n.

Rational Points on a Sphere

As another application of the same idea, we can find all the rational points on the sphere $x^2 + y^2 + z^2 = 1$, the triples (x, y, z) of rational numbers that satisfy this equation. To do this we consider a line from the north pole $(0, 0, 1)$ to a point $(u, v, 0)$ in the xy-plane. This line intersects the sphere at some point (x, y, z), and we want to find formulas expressing x, y, and z in terms of u and v. To do this we use the following figure:



Suppose we look at the vertical plane containing the triangle ONQ. From our earlier analysis of rational points on a circle of radius 1 we know that if the segment OQ has length $|OQ| = r$, then $|OP'| = \frac{2r}{r^2+1}$ and $|PP'| = \frac{r^2-1}{r^2+1}$. From the right triangle OBQ we see that $u^2 + v^2 = r^2$ since $u = |OB|$ and $v = |BQ|$. The triangle OBQ is similar to the triangle OAP'. Since the length of OP' is $\frac{2}{r^2+1}$ times the length of OQ we conclude from similar triangles that

$$x = |OA| = \frac{2}{r^2+1}|OB| = \frac{2}{r^2+1} \cdot u = \frac{2u}{u^2+v^2+1}$$

and

$$y = |AP'| = \frac{2}{r^2+1}|BQ| = \frac{2}{r^2+1} \cdot v = \frac{2v}{u^2+v^2+1}$$

Also we have

$$z = |PP'| = \frac{r^2-1}{r^2+1} = \frac{u^2+v^2-1}{u^2+v^2+1}$$

Summarizing, we have expressed x, y, and z in terms of u and v by the formulas

$$x = \frac{2u}{u^2+v^2+1} \qquad y = \frac{2v}{u^2+v^2+1} \qquad z = \frac{u^2+v^2-1}{u^2+v^2+1}$$

These formulas imply that we get a rational point (x,y,z) on the sphere $x^2+y^2+z^2 = 1$ for each pair of rational numbers (u,v). We get all rational points on the sphere in this way (except for the north pole $(0,0,1)$, of course) since it is possible to express u and v in terms of x, y, and z by the formulas

$$u = \frac{x}{1-z} \qquad v = \frac{y}{1-z}$$

which one can easily verify by substituting into the previous formulas.

Here is a short table giving a few rational points on the sphere and the corresponding integer solutions of the equation $a^2+b^2+c^2=d^2$:

(u,v)	(x,y,z)	(a,b,c,d)
$(1,1)$	$(2/3,2/3,1/3)$	$(2,2,1,3)$
$(2,2)$	$(4/9,4/9,7/9)$	$(4,4,7,9)$
$(1,3)$	$(2/11,6/11,9/11)$	$(2,6,9,11)$
$(2,3)$	$(2/7,3/7,6/7)$	$(2,3,6,7)$
$(1,4)$	$(1/9,4/9,8/9)$	$(1,4,8,9)$

As with rational points on the circle $x^2+y^2=1$, rational points on the sphere $x^2+y^2+z^2=1$ are dense, so there are lots of them scattered all over the sphere.

In linear algebra courses one is often called upon to create unit vectors (x,y,z) by taking a given vector and rescaling it to have length 1 by dividing it by its length. For example, the vector $(1,1,1)$ has length $\sqrt{3}$ so the corresponding unit vector is $(1/\sqrt{3},1/\sqrt{3},1/\sqrt{3})$. It is rare that this process produces unit vectors having rational coordinates, but we now have a method for creating as many rational unit vectors as we like.

Incidentally, there is a name for the correspondence we have described between points (x,y,z) on the unit sphere and points (u,v) in the plane: it is called *stereographic projection*. One can think of the sphere and the plane as being made of clear glass, and one puts one's eye at the north pole of the sphere and looks downward and outward in all directions to see points on the sphere projected onto points in the plane, and vice versa. The north pole itself does not project onto any point in the plane, but points approaching the north pole project to points approaching infinity in the plane, so one can think of the north pole as corresponding to an imaginary infinitely distant "point" in the plane. This geometric viewpoint somehow makes infinity less of a mystery, as it just corresponds to a point on the sphere, and points on a sphere are not very mysterious. (Though in the early days of polar exploration the north pole may have seemed very mysterious and infinitely distant!)

Pythagorean Triples and Quadratic Forms

There are many questions one can ask about Pythagorean triples (a,b,c). For example, we could begin by asking which numbers actually arise as the numbers a, b, or c in some Pythagorean triple. It is sufficient to answer the question just for primitive Pythagorean triples, since the remaining ones are obtained just by multiplying by arbitrary positive integers. We know all primitive Pythagorean triples arise from the formula

$$(a,b,c) = (2pq, p^2 - q^2, p^2 + q^2)$$

where p and q have no common factor and are not both odd. Determining whether a given number can be expressed in the form $2pq$, $p^2 - q^2$, or $p^2 + q^2$ is a special case of the general question of deciding when an equation $Ap^2 + Bpq + Cq^2 = n$ has an integer solution p, q, for given integers A, B, C, and n. Expressions of the form $Ax^2 + Bxy + Cy^2$ are called *quadratic forms*. These will be the main topic studied in Chapters 4–6, where we will develop some general theory addressing the question of what values a quadratic form takes on when all the numbers involved are integers. For now, let us just look at the special cases at hand.

First let us consider which numbers occur as a or b in primitive Pythagorean triples (a,b,c). A trivial case is the equation $0^2 + 1^2 = 1^2$ which shows that 0 and 1 can be realized by the triple $(0,1,1)$ which is primitive, so let us focus on realizing numbers bigger than 1. If we look at the earlier table of Pythagorean triples we see that all the numbers up to 15 can be realized as a or b in primitive triples except for 2, 6, 10, and 14. This might lead us to guess that the numbers realizable as a or b in primitive Pythagorean triples are the numbers not of the form $4k + 2$, or in other words, numbers not congruent to 2 modulo 4. This is indeed true, and can be proved as follows. First note that since $2pq$ is even, $p^2 - q^2$ must be odd, otherwise both a and b would be even, violating primitivity. Now, every odd number is expressible in the form $p^2 - q^2$ since $2k + 1 = (k + 1)^2 - k^2$, so in fact every odd number is the difference between two consecutive squares. Taking $p = k + 1$ and $q = k$ yields a primitive triple since k and $k+1$ always have opposite parity and no common factors. This takes care of realizing odd numbers. For even numbers, they would have to be expressible as $2pq$ with p and q of opposite parity, which forces pq to be even so $2pq$ is a multiple of 4 and hence cannot be of the form $4k + 2$. On the other hand, if we take $p = 2k$ and $q = 1$ then $2pq = 4k$ with p and q having opposite parity and no common factors.

To summarize, we have shown that all positive numbers $2k+1$ and $4k$ occur as a or b in primitive Pythagorean triples but none of the numbers $4k + 2$ occur. To finish the story, note that a number $a = 4k + 2$ which can't be realized in a primitive triple can be realized by a nonprimitive triple just by taking a triple (a,b,c) with $a = 2k+1$ and doubling each of a, b, and c. Thus all numbers can be realized as a or b in Pythagorean triples (a,b,c).

Now let us ask which numbers c can occur in Pythagorean triples (a,b,c), so we are trying to find a solution of $p^2+q^2=c$ for a given number c. Pythagorean triples (p,q,r) give solutions when c is equal to a square r^2, but we are asking now about arbitrary numbers c. It suffices to figure out which numbers c occur in primitive triples (a,b,c), since by multiplying the numbers c in primitive triples by arbitrary numbers we get the numbers c in arbitrary triples. A look at the earlier table shows that the numbers c that can be realized by primitive triples (a,b,c) seem to be fairly rare: only 5, 13, 17, 25, 29, 37, 41, 53, 61, 65, and 85 occur in the table. These are all odd, and in fact they are all congruent to 1 modulo 4. This always has to be true because p and q are of opposite parity, so one of p^2 and q^2 is congruent to 0 modulo 4 while the other is congruent to 1, hence p^2+q^2 is congruent to 1 modulo 4. More interesting is the fact that most of the numbers on the list are prime numbers, and the ones that aren't prime are products of earlier primes in the list: $25=5\cdot 5$, $65=5\cdot 13$, $85=5\cdot 17$. From this somewhat slim evidence one might conjecture that the numbers c occurring in primitive Pythagorean triples are exactly the numbers that are products of primes congruent to 1 modulo 4. The first prime satisfying this condition that isn't on the original list is 73, and this is realized as $p^2+q^2=8^2+3^2$, in the triple $(48,55,73)$. The next two primes congruent to 1 modulo 4 are $89=8^2+5^2$ and $97=9^2+4^2$, so the conjecture continues to look good. Proving the general conjecture is not easy, however, and we will take up this question in Chapter 6 when we fully answer the question of which numbers can be expressed as the sum of two squares.

Another question one can ask about Pythagorean triples is, how many are there where two of the three numbers differ by only 1? In the earlier table there are several: $(3,4,5)$, $(5,12,13)$, $(7,24,25)$, $(20,21,29)$, $(9,40,41)$, $(11,60,61)$, and $(13,84,85)$. As the pairs of numbers that are adjacent get larger, the corresponding right triangles are either approximately 45-45-90 right triangles as with the triple $(20,21,29)$, or long thin triangles as with $(13,84,85)$. To analyze the possibilities, note first that if two of the numbers in a triple (a,b,c) differ by 1 then the triple has to be primitive, so we can use our formula $(a,b,c)=(2pq,p^2-q^2,p^2+q^2)$. If b and c differ by 1 then we would have $(p^2+q^2)-(p^2-q^2)=2q^2=1$ which is impossible. If a and c differ by 1 then we have $p^2+q^2-2pq=(p-q)^2=1$ so $p-q=\pm 1$, and in fact $p-q=+1$ since we must have $p>q$ in order for $b=p^2-q^2$ to be positive. Thus we get the infinite sequence of solutions $(p,q)=(2,1),(3,2),(4,3),\cdots$ with corresponding triples $(4,3,5),(12,5,13),(24,7,25),\cdots$. Note that these are the same triples we obtained earlier that realize all the odd values $b=3,5,7,\cdots$.

The remaining case is that a and b differ by 1. Thus we have the equation $p^2-2pq-q^2=\pm 1$. The left side doesn't factor using integer coefficients, so it's not so easy to find integer solutions this time. In the table there are only the two triples $(4,3,5)$ and $(20,21,29)$, with $(p,q)=(2,1)$ and $(5,2)$. After some trial and error one could find the next solution $(p,q)=(12,5)$ which gives the triple $(120,119,169)$. Is there a pattern in the solutions $(2,1),(5,2),(12,5)$? One has the numbers $1,2,5,12$, and perhaps it isn't too much of a stretch to notice that the third number is twice the second plus the first, while the fourth number is twice the third plus the second. If this pattern continued, the next number would be $29=2\cdot 12+5$, giving $(p,q)=(29,12)$, and this does indeed satisfy $p^2-2pq-q^2=1$, yielding the Pythagorean triple $(696,697,985)$. These numbers are increasing rather rapidly, and the next case $(p,q)=(70,29)$ yields an even bigger Pythagorean triple $(4060,4059,5741)$. Could there be other solutions of $p^2-2pq-q^2=\pm 1$ with smaller numbers that we missed? We will develop tools in Chapters 4 and 5 to find all the integer solutions, and it will turn out that the sequence we have just discovered gives them all.

Although the quadratic form $p^2-2pq-q^2$ does not factor using integer coefficients, it can be simplified slightly be rewriting it as $(p-q)^2-2q^2$. Then if we change variables by setting

$$x=p-q$$
$$y=q$$

we obtain the quadratic form x^2-2y^2. Finding integer solutions of $x^2-2y^2=n$ is equivalent to finding integer solutions of $p^2-2pq-q^2=n$ since integer values of p and q give integer values of x and y, and conversely, integer values of x and y give integer values of p and q since when we solve for p and q in terms of x and y we again get equations with integer coefficients:

$$p=x+y$$
$$q=y$$

Thus the quadratic forms $p^2-2pq-q^2$ and x^2-2y^2 are completely equivalent, and finding integer solutions of $p^2-2pq-q^2=\pm 1$ is equivalent to finding integer solutions of $x^2-2y^2=\pm 1$.

The equation $x^2-2y^2=\pm 1$ is an instance of the equation $x^2-Dy^2=\pm 1$ which is known as *Pell's equation* (although sometimes this term is used only when the right hand side of the equation is $+1$ and the other case is called the negative Pell equation). This is a very famous equation in number theory which has arisen in many different contexts going back hundreds of years. We will develop techniques for finding all integer solutions of Pell's equation for arbitrary values of D in Chapters 4 and 5. It is interesting that certain fairly small values of D can force the solutions to be quite large. For example for $D=61$ the smallest positive integer solution of $x^2-61y^2=1$ is the rather large pair

$$(x,y)=(1766319049,226153980)$$

As far back as the eleventh and twelfth centuries mathematicians in India knew how to find this solution. It was rediscovered in the seventeenth century by Fermat in France, who also gave the smallest solution of $x^2 - 109y^2 = 1$, the even larger pair

$$(x, y) = (158070671986249, 15140424455100)$$

The way that the size of the smallest solution of $x^2 - Dy^2 = 1$ depends upon D is very erratic and is still not well understood today.

Pythagorean Triples and Complex Numbers

There is another way of looking at Pythagorean triples that involves complex numbers, surprisingly enough. The starting point here is the observation that $a^2 + b^2$ can be factored as $(a + bi)(a - bi)$ where $i = \sqrt{-1}$. If we rewrite the equation $a^2 + b^2 = c^2$ as $(a + bi)(a - bi) = c^2$ then since the right side of the equation is a square, we might wonder whether each term on the left side would have to be a square too. For example, in the case of the triple $(3, 4, 5)$ we have $(3 + 4i)(3 - 4i) = 5^2$ with $3 + 4i = (2 + i)^2$ and $3 - 4i = (2 - i)^2$. So let us ask optimistically whether the equation $(a + bi)(a - bi) = c^2$ can be rewritten as $(p + qi)^2(p - qi)^2 = c^2$ with $a + bi = (p + qi)^2$ and $a - bi = (p - qi)^2$. We might hope also that the equation $(p + qi)^2(p - qi)^2 = c^2$ was obtained by simply squaring the equation $(p + qi)(p - qi) = c$. Let us see what happens when we multiply these various products out:

$$\begin{aligned} a + bi &= (p + qi)^2 = (p^2 - q^2) + (2pq)i \\ &\qquad \text{hence} \quad a = p^2 - q^2 \quad \text{and} \quad b = 2pq \\ a - bi &= (p - qi)^2 = (p^2 - q^2) - (2pq)i \\ &\qquad \text{hence again} \quad a = p^2 - q^2 \quad \text{and} \quad b = 2pq \\ c &= (p + qi)(p - qi) = p^2 + q^2 \end{aligned}$$

Thus we have miraculously recovered the formulas for Pythagorean triples that we obtained earlier by geometric means (with a and b switched, which doesn't really matter):

$$a = p^2 - q^2 \qquad b = 2pq \qquad c = p^2 + q^2$$

Of course, our derivation of these formulas just now depended on several assumptions that we haven't justified, but it does suggest that looking at complex numbers of the form $a + bi$ where a and b are integers might be a good idea. There is a name for complex numbers of this form $a + bi$ with a and b integers. They are called *Gaussian integers*, since the great mathematician and physicist C. F. Gauss made a thorough algebraic study of them some 200 years ago. We will develop the basic properties of Gaussian integers in Chapter 7, in particular explaining why the derivation of the formulas above is valid.

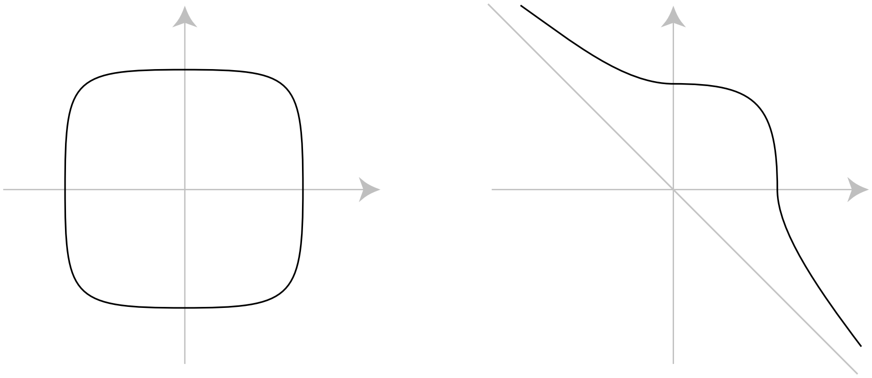
Diophantine Equations

Equations like $x^2 + y^2 = z^2$ or $x^2 - Dy^2 = 1$ that involve polynomials with integer coefficients, and where the solutions sought are required to be integers, are called

Diophantine equations after the Greek mathematician Diophantus (ca. 250 A.D.) who wrote a book about these equations that was very influential when European mathematicians started to consider this topic much later in the 1600s. Usually Diophantine equations are very hard to solve because of the restriction to integer solutions. The first really interesting case is quadratic Diophantine equations. By the year 1800 there was quite a lot known about the quadratic case, and we will be focusing on this case in this book.

Diophantine equations of higher degree than quadratic are much more challenging to understand. Probably the most famous one is $x^n + y^n = z^n$ where n is a fixed integer greater than 2. When the French mathematician Fermat in the 1600s was reading about Pythagorean triples in his copy of Diophantus' book he made a marginal note that, in contrast with the equation $x^2 + y^2 = z^2$, the equation $x^n + y^n = z^n$ has no solutions with positive integers x, y, z when $n > 2$ and that he had a marvelous proof which unfortunately the margin was too narrow to contain. This is one of many statements that he claimed were true but never wrote proofs of for public distribution, nor have proofs been found among his manuscripts. Over the next century other mathematicians discovered proofs for all his other statements, but this one was far more difficult to verify. The issue is clouded by the fact that he only wrote this statement down the one time, whereas all his other important results were stated numerous times in his correspondence with other mathematicians of the time. So perhaps he only briefly believed he had a proof. In any case, the statement has become known as Fermat's Last Theorem. It was finally proved in the 1990s by Andrew Wiles, using some very deep mathematics developed over the preceding couple decades.

We have seen that finding integer solutions of $x^2+y^2 = z^2$ is equivalent to finding rational points on the circle $x^2+y^2 = 1$, and in the same way finding integer solutions of $x^n+y^n = z^n$ is equivalent to finding rational points on the curve $x^n+y^n = 1$. For even values of $n > 2$ this curve looks like a flattened out circle while for odd n it has a rather different shape, extending out to infinity in the second and fourth quadrants, asymptotic to the line $y = -x$:



Fermat's Last Theorem is equivalent to the statement that these curves have no rational points except their intersections with the coordinate axes, where either x or

y is 0. It is curious that these curves only contain a finite number of rational points (either two points or four points, depending on whether n is odd or even) whereas quadratic curves like $x^2+y^2=n$ either contain no rational points or an infinite dense set of rational points.

Exercises

1. (a) Make a list of the 16 primitive Pythagorean triples (a,b,c) with $c \le 100$, regarding (a,b,c) and (b,a,c) as the same triple.
(b) How many more would there be if we allowed nonprimitive triples?
(c) How many triples (primitive or not) are there with $c = 65$?

2. (a) Find all the positive integer solutions of $x^2 - y^2 = 512$ by factoring $x^2 - y^2$ as $(x+y)(x-y)$ and considering the possible factorizations of 512.
(b) Show that the equation $x^2 - y^2 = n$ has only a finite number of integer solutions for each value of $n > 0$.
(c) Find a value of $n > 0$ for which the equation $x^2 - y^2 = n$ has at least 100 different positive integer solutions.

3. (a) Show that there are only a finite number of Pythagorean triples (a,b,c) with a equal to a given number n.
(b) Show that there are only a finite number of Pythagorean triples (a,b,c) with c equal to a given number n.

4. Find an infinite sequence of primitive Pythagorean triples where two of the numbers in each triple differ by 2.

5. Find a right triangle whose sides have integer lengths and whose acute angles are close to 30 and 60 degrees by first finding the irrational value of r that corresponds to a right triangle with acute angles exactly 30 and 60 degrees, then choosing a rational number close to this irrational value of r.

6. Find a right triangle whose sides have integer lengths and where one of the nonhypotenuse sides is approximately twice as long as the other, using a method like the one in the preceding problem. (One possible answer might be the $(8,15,17)$ triangle, or a triangle similar to this, but you should do better than this.)

7. Find a rational point on the sphere $x^2+y^2+z^2=1$ whose x, y, and z coordinates are nearly equal.

8. (a) Derive formulas that give all the rational points on the circle $x^2+y^2=2$ in terms of a rational parameter m, the slope of the line through the point $(1,1)$ on the circle. (The value $m=\infty$ should be allowed as well, yielding the point $(1,-1)$.) The calculations may be a little messy, but they work out fairly nicely in the end to give

$$x = \frac{m^2-2m-1}{m^2+1}, \qquad y = \frac{-m^2-2m+1}{m^2+1}$$

(b) Using these formulas, find five different rational points on the circle in the first quadrant, and hence five solutions of $a^2 + b^2 = 2c^2$ with positive integers a, b, c.
(c) The equation $a^2 + b^2 = 2c^2$ can be rewritten as $c^2 = (a^2 + b^2)/2$, which says that c^2 is the average of a^2 and b^2, or in other words, the squares a^2, c^2, b^2 form an arithmetic progression. One can assume $a < b$ by switching a and b if necessary. Find four such arithmetic progressions of three increasing squares where in each case the three numbers have no common divisors.

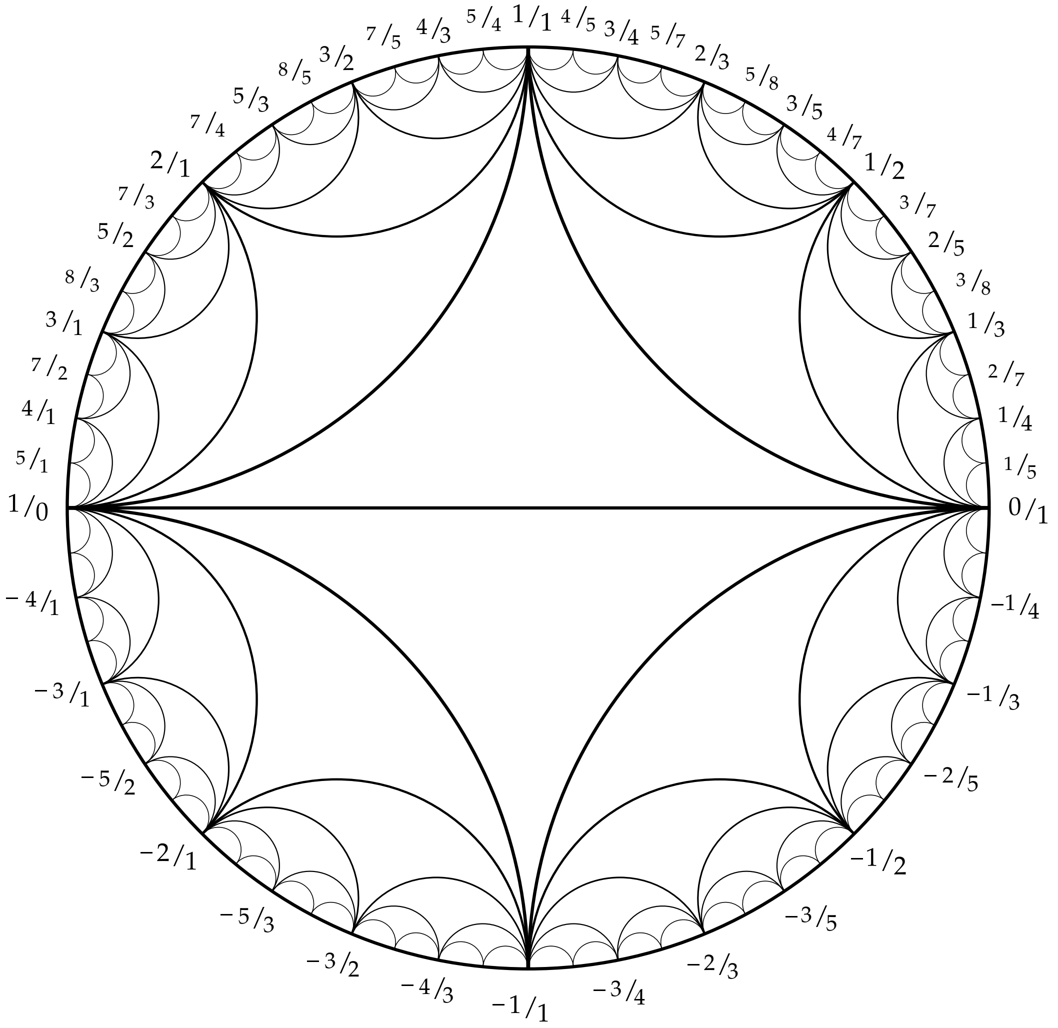
9. (a) Find formulas that give all the rational points on the upper branch of the hyperbola $y^2 - x^2 = 1$.
(b) Can you find any relationship between these rational points and Pythagorean triples?

10. (a) For integers x, what are the possible values of x^2 modulo 8?
(b) Show that the equation $x^2 - 2y^2 = \pm 3$ has no integer solutions by considering this equation modulo 8.
(c) Show that there are no primitive Pythagorean triples (a, b, c) with a and b differing by 3.

11. Show that for every Pythagorean triple (a, b, c) the product abc must be divisible by 60. (It suffices to show that abc is divisible by 3, 4, and 5.)

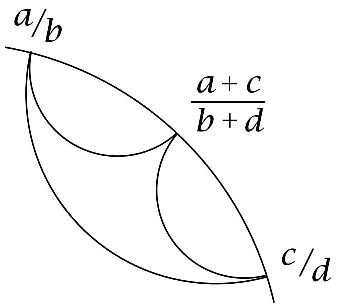
Chapter 1. The Farey Diagram

Our goal is to use geometry to study numbers. Of the various kinds of numbers, the simplest are integers, along with their ratios, the rational numbers. The large figure below shows a very interesting diagram displaying rational numbers and certain relations between them that we will be exploring. This diagram, along with several variants of it that will be introduced later, is known as the *Farey diagram*. The origin of the name will be explained when we get to one of these variants.



What is shown here is not the whole diagram but only a finite part of it. The actual diagram has infinitely many curvilinear triangles, getting smaller and smaller out near the boundary circle. The diagram can be constructed by first inscribing the two big triangles in the circle, then adding the four triangles that share an edge with the two big triangles, then the eight triangles sharing an edge with these four, then sixteen more triangles, and so on forever. With a little practice one can draw the diagram without lifting one's pencil from the paper: First draw the outer circle starting at the left or right side, then the diameter, then make the two large triangles, then the four next-largest triangles, etc.

The vertices of all the triangles are labeled with fractions a/b, including the fraction $1/0$ for ∞, according to the following scheme. In the upper half of the diagram first label the vertices of the big triangles $0/1$, $1/1$, and $1/0$ as shown. Then by induction, if the labels at the two ends of the long edge of a triangle are a/b and c/d, the label on the third vertex of the triangle is $\frac{a+c}{b+d}$. This fraction is called the *mediant* of a/b and c/d.



The labels in the lower half of the diagram follow the same scheme, starting with the labels $0/1$, $-1/1$, and $-1/0$ on the large triangle. Using $-1/0$ instead of $1/0$ as the label of the vertex at the far left means that we are regarding $+\infty$ and $-\infty$ as the same. The labels in the lower half of the diagram are the negatives of those in the upper half, and the labels in the left half are the reciprocals of those in the right half.

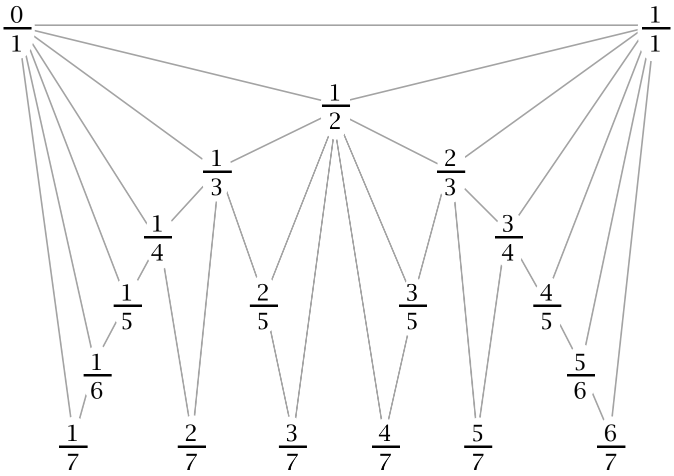
The labels occur in their proper order around the circle, increasing from $-\infty$ to $+\infty$ as one goes around the circle in the counterclockwise direction. To see why this is so, it suffices to look at the upper half of the diagram where all numbers are positive. What we want to show is that the mediant $\frac{a+c}{b+d}$ is always a number between $\frac{a}{b}$ and $\frac{c}{d}$ (hence the term "mediant"). Thus we want to see that if $\frac{a}{b} > \frac{c}{d}$ then $\frac{a}{b} > \frac{a+c}{b+d} > \frac{c}{d}$. Since we are dealing with positive numbers, the inequality $\frac{a}{b} > \frac{c}{d}$ is equivalent to $ad > bc$, and $\frac{a}{b} > \frac{a+c}{b+d}$ is equivalent to $ab + ad > ab + bc$ which follows from $ad > bc$. Similarly, $\frac{a+c}{b+d} > \frac{c}{d}$ is equivalent to $ad + cd > bc + cd$ which also follows from $ad > bc$.

We will show in the next chapter that the mediant rule for labeling vertices in the diagram automatically produces labels that are fractions in lowest terms. It is not immediately apparent why this should be so. For example, the mediant of $1/3$ and $2/3$ is $3/6$, which is not in lowest terms, and the mediant of $2/7$ and $3/8$ is $5/15$, again not in lowest terms. Somehow cases like this don't occur in the diagram.

Another non-obvious fact about the diagram is that all rational numbers occur eventually as labels of vertices. This will be shown in the next chapter as well.

Farey Series

We can build the set of rational numbers by starting with the integers and then inserting in succession all the halves, thirds, fourths, fifths, sixths, and so on. Let us look at what happens if we restrict to rational numbers between 0 and 1. Starting with 0 and 1 we first insert $1/2$, then $1/3$ and $2/3$, then $1/4$ and $3/4$, skipping $2/4$ which we already have, then inserting $1/5$, $2/5$, $3/5$, and $4/5$, then $1/6$ and $5/6$, etc. This process can be pictured as in the following diagram:



The interesting thing to notice is:

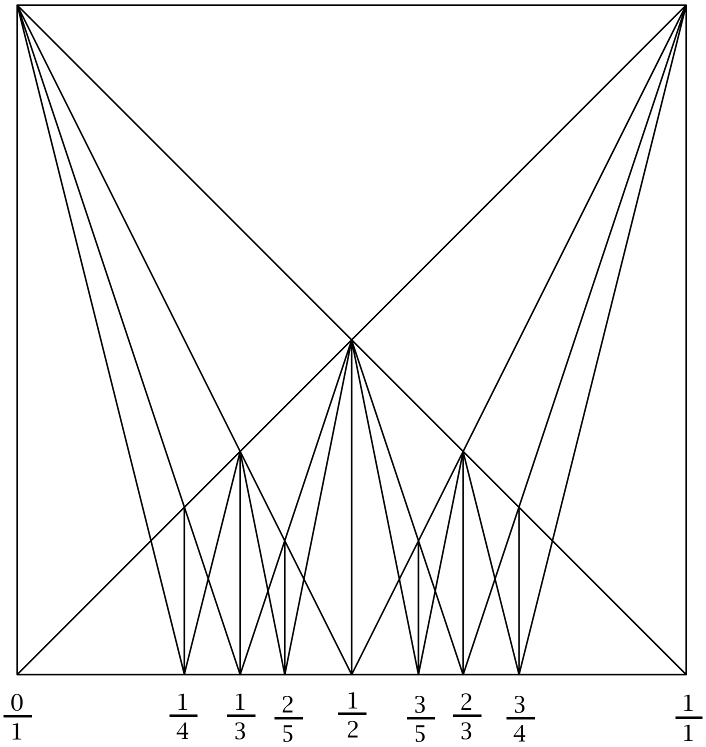
> *Each time a new number is inserted, it forms the third vertex of a triangle whose other two vertices are its two nearest neighbors among the numbers already listed, and if these two neighbors are a/b and c/d then the new vertex is exactly the mediant $\frac{a+c}{b+d}$.*

The discovery of this curious phenomenon in the early 1800s was initially attributed to a geologist and amateur mathematician named Farey, although it turned out that he was not the first person to have noticed it. In spite of this confusion, the sequence of fractions a/b between 0 and 1 with denominator less than or equal to a given number n is usually called the nth *Farey series* F_n. For example, here is F_7:

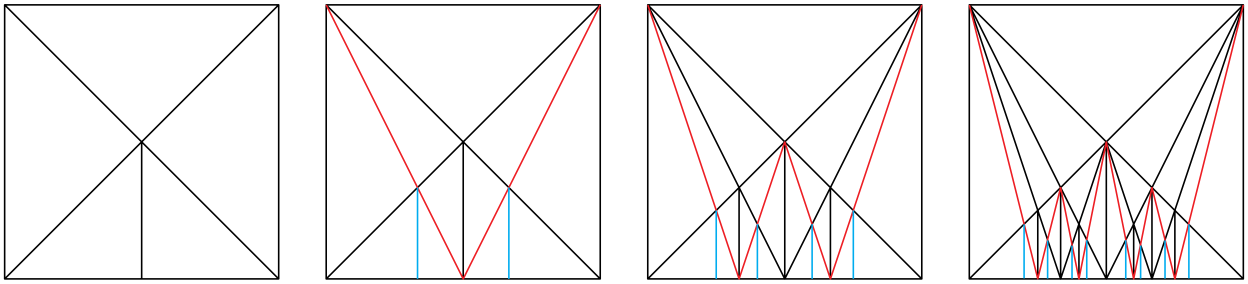
$$\frac{0}{1}\ \frac{1}{7}\ \frac{1}{6}\ \frac{1}{5}\ \frac{1}{4}\ \frac{2}{7}\ \frac{1}{3}\ \frac{2}{5}\ \frac{3}{7}\ \frac{1}{2}\ \frac{4}{7}\ \frac{3}{5}\ \frac{2}{3}\ \frac{5}{7}\ \frac{3}{4}\ \frac{4}{5}\ \frac{5}{6}\ \frac{6}{7}\ \frac{1}{1}$$

These numbers trace out the up-and-down path across the bottom of the figure above. For the next Farey series F_8 we would insert $1/8$ between $0/1$ and $1/7$, $3/8$ between $1/3$ and $2/5$, $5/8$ between $3/5$ and $2/3$, and finally $7/8$ between $6/7$ and $1/1$.

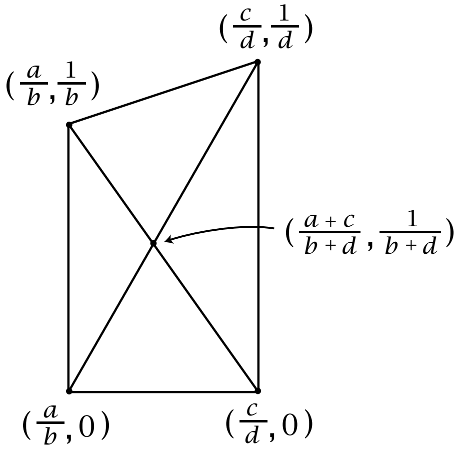
There is a cleaner way to draw the preceding diagram using straight lines in a square:



One can construct this diagram in stages, as indicated in the sequence of figures below. Start with a square together with its diagonals and a vertical line from their intersection point down to the bottom edge of the square. Next, connect the resulting midpoint of the lower edge of the square to the two upper corners of the square and drop vertical lines down from the two new intersection points this produces. Now add a W-shaped zigzag and drop verticals again. It should then be clear how to continue.



A nice feature of this construction is that if we start with a square whose sides have length 1 and place this square so that its bottom edge lies along the x-axis with the lower left corner of the square at the origin, then the construction assigns labels to the vertices along the bottom edge of the square that are exactly the x coordinates of these points. Thus the vertex labeled $1/2$ really is at the midpoint of the bottom edge of the square, and the vertices labeled $1/3$ and $2/3$ really are $1/3$ and $2/3$ of the way along this edge, and so forth. In order to verify this fact the key observation is the following: For a vertical line segment in the diagram whose lower endpoint is at the point $(\frac{a}{b},0)$ on the x-axis, the upper endpoint is at the point $(\frac{a}{b},\frac{1}{b})$. This is obviously true at the first stage of the construction, and it continues to hold at each successive stage since for a quadrilateral whose four vertices have coordinates as shown in the figure at the right, the two diagonals intersect at the point $(\frac{a+c}{b+d},\frac{1}{b+d})$. For example, to verify that $(\frac{a+c}{b+d},\frac{1}{b+d})$ is on the line from $(\frac{a}{b},0)$ to $(\frac{c}{d},\frac{1}{d})$ it suffices to show that the line segments from $(\frac{a}{b},0)$ to $(\frac{a+c}{b+d},\frac{1}{b+d})$ and from $(\frac{a+c}{b+d},\frac{1}{b+d})$ to $(\frac{c}{d},\frac{1}{d})$ have the same slope. These slopes are


$(\frac{c}{d},\frac{1}{d})$
$(\frac{a}{b},\frac{1}{b})$
$(\frac{a+c}{b+d},\frac{1}{b+d})$
$(\frac{a}{b},0)$
$(\frac{c}{d},0)$

$$\frac{1/(b+d)-0}{(a+c)/(b+d)-a/b}\cdot\frac{b(b+d)}{b(b+d)}=\frac{b}{b(a+c)-a(b+d)}=\frac{b}{bc-ad}$$

and

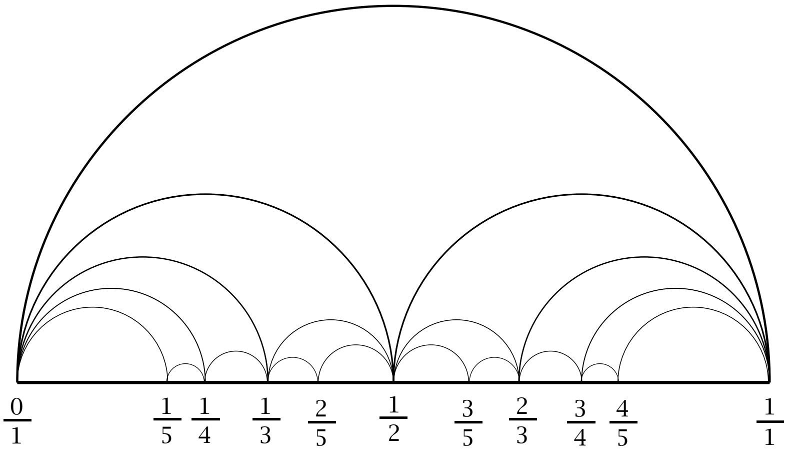
$$\frac{1/d-1/(b+d)}{c/d-(a+c)/(b+d)}\cdot\frac{d(b+d)}{d(b+d)}=\frac{b+d-d}{c(b+d)-d(a+c)}=\frac{b}{bc-ad}$$

so they are equal. The same argument works for the other diagonal, just by interchanging $\frac{a}{b}$ and $\frac{c}{d}$.

Going back to the square diagram, this fact that we have just shown implies that the successive Farey series can be obtained by taking the vertices that lie above the line $y=\frac{1}{2}$, then the vertices above $y=\frac{1}{3}$, then above $y=\frac{1}{4}$, and so on. Here we are assuming the two properties of the Farey diagram that will be shown in the next chapter, that all rational numbers occur eventually as labels on vertices, and that these labels are always fractions in lowest terms.

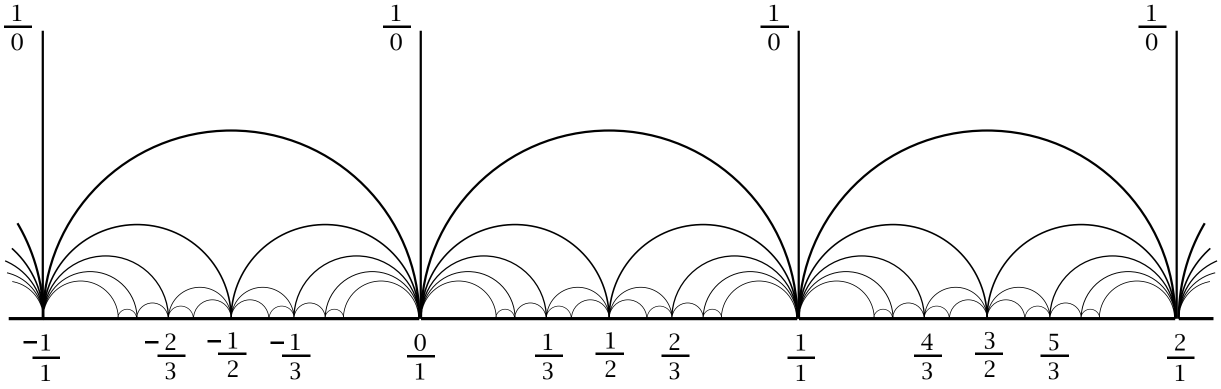
The Upper Half-Plane Farey Diagram

In the square diagram depicting the Farey series, the most important thing for our purposes is the triangles, not the vertical lines. We can get rid of all the vertical lines by shrinking each one to its lower endpoint, converting each triangle into a curvilinear triangle with semicircles as edges, as shown in the diagram below.



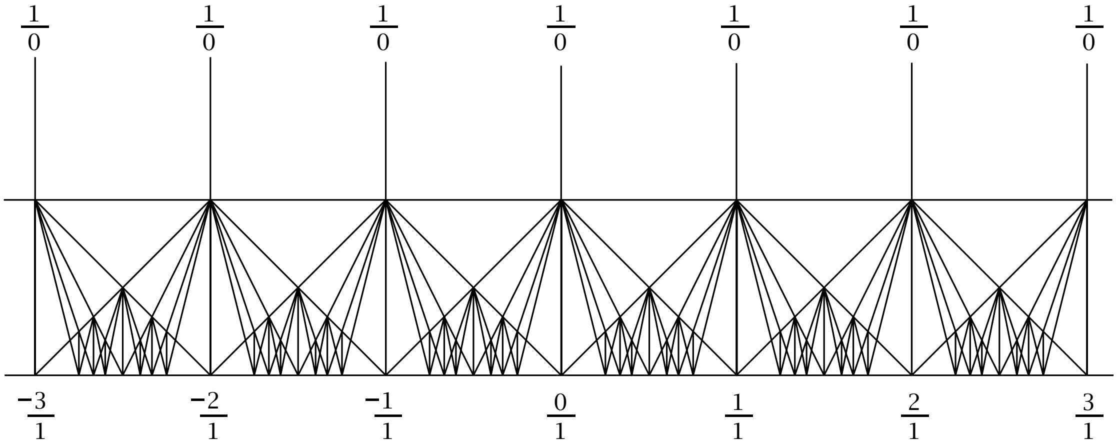
This looks more like a portion of the Farey diagram we started with at the beginning of the chapter, but with the outer boundary circle straightened into a line. The advantage of the new version is that the labels on the vertices are exactly in their correct places along the x-axis, so the vertex labeled $\frac{a}{b}$ is exactly at the point $\frac{a}{b}$ on the x-axis.

This diagram can be enlarged so as to include similar diagrams for fractions between all pairs of adjacent integers, not just 0 and 1, all along the x-axis:



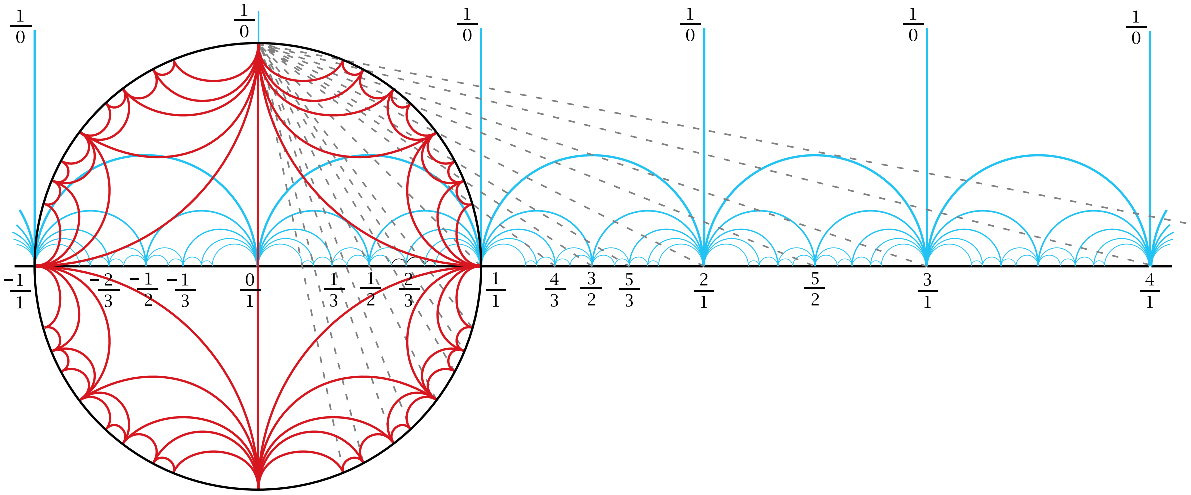
We can also put in vertical lines at the integer points, extending upward to infinity. These correspond to the edges having one endpoint at the vertex $1/0$ in the original Farey diagram.

We could also form a linear version of the full Farey diagram from copies of the square:

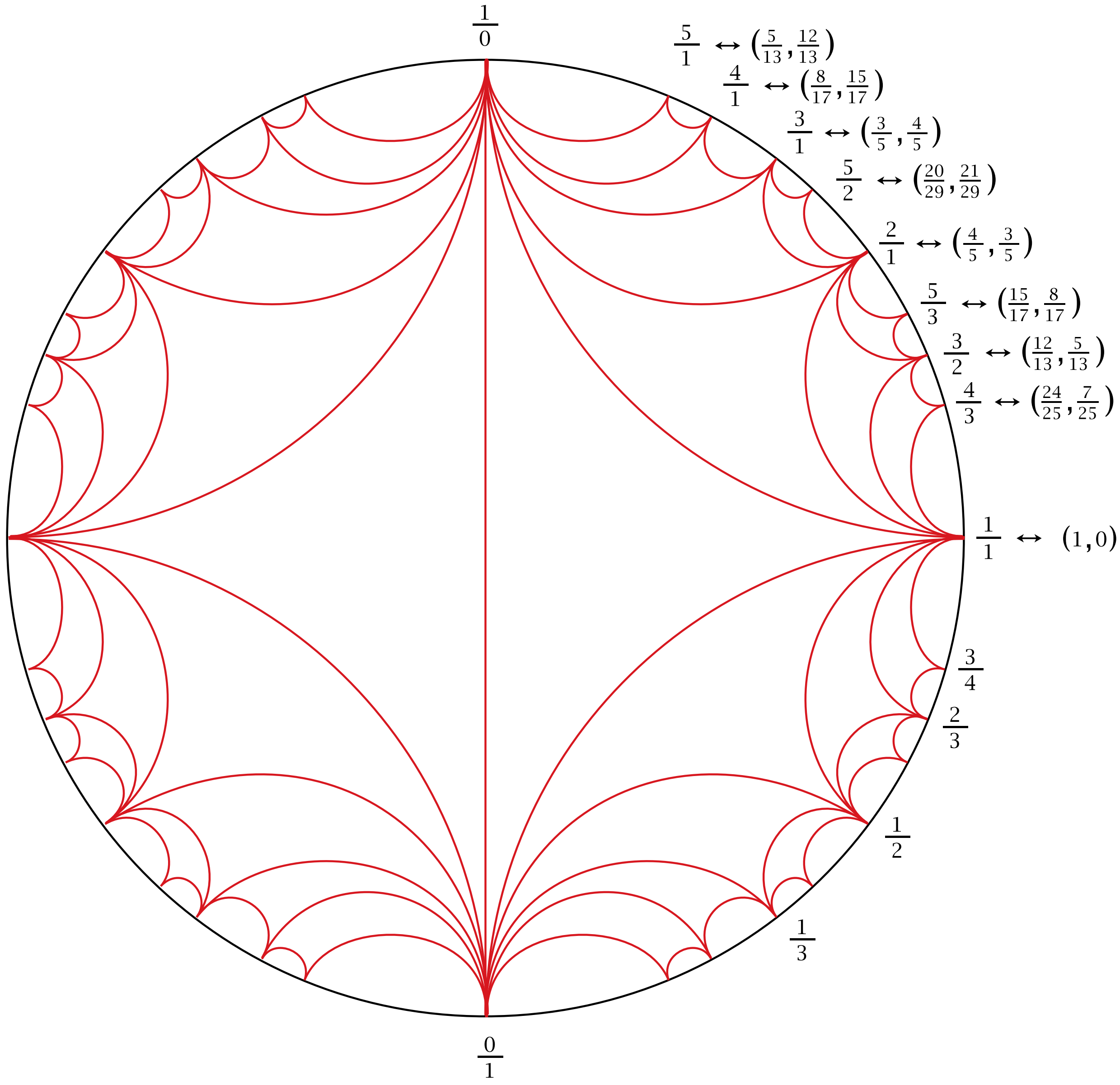


Relation with Pythagorean Triples

Next we describe a variant of the circular Farey diagram that is closely related to Pythagorean triples. Recall from Chapter 0 that rational points (x,y) on the unit circle correspond to rational points p/q on the x-axis by means of lines through the point $(0,1)$ on the circle. In formulas, $(x,y) = (\frac{2pq}{p^2+q^2}, \frac{p^2-q^2}{p^2+q^2})$. Using this correspondence, we can label the rational points on the circle by the corresponding rational points on the x-axis and then construct a new Farey diagram in the circle by filling in triangles by the mediant rule just as before.



The result is a version of the circular Farey diagram that is rotated by 90 degrees to put $1/0$ at the top of the circle, and there are also some perturbations of the positions of the other vertices and the shapes of the triangles. The next figure shows an enlargement of the new part of the diagram, with the vertices labeled by both the fraction p/q and the coordinates (x,y) of the vertex:

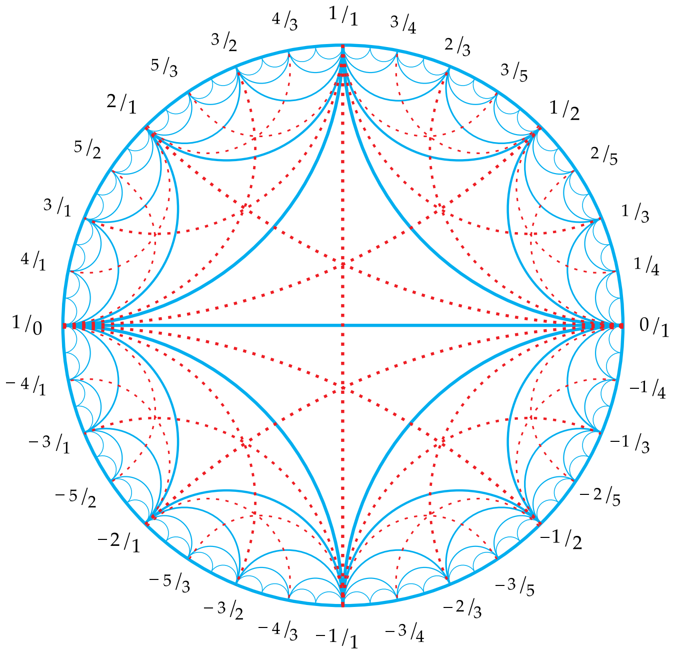


The Determinant Rule for Edges

The construction we have described for the Farey diagram involves an inductive process, where more and more triangles are added in succession. With a construction like this it is not easy to tell by a simple calculation whether or not two given rational numbers a/b and c/d are joined by an edge in the diagram. Fortunately there is such a criterion:

> *Two rational numbers a/b and c/d are joined by an edge in the Farey diagram exactly when the determinant $ad-bc$ of the matrix $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ is ± 1. This applies also when one of a/b or c/d is $\pm 1/0$.*

We will prove this in the next chapter. What it means in terms of the standard Farey diagram is that if one were to start with the upper half of the xy-plane and insert vertical lines through all the integer points on the x-axis, and then insert semicircles perpendicular to the x-axis joining each pair of rational points a/b and c/d such that $ad - bc = \pm 1$, then no two of these vertical lines or semicircles would cross, and they would divide the upper half of the plane into non-overlapping triangles. This is really quite remarkable when you think about it, and it does not happen for other values of the determinant besides ± 1. For example, for determinant ± 2 the edges would be the dotted lines in the figure below. Here there are three lines crossing in each triangle of the original Farey diagram, and these lines divide each triangle of the Farey diagram into six smaller triangles.



Exercises

1. This problem involves another version of the Farey diagram, or at least the positive part of the diagram, the part consisting of the triangles whose vertices are labeled by fractions p/q with $p \geq 0$ and $q \geq 0$. In this variant of the diagram the vertex labeled p/q is placed at the point (q, p) in the plane. Thus p/q is the slope of the line through the origin and (q, p). The edges of this new Farey diagram are straight line segments connecting the pairs of vertices that are connected in the original Farey diagram. For example there is a triangle with vertices $(1, 0)$, $(0, 1)$, and $(1, 1)$ corresponding to the big triangle in the upper half of the circular Farey diagram.

What you are asked to do in this problem is just to draw the portion of the new Farey diagram consisting of all the triangles whose vertices (q, p) satisfy $0 \leq q \leq 5$ and $0 \leq p \leq 5$. Note that since fractions p/q labeling vertices are always in lowest terms, the points (q, p) such that q and p have a common divisor greater than 1 are not vertices of the diagram.

A parenthetical comment: With this model of the Farey diagram the operation of forming the mediant of two fractions just corresponds to standard vector addition $(a, b) + (c, d) = (a + c, b + d)$, which may make the mediant operation seem more natural.

2. Compute the Farey series F_{10}.

Chapter 2. Continued Fractions

Here are two typical examples of continued fractions:

$$\frac{7}{16} = \cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{2}}} \qquad\qquad \frac{67}{24} = 2+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{4}}}}$$

To compute the value of a continued fraction one starts in the lower right corner and works one's way upward. For example in the continued fraction for $\frac{7}{16}$ one starts with $3+\frac{1}{2}=\frac{7}{2}$, then taking 1 over this gives $\frac{2}{7}$, and adding the 2 to this gives $\frac{16}{7}$, and finally 1 over this gives $\frac{7}{16}$.

Here is the general form of a continued fraction:

$$\frac{p}{q} = a_0 + \cfrac{1}{a_1+\cfrac{1}{a_2+\ddots+\cfrac{1}{a_n}}}$$

To write this in more compact form on a single line one can write it as

$$\frac{p}{q} = a_0 + {}^{1}\!\nearrow\!{}_{a_1} + {}^{1}\!\nearrow\!{}_{a_2} + \cdots + {}^{1}\!\nearrow\!{}_{a_n}$$

For example:

$$\frac{7}{16} = {}^{1}\!\nearrow\!{}_{2} + {}^{1}\!\nearrow\!{}_{3} + {}^{1}\!\nearrow\!{}_{2} \qquad\qquad \frac{67}{24} = 2 + {}^{1}\!\nearrow\!{}_{1} + {}^{1}\!\nearrow\!{}_{3} + {}^{1}\!\nearrow\!{}_{1} + {}^{1}\!\nearrow\!{}_{4}$$

This way of writing continued fractions with upward-pointing diagonal arrows is intended to be a more legible version of the classical notation

$$a_0 + \frac{1}{a_1+}\,\frac{1}{a_2+}\cdots\frac{1}{a_n}$$

often found in older books. A more abbreviated notation common in other books is simply $[a_0; a_1, a_2, \cdots, a_n]$, although we will not use this notation here.

To compute the continued fraction for a given rational number one starts in the upper left corner and works one's way downward, as the following example shows:

$$\frac{67}{24} = 2+\frac{19}{24} = 2+\frac{1}{24/19} = 2+\frac{1}{1+5/19} = 2+\cfrac{1}{1+\cfrac{1}{19/5}}$$

$$= 2+\cfrac{1}{1+\cfrac{1}{3+4/5}} = 2+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{5/4}}} = 2+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{4}}}}$$

If one is good at mental arithmetic and the numbers aren't too large, only the final form of the answer needs to be written down: $\frac{67}{24} = 2 + {}^{1}\!\nearrow\!{}_{1} + {}^{1}\!\nearrow\!{}_{3} + {}^{1}\!\nearrow\!{}_{1} + {}^{1}\!\nearrow\!{}_{4}$.

The Euclidean Algorithm

The process for computing the continued fraction for a given rational number is known as the *Euclidean Algorithm*. It consists of repeated division, at each stage dividing the previous remainder into the previous divisor. The procedure for $67/24$ is shown at the right. Note that the numbers in the shaded box are the numbers a_i in the continued fraction. These are the quotients of the successive divisions. They are sometimes called the *partial quotients* of the original fraction.

$$\begin{array}{rcl}
67 & = & 2 \cdot 24 + 19 \\
24 & = & 1 \cdot 19 + 5 \\
19 & = & 3 \cdot 5 + 4 \\
5 & = & 1 \cdot 4 + 1 \\
4 & = & 4 \cdot 1 + 0
\end{array}$$

One of the classical uses for the Euclidean algorithm is to find the greatest common divisor of two given numbers. If one applies the algorithm to two numbers p and q, dividing the smaller into the larger, then the remainder into the first divisor, and so on, then the greatest common divisor of p and q turns out to be the last nonzero remainder. For example, starting with $p = 72$ and $q = 201$ the calculation is shown at the right, and the last nonzero remainder is 3, which is the greatest common divisor of 72 and 201. (In fact the fraction $201/72$ equals $67/24$, which explains why the successive quotients for this example are the same as in the preceding example.) It is easy to see from the displayed equations why 3 has to be the greatest common divisor of 72 and 201, since from the first equation it follows that any divisor of 72 and 201 must also divide 57, then the second equation shows it must divide 15, the third equation then shows it must divide 12, and the fourth equation shows it must divide 3, the last nonzero remainder. Conversely, if a number divides the last nonzero remainder 3, then the last equation shows it must also divide the 12, and the next-to-last equation then shows it must divide 15, and so on until we conclude that it divides all the numbers not in the shaded rectangle, including the original two numbers 72 and 201. The same reasoning applies in general.

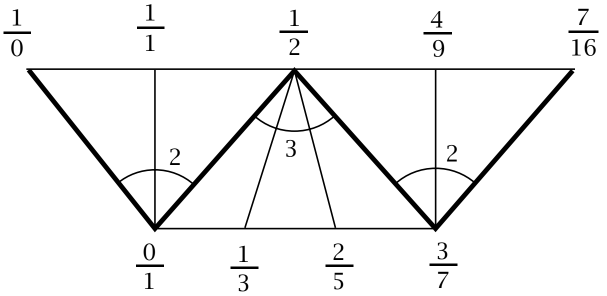
$$\begin{array}{rcl}
201 & = & 2 \cdot 72 + 57 \\
72 & = & 1 \cdot 57 + 15 \\
57 & = & 3 \cdot 15 + 12 \\
15 & = & 1 \cdot 12 + \textcircled{3} \\
12 & = & 4 \cdot 3 + 0
\end{array}$$

A more obvious way to try to compute the greatest common divisor of two numbers would be to factor each of them into a product of primes, then look to see which primes occurred as factors of both, and to what power. But to factor a large number into its prime factors is a very laborious and time-consuming process. For example, even a large computer would have a hard time factoring a number of a hundred digits into primes, so it would not be feasible to find the greatest common divisor of a pair of hundred-digit numbers this way. However, the computer would have no trouble at all applying the Euclidean algorithm to find their greatest common divisor.

Having seen what continued fractions are, let us now see what they have to do with the Farey diagram. Some examples will illustrate this best, so let us first look at the continued fraction for $7/16$ again. This has $2, 3, 2$ as its sequence of partial quotients.

We use these three numbers to build a strip of three large triangles subdivided into 2, 3, and 2 smaller triangles, from left to right:

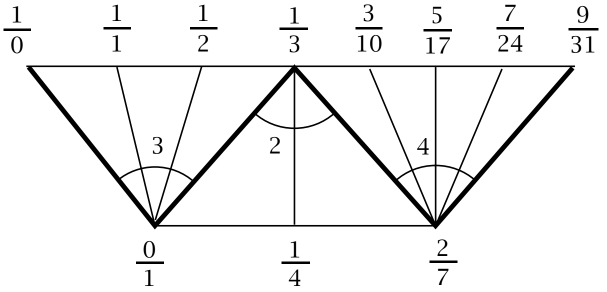
$$\frac{7}{16} = \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{2}}}$$



We can think of the diagram as being formed from three “fans”, where the first fan is made from the first 2 small triangles, the second fan from the next 3 small triangles, and the third fan from the last 2 small triangles. Now we begin labeling the vertices of this strip. On the left edge we start with the labels $1/0$ and $0/1$. Then we use the mediant rule for computing the third label of each triangle in succession as we move from left to right in the strip. Thus we insert, in order, the labels $1/1$, $1/2$, $1/3$, $2/5$, $3/7$, $4/9$, and finally $7/16$.

Was it just an accident that the final label was the fraction $7/16$ that we started with, or does this always happen? Doing more examples should help us decide. Here is a second example:

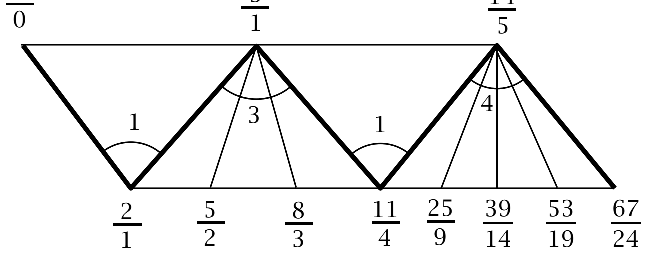
$$\frac{9}{31} = \cfrac{1}{3 + \cfrac{1}{2 + \cfrac{1}{4}}}$$



Again the final vertex on the right has the same label as the fraction we started with. The reader is encouraged to try more examples to make sure we are not rigging things to get a favorable outcome by only choosing examples that work.

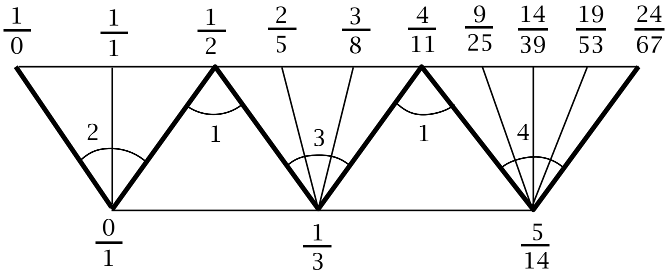
In fact this always works for fractions p/q between 0 and 1. For fractions larger than 1 the procedure works if we modify it by replacing the label $0/1$ with the initial integer $a_0/1$ in the continued fraction $a_0 + {}^{1}\!\diagup_{a_1} + {}^{1}\!\diagup_{a_2} + \cdots + {}^{1}\!\diagup_{a_n}$. This is illustrated by the $67/24$ example:

$$\frac{67}{24} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{4}}}}$$



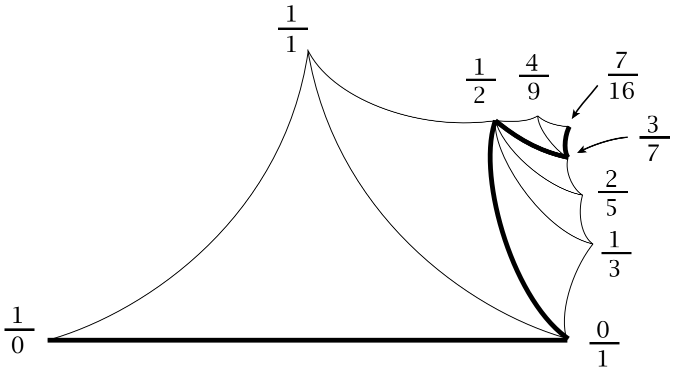
For comparison, here is the corresponding strip for the reciprocal, $24/67$:

$$\frac{24}{67} = \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{4}}}}}$$

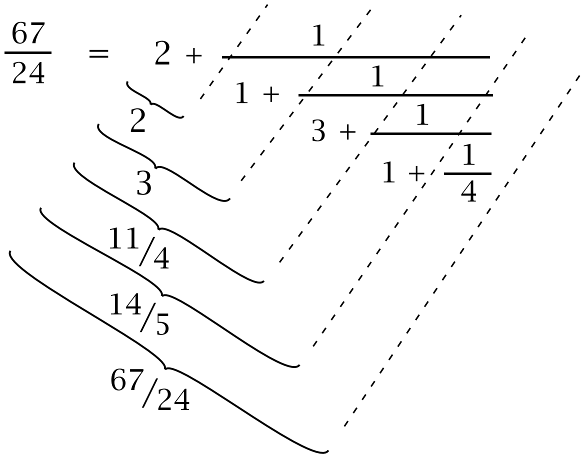


Now let us see how all this relates to the Farey diagram. Since the rule for labeling vertices in the triangles along the horizontal strip for a fraction p/q is the mediant rule, each of the triangles in the strip is a triangle in the Farey diagram, somewhat distorted in shape, and the strip of triangles can be regarded as a sequence of adjacent triangles in the diagram. Here is what this looks like for the fraction $7/16$ in the circular Farey diagram, slightly distorted for the sake of visual clarity:

$$\frac{7}{16} = \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{2}}}$$



In the strip of triangles for a fraction p/q there is a zigzag path from $1/0$ to p/q that we have indicated by the heavily shaded edges. The vertices that this zigzag path passes through have a special significance. They are the fractions that occur as the values of successively larger initial portions of the continued fraction, as illustrated in the following example:



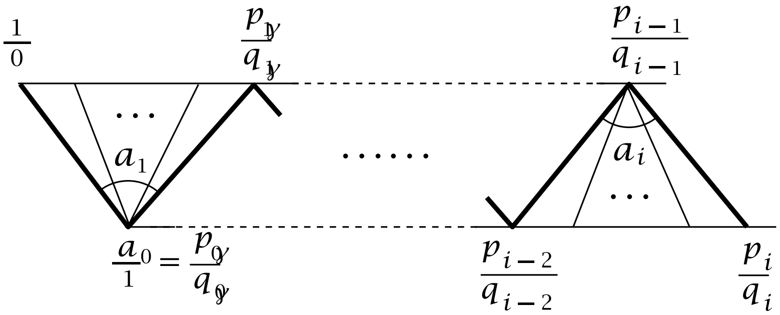
$$\frac{67}{24} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{4}}}}$$

These fractions are called the *convergents* for the given fraction. Thus the convergents for $67/24$ are 2, 3, $11/4$, $14/5$, and $67/24$ itself.

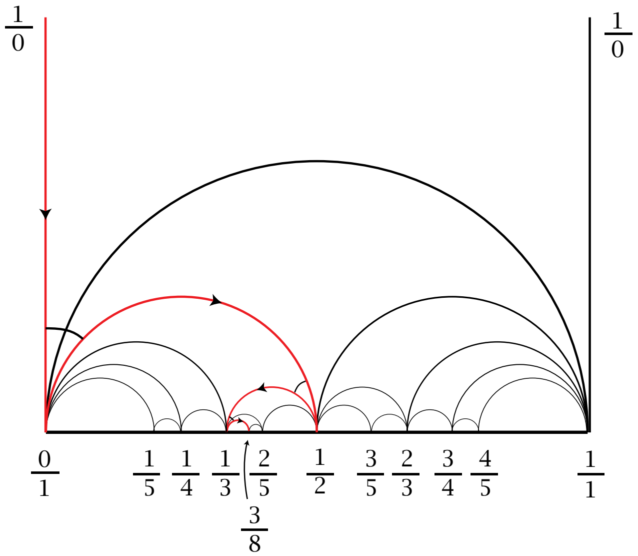
From the preceding examples one can see that each successive vertex label p_i/q_i along the zigzag path for a continued fraction $\frac{p}{q} = a_0 + {}^1\!/_{a_1} + {}^1\!/_{a_2} + \cdots + {}^1\!/_{a_n}$ is computed in terms of the two preceding vertex labels according to the rule

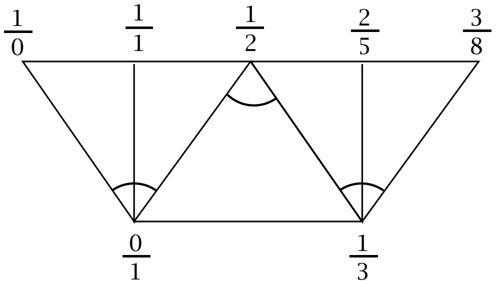
$$\frac{p_i}{q_i} = \frac{a_i p_{i-1} + p_{i-2}}{a_i q_{i-1} + q_{i-2}}$$

This is because the mediant rule is being applied a_i times, 'adding' p_{i-1}/q_{i-1} to the previously obtained fraction each time until the next label p_i/q_i is obtained.



It is interesting to see what the zigzag paths corresponding to continued fractions look like in the upper half-plane Farey diagram. The next figure shows the simple example of the continued fraction for $3/8$. We can see here that the five triangles of the strip correspond to the four curvilinear triangles lying directly above $3/8$ in the Farey diagram, plus the fifth 'triangle' extending upward to infinity, bounded on the left and right by the vertical lines above $0/1$ and $1/1$, and bounded below by the semicircle from $0/1$ to $1/1$.





This example is typical of the general case, where the zigzag path for a continued fraction $\frac{p}{q} = a_0 + {}^{1}\!\diagup_{a_1} + {}^{1}\!\diagup_{a_2} + \cdots + {}^{1}\!\diagup_{a_n}$ becomes a 'pinball path' in the Farey diagam, starting down the vertical line from $1/0$ to $a_0/1$, then turning left across a_1 triangles, then right across a_2 triangles, then left across a_3 triangles, continuing to alternate left and right turns until reaching the final vertex p/q. Two consequences of this are:

(1) The convergents are alternately smaller than and greater than p/q.

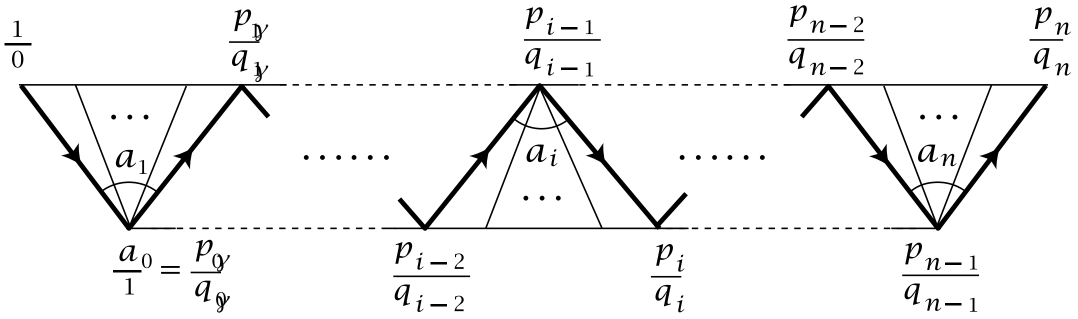
(2) The triangles that form the strip of triangles for p/q are exactly the triangles in the Farey diagram that lie directly above the point p/q on the x-axis.

Here is a general statement describing the relationship between continued fractions and the Farey diagram that we have observed in all our examples so far:

Theorem 2.1. *The convergents for a continued fraction* $\frac{p}{q} = a_0 + {}^1\!/_{a_1} + {}^1\!/_{a_2} + \cdots + {}^1\!/_{a_n}$ *are the vertices along a zigzag path consisting of a finite sequence of edges in the Farey diagram, starting at* $1/0$ *and ending at* p/q*. The path starts along the edge from* $1/0$ *to* $a_0/1$*, then turns left across a fan of* a_1 *triangles, then right across a fan of* a_2 *triangles, etc., finally ending at* p/q*.*

In particular, since every positive rational number has a continued fraction expansion, we see that every positive rational number occurs eventually as the label of some vertex in the positive half of the diagram. All negative rational numbers then occur as labels in the negative half.

Proof of the Theorem: The continued fraction $\frac{p}{q} = a_0 + {}^1\!/_{a_1} + {}^1\!/_{a_2} + \cdots + {}^1\!/_{a_n}$ determines a strip of triangles:



$\frac{1}{0}$
$\frac{p_1}{q_1}$
$\frac{p_{i-1}}{q_{i-1}}$
$\frac{p_{n-2}}{q_{n-2}}$
$\frac{p_n}{q_n}$
a_1
a_i
a_n
$\frac{a_0}{1} = \frac{p_0}{q_0}$
$\frac{p_{i-2}}{q_{i-2}}$
$\frac{p_i}{q_i}$
$\frac{p_{n-1}}{q_{n-1}}$

We will show that the label p_n/q_n on the final vertex in this strip is equal to p/q, the value of the continued fraction. Replacing n by i, we conclude that this holds also for each initial seqment $a_0 + {}^1\!/_{a_1} + {}^1\!/_{a_2} + \cdots + {}^1\!/_{a_i}$ of the continued fraction. This is just saying that the vertices p_i/q_i along the strip are the convergents to p/q, which is what the theorem claims.

To prove that $p_n/q_n = p/q$ we will use 2×2 matrices. Consider the product

$$P = \begin{pmatrix} 1 & a_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & a_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & a_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & a_n \end{pmatrix}$$

We can multiply this product out starting either from the left or from the right. Suppose first that we multiply starting at the left. The initial matrix is $\begin{pmatrix} 1 & a_0 \\ 0 & 1 \end{pmatrix}$ and we can view the two columns of this matrix as the two fractions $1/0$ and $a_0/1$ labeling the left edge of the strip of triangles. When we multiply this matrix by the next matrix we get

$$\begin{pmatrix} 1 & a_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & a_1 \end{pmatrix} = \begin{pmatrix} a_0 & 1 + a_0 a_1 \\ 1 & a_1 \end{pmatrix} = \begin{pmatrix} p_0 & p_1 \\ q_0 & q_1 \end{pmatrix}$$

The two columns here give the fractions at the ends of the second edge of the zigzag path. The same thing happens for subsequent matrix multiplications, as multiplying by the next matrix in the product takes the matrix corresponding to one edge of the zigzag path to the matrix corresponding to the next edge:

$$\begin{pmatrix} p_{i-2} & p_{i-1} \\ q_{i-2} & q_{i-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & a_i \end{pmatrix} = \begin{pmatrix} p_{i-1} & p_{i-2} + a_i p_{i-1} \\ q_{i-1} & q_{i-2} + a_i q_{i-1} \end{pmatrix} = \begin{pmatrix} p_{i-1} & p_i \\ q_{i-1} & q_i \end{pmatrix}$$

In the end, when all the matrices have been multiplied, we obtain the matrix corresponding to the last edge in the strip from p_{n-1}/q_{n-1} to p_n/q_n. Thus the second column of the product P is p_n/q_n, and what remains is to show that this equals the value p/q of the continued fraction $a_0 + {}^{1}\!\nearrow_{a_1} + {}^{1}\!\nearrow_{a_2} + \cdots + {}^{1}\!\nearrow_{a_n}$.

The value of the continued fraction $a_0 + {}^{1}\!\nearrow_{a_1} + {}^{1}\!\nearrow_{a_2} + \cdots + {}^{1}\!\nearrow_{a_n}$ is computed by working from right to left. If we let r_i/s_i be the value of the tail ${}^{1}\!\nearrow_{a_i} + {}^{1}\!\nearrow_{a_{i+1}} + \cdots + {}^{1}\!\nearrow_{a_n}$ of the continued fraction, then $r_n/s_n = 1/a_n$ and we have

$$\frac{r_i}{s_i} = \frac{1}{a_i + \dfrac{r_{i+1}}{s_{i+1}}} = \frac{s_{i+1}}{a_i s_{i+1} + r_{i+1}} \qquad \text{and finally} \qquad \frac{p}{q} = a_0 + \frac{r_1}{s_1} = \frac{a_0 s_1 + r_1}{s_1}$$

In terms of matrices this implies that we have

$$\begin{pmatrix} r_n \\ s_n \end{pmatrix} = \begin{pmatrix} 1 \\ a_n \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 \\ 1 & a_i \end{pmatrix} \begin{pmatrix} r_{i+1} \\ s_{i+1} \end{pmatrix} = \begin{pmatrix} s_{i+1} \\ r_{i+1} + a_i s_{i+1} \end{pmatrix} = \begin{pmatrix} r_i \\ s_i \end{pmatrix}$$

$$\text{and} \quad \begin{pmatrix} 1 & a_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} r_1 \\ s_1 \end{pmatrix} = \begin{pmatrix} r_1 + a_0 s_1 \\ s_1 \end{pmatrix} = \begin{pmatrix} p \\ q \end{pmatrix}$$

This means that when we multiply out the product P starting from the right, then the second columns will be successively $\begin{pmatrix} r_n \\ s_n \end{pmatrix}, \begin{pmatrix} r_{n-1} \\ s_{n-1} \end{pmatrix}, \cdots, \begin{pmatrix} r_1 \\ s_1 \end{pmatrix}$ and finally $\begin{pmatrix} p \\ q \end{pmatrix}$. We already showed this second column is $\begin{pmatrix} p_n \\ q_n \end{pmatrix}$, so $p/q = p_n/q_n$ and the proof is complete. □

An interesting fact that can be deduced from the preceding proof is that for a continued fraction ${}^{1}\!\nearrow_{a_1} + {}^{1}\!\nearrow_{a_2} + \cdots + {}^{1}\!\nearrow_{a_n}$ with no initial integer a_0, if we reverse the order of the numbers a_i, this leaves the denominator unchanged. For example

$${}^{1}\!\nearrow_{2} + {}^{1}\!\nearrow_{3} + {}^{1}\!\nearrow_{4} = \frac{13}{30} \qquad \text{and} \qquad {}^{1}\!\nearrow_{4} + {}^{1}\!\nearrow_{3} + {}^{1}\!\nearrow_{2} = \frac{7}{30}$$

To see why this must always be true we use the operation of transposing a matrix to interchange its rows and columns. For a 2×2 matrix this just amounts to interchanging the upper-right and lower-left entries:

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix}^T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Transposing a product of matrices reverses the order of the factors: $(AB)^T = B^T A^T$, as can be checked by direct calculation. In the product

$$\begin{pmatrix} 0 & 1 \\ 1 & a_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & a_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & a_n \end{pmatrix} = \begin{pmatrix} p_{n-1} & p_n \\ q_{n-1} & q_n \end{pmatrix}$$

the individual matrices on the left side of the equation are symmetric with respect to transposition, so the transpose of the product is obtained by just reversing the order of the factors:

$$\begin{pmatrix} 0 & 1 \\ 1 & a_n \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & a_{n-1} \end{pmatrix}\cdots\begin{pmatrix} 0 & 1 \\ 1 & a_1 \end{pmatrix} = \begin{pmatrix} p_{n-1} & q_{n-1} \\ p_n & q_n \end{pmatrix}$$

Thus the denominator q_n is unchanged, as claimed.

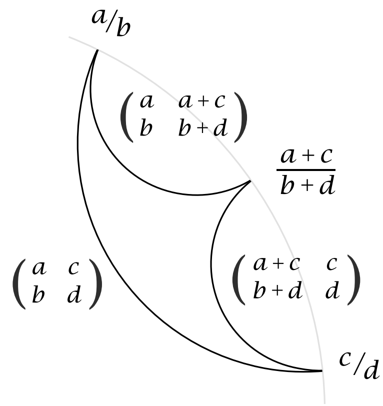
There is also a fairly simple relationship between the numerators. In the example of $13/30$ and $7/30$ we see that the product of the numerators, 91, is congruent to 1 modulo the denominator. In the general case the product of the numerators is $p_n q_{n-1}$ and this is congruent to $(-1)^{n+1}$ modulo the denominator q_n. To verify this, we note that the determinant of each factor $\begin{pmatrix} 0 & 1 \\ 1 & a_i \end{pmatrix}$ is -1 so since the determinant of a product is the product of the determinants, we have $p_{n-1}q_n - p_n q_{n-1} = (-1)^n$, which says that $p_n q_{n-1}$ is congruent to $(-1)^{n+1}$ modulo q_n.

Determinants Determine Edges

We constructed the Farey diagram by an inductive procedure, inserting successive edges according to the mediant rule, but there is another rule that can be used to characterize the edges in the diagram:

Theorem 2.2. *In the Farey diagram, two vertices labeled a/b and c/d are joined by an edge if and only if the determinant $ad - bc$ of the matrix $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$ is equal to ± 1.*

Proof: First we show that for an arbitrary edge in the diagram joining a/b to c/d, the associated matrix $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$ has determinant ± 1. This is obviously true for the edges in the two largest triangles in the circular version of the diagram. For the smaller triangles we proceed by induction. The figure at the right shows the three matrices corresponding to the edges of one of these smaller triangles. By induction we assume we know that $ad - bc = \pm 1$ for the long edge of the triangle. Then the determinant condition holds also for the two shorter edges of the triangle since $a(b+d) - b(a+c) = ad - bc$ and $(a+c)d - (b+d)c = ad - bc$.

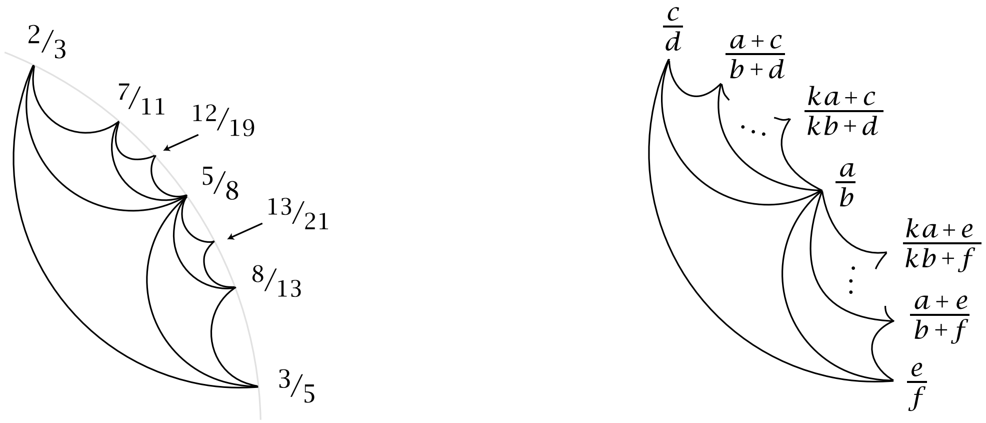

a/b
$\begin{pmatrix} a & a+c \\ b & b+d \end{pmatrix}$
$\frac{a+c}{b+d}$
$\begin{pmatrix} a & c \\ b & d \end{pmatrix}$
$\begin{pmatrix} a+c & c \\ b+d & d \end{pmatrix}$
c/d

Before proving the converse let us pause to apply what we have shown so far to deduce a basic fact about the Farey diagram that was mentioned but not proved when we first constructed the diagram:

Corollary 2.3. *The mediant rule for labeling the vertices in the Farey diagram always produces labels a/b that are fractions in lowest terms.*

Proof: Consider an edge joining a vertex labeled a/b to some other vertex labeled c/d. We know from the argument given above that $ad - bc = \pm 1$. This equation implies that a and b can have no common divisor greater than 1 since any common divisor of a and b must divide the products ad and bc, hence also the difference $ad - bc = \pm 1$, but the only divisors of ± 1 are ± 1. □

Now we return to proving the converse half of the theorem, which says that there is an edge joining a/b to c/d whenever $ad - bc = \pm 1$. To do this we will examine how all the edges emanating from a fixed vertex a/b are related. To begin, if $a/b = 0/1$ then the matrices $\begin{pmatrix} 0 & c \\ 1 & d \end{pmatrix}$ with determinant ± 1 are the matrices $\begin{pmatrix} 0 & \pm 1 \\ 1 & d \end{pmatrix}$, and these correspond exactly to the edges in the diagram from $0/1$ to $\pm 1/d$. There is a similar exact correspondence for the edges from $1/0$. For the other vertices a/b, the example $a/b = 5/8$ is shown in the left half of the figure below. The first edges drawn to this vertex come from $2/3$ and $3/5$, and after this all the other edges from $5/8$ are drawn in turn. As one can see, they are all obtained by adding $(5, 8)$ to $(2, 3)$ or $(3, 5)$ repeatedly. If we choose any one of these edges from $5/8$, say the edge to $2/3$ for example, then the edges from $5/8$ have their other endpoints at the fractions $(2 + 5k)/(3 + 8k)$ as k ranges over all integers, with positive values of k giving the edges on the upper side of the edge to $2/3$ and negative values of k giving the edges on the lower side of the edge to $2/3$.



The same thing happens for an arbitrary value of a/b as shown in the right half of the figure, where a/b initially arises as the mediant of c/d and e/f. In this case if we choose the edge to c/d as the starting edge, then the other edges go from a/b to $(c + ka)/(d + kb)$. In particular, when $k = -1$ we get the edge to $(c - a)/(d - b) = (a - c)/(b - d) = e/f$.

To finish the argument we need to know how the various matrices $\left(\begin{smallmatrix} a & x \\ b & y \end{smallmatrix}\right)$ of determinant $ay - bx = \pm 1$ having the same first column are related. This can be deduced from the following result about integer solutions of linear equations with integer coefficients:

Lemma 2.4. *Suppose a and b are integers with no common divisor greater than 1. If one solution of $ay - bx = n$ is $(x, y) = (c, d)$, then the general solution is $(x, y) = (c + ka, d + kb)$ for k an arbitrary integer.*

The proof will use the same basic argument as is used in linear algebra to show that the general solution of a system of nonhomogeneous linear equations is obtained from any particular solution by adding the general solution of the associated system of homogeneous equations.

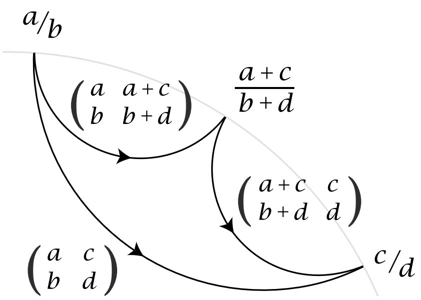
Before giving the proof let us introduce a convenient bit of standard terminology. If two integers a and b have no common divisor greater than 1 then a and b are said to be *coprime*. One can also say that a is coprime to b, or symmetrically, b is coprime to a. A commonly used synonym for coprime is *relatively prime*.

Proof: One solution $(x,y)=(c,d)$ of $ay-bx=n$ is given. For an arbitrary solution (x,y) we look at the difference $(x_0,y_0)=(x-c,y-d)$. This satisfies $ay_0-bx_0=0$, or in other words, $ay_0=bx_0$. Since a and b are coprime, the equation $ay_0=bx_0$ implies that x_0 must be a multiple of a and y_0 must be a multiple of b, in fact the same multiple in both cases so that the equation becomes $a(kb)=b(ka)$. Thus we have $(x_0,y_0)=(ka,kb)$ for some integer k. Thus every solution of $ay-bx=n$ has the form $(x,y)=(c+x_0,d+y_0)=(c+ka,d+kb)$, and it is clear that these formulas for x and y give solutions for all values of k. □

Now we can easily finish the proof of the theorem. The lemma in the cases $n=\pm1$ implies that the edges in the Farey diagram with a/b at one endpoint account for all matrices $\left(\begin{smallmatrix} a & x \\ b & y \end{smallmatrix}\right)$ of determinant $ay-bx=\pm1$. □

There is some ambiguity in the correspondence between edges of the Farey diagram and matrices $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$ of determinant ±1. For one thing, either column of the matrix can be multiplied by -1, changing the sign of the determinant without changing the value of the fractions a/b and c/d. This ambiguity can be eliminated by choosing all of a, b, c, and d to be positive for edges in the upper half of the circular Farey diagram, and choosing just the numerators a and c to be negative for edges in the lower half of the diagram. The only other ambiguity is that both $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} c & a \\ d & b \end{smallmatrix}\right)$ correspond to the same edge. This ambiguity can be eliminated by orienting the edges by placing an arrowhead on each edge pointing from the vertex corresponding to the first column of the matrix to the vertex corresponding to the second column. Changing the orientation of an edge switches the two columns of the matrix, which changes the sign of the determinant.

The identity matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ has determinant $+1$ and corresponds to the edge from $1/0$ to $0/1$ oriented from left to right in the circular diagram. We can use this orientation to give orientations to all other edges when we build the diagram using the mediant rule. In the upper half of the diagram this makes all edges be oriented toward the right, or in


a/b
$\frac{a+c}{b+d}$
$\begin{pmatrix} a & a+c \\ b & b+d \end{pmatrix}$
$\begin{pmatrix} a+c & c \\ b+d & d \end{pmatrix}$
$\begin{pmatrix} a & c \\ b & d \end{pmatrix}$
c/d

other words from a/b to c/d with $a/b > c/d$. With this orientation, all the corresponding matrices have determinant $+1$ since $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ has determinant $+1$ and we have seen that the determinant doesn't change when we add new edges by the mediant rule. When we use the mediant rule to construct the lower half of the diagram we have to start with $-1/0$ instead of $1/0$. This means that we are starting with the matrix $\left(\begin{smallmatrix}-1&0\\0&1\end{smallmatrix}\right)$ instead of $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$. Since the determinant of $\left(\begin{smallmatrix}-1&0\\0&1\end{smallmatrix}\right)$ is -1, this means that the edges in the lower half of the diagram, when oriented toward the right as in the upper half, correspond to matrices of determinant -1.

The Diophantine Equation ax+by=n

The Euclidean algorithm and continued fractions can be used to compute all the integer solutions of a linear equation $ax + by = n$ where a, b, and n are given integers. We can assume neither a nor b is zero, otherwise the equation is rather trivial. Changing the signs of x or y if necessary, we can rewrite the equation in the form $ax - by = n$ where a and b are both positive.

If a and b have greatest common divisor $d > 1$, then since d divides a and b it must divide $ax - by$, so d must divide n if the equation is to have any solutions at all. If d does divide n we can divide both sides of the equation by d to get a new equation of the same type as the original one and having the same solutions, but with the new coefficients a and b being coprime. For example, the equation $6x-15y = 21$ reduces in this way to the equation $2x - 5y = 7$. Thus we can assume from now on that a and b are coprime.

The Lemma from a page or two back shows how to find the general solution of $ax-by = n$ once we have found one particular solution. To find a particular solution it suffices to do the case $n = 1$ since if we have a solution of $ax - by = 1$, we can multiply x and y by n to get a solution of $ax - by = n$. For small values of a and b a solution of $ax - by = 1$ can be found more or less by inspection since the equation $ax - by = 1$ says that we have a multiple of a that is 1 greater than a multiple of b. For example, for the equation $2x - 5y = 1$ the smallest multiples of 2 that is one greater than a multiple of 5 is $2 \cdot 3 > 5 \cdot 1$, so a solution of $2x - 5y = 1$ is $(x, y) = (3, 1)$. A solution of $2x - 5y = 7$ is then $(x, y) = (21, 7)$. By the earlier Lemma, the general solution of $2x-5y = 7$ is $(x, y) = (21+5k, 7+2k)$ for arbitrary integers k. The smallest positive solution is $(6, 1)$, obtained by setting $k = -3$. This means we could also write the general solution as $(6 + 5k, 1 + 2k)$.

Solutions of $ax - by = 1$ always exist when a and b are coprime, and a way to find one is to find an edge in the Farey diagram with a/b at one end of the edge. This can be done by using the Euclidean algorithm to compute the strip of triangles from $1/0$ to a/b. As an example, let us solve $67x-24y = 1$. We already computed the strip of triangles for $67/24$ earlier in the chapter. The vertex preceding $67/24$ in the zigzag path is $14/5$ and this vertex lies above $67/24$ so we have $14/5 > 67/24$ and hence the matrix $\begin{pmatrix} 14 & 67 \\ 5 & 24 \end{pmatrix}$ has determinant $+1$. (One can easily distinguish determinant $+1$ from determinant -1 by computing just the last digit of the determinant.) Thus we have $14 \cdot 24 - 5 \cdot 67 = 1$ so one solution of $67x - 24y = 1$ is $(x, y) = (-5, -14)$ and the general solution is $(x, y) = (-5 + 24k, -14 + 67k)$. We could also use the edge from $53/19$ to $67/24$, so $\begin{pmatrix} 67 & 53 \\ 24 & 19 \end{pmatrix}$ has determinant $+1$, yielding another formula for the general solution $(19 + 24k, 53 + 67k)$.

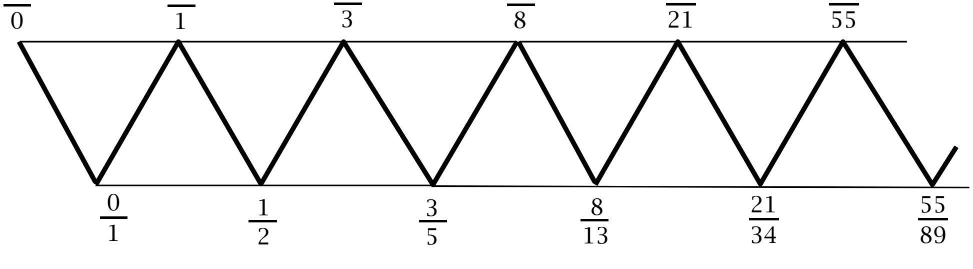
From a geometric point of view, finding the integer solutions of $ax + by = n$ is finding the points on the line $ax + by = n$ in the xy-plane having both coordinates integers. The points in the plane having both coordinates integers form a square grid called the *integer lattice*. Thus we wish to see which points in the integer lattice lie on the line $ax + by = n$. This equation can be written in the form $y = mx + b$ where the slope m and the y-intercept b are both rational. Conversely, an equation $y = mx + b$ with m and b rational can be written as an equation $ax + by = n$ with a, b, and n integers by multiplying through by a common denominator of m and b. Sometimes the equation $ax + by = n$ has no integer solutions, as we have seen, namely when n is not a multiple of the greatest common divisor of a and b, for example the equation $2x + 2y = 1$. In these cases the line $ax + by = n$ passes through no integer lattice points. In the opposite case that there does exist an integer solution, there are infinitely many, and they correspond to integer lattice points spaced at equal intervals along the line.

Infinite Continued Fractions

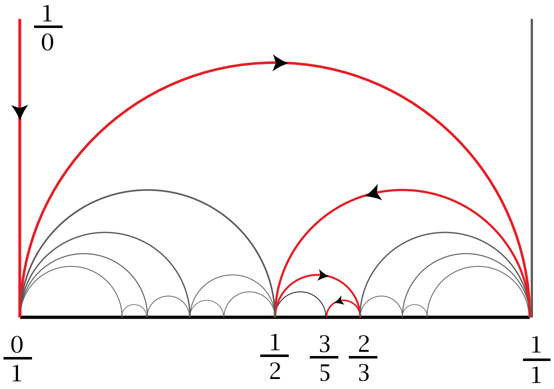
We have seen that all rational numbers can be represented as continued fractions $a_0 + {}^1\!\diagup\!{}_{a_1} + {}^1\!\diagup\!{}_{a_2} + \cdots + {}^1\!\diagup\!{}_{a_n}$, but what about irrational numbers? It turns out that these can be represented as *infinite* continued fractions $a_0 + {}^1\!\diagup\!{}_{a_1} + {}^1\!\diagup\!{}_{a_2} + {}^1\!\diagup\!{}_{a_3} + \cdots$. A simple example is ${}^1\!\diagup\!{}_1 + {}^1\!\diagup\!{}_1 + {}^1\!\diagup\!{}_1 + \cdots$, or in its expanded form:

$$\cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}}}$$

The corresponding strip of triangles is infinite:



Notice that these fractions after $1/0$ are the successive ratios of the famous Fibonacci sequence $0, 1, 1, 2, 3, 5, 8, 13, 21, \cdots$ where each number is the sum of its two predecessors. The sequence of convergents is thus $0/1, 1/1, 1/2, 2/3, 3/5, 5/8, 8/13, \cdots$, the vertices along the zigzag path. The way this zigzag path looks in the standard Farey diagram is shown in the figure at the right. What happens when we follow this path farther and farther? The path consists of an infinite sequence of semicircles, each one shorter than the preceding one and sharing a common endpoint. The left endpoints of the semicircles form an increasing sequence of numbers which have to be approaching a certain limiting value x. We know x has to be finite since it is certainly less than each of the right-hand endpoints of the semicircles, the convergents $1/1, 2/3, 5/8, \cdots$. Similarly the right endpoints of the semicircles form a decreasing sequence of numbers approaching a limiting value y greater than each of the left-hand endpoints $0/1, 1/2, 3/5, \cdots$. Obviously $x \le y$. Is it possible that x is not equal to y? If this happened, the infinite sequence of semicircles would be approaching the semicircle from x to y. Above this semicircle there would then be an infinite number of semicircles, all the semicircles in the infinite sequence. Between x and y there would have to be a rational numbers p/q (between any two real numbers there is always a rational number), so above this rational number there would be an infinite number of semicircles, hence an infinite number of triangles in the Farey diagram. But we know that there are only finitely many triangles above any rational number p/q, namely the triangles that appear in the strip for the continued fraction for p/q. This contradiction shows that x has to be equal to y. Thus the sequence of convergents along the edges of the infinite strip of triangles converges to a unique real number x. (This is why the convergents are called convergents.)



This argument works for arbitrary infinite continued fractions, so we have shown the following general result:

Proposition 2.5. *For every infinite continued fraction* $a_0 + {}^1\!/_{a_1} + {}^1\!/_{a_2} + {}^1\!/_{a_3} + \cdots$ *the convergents converge to a unique limit.*

This limit is by definition the value of the infinite continued fraction. There is a simple method for computing the value in the example involving Fibonacci numbers. We begin by setting

$$x = {}^1\!/_1 + {}^1\!/_1 + {}^1\!/_1 + \cdots$$

Then if we take the reciprocals of both sides of this equation we get

$$\frac{1}{x} = 1 + {}^1\!/_1 + {}^1\!/_1 + {}^1\!/_1 + \cdots$$

The right side of this equation is just $1 + x$, so we can easily solve for x:

$$\begin{aligned}\frac{1}{x} &= 1 + x \\ 1 &= x + x^2 \\ x^2 + x - 1 &= 0 \\ x &= \frac{-1 \pm \sqrt{5}}{2}\end{aligned}$$

We know x is positive, so this rules out the negative root and we are left with the final value $x = (-1 + \sqrt{5})/2$. (This number, approximately $.618$, goes by the name of the golden ratio because of its many interesting and beautiful properties.)

Proposition 2.6. *Every irrational number has an expression as an infinite continued fraction, and this continued fraction is unique.*

Proof: In the Farey diagram consider the vertical line L going upward from a given irrational number x on the x-axis. The lower endpoint of L is not a vertex of the Farey diagram since x is irrational. Thus as we move downward along L we cross a sequence of triangles, entering each triangle by crossing its upper edge and exiting the triangle by crossing one of its two lower edges. When we exit one triangle we are entering another, the one just below it, so the sequence of triangles and edges we cross must be infinite. The left and right endpoints of the edges in the sequence must be approaching the single point x by the argument we gave in the preceding proposition, so the edges themselves are approaching x. Thus the triangles in the sequence form a single infinite strip consisting of an infinite sequence of fans with their pivot vertices on alternate sides of the strip. The zigzag path along this strip gives a continued fraction for x.

For the uniqueness, we have seen that an infinite continued fraction for x corresponds to a zigzag path in the infinite strip of triangles lying above x. This set of triangles is unique so the strip is unique, and there is only one path in this strip that starts at $1/0$ and then does left and right turns alternately, starting with a left turn. The initial turn must be to the left because the first two convergents are a_0 and $a_0 + \frac{1}{a_1}$, with $a_0 + \frac{1}{a_1} > a_0$ since $a_1 > 0$. After the path traverses the first edge, no subsequent edge of the path can go along the border of the strip since this would entail two successive left turns or two successive right turns. □

The arguments we have just given can be used to prove a fact about the standard Farey diagram that we have been taking more or less for granted. This is the fact that the triangles in the diagram completely cover the upper halfplane. In other words, every point (x, y) with $y > 0$ lies either in the interior of some triangle or on the common edge between two triangles. To see why, consider the vertical line L in the upper halfplane through the given point (x, y). If x is an integer then (x, y) is on one of the vertical edges of the diagram. Thus we can assume x is not an integer and hence L is not one of the vertical edges of the diagram. The line L will then be contained in the strip of triangles corresponding to the continued fraction for x. This is a finite strip if x is rational and an infinite strip if x is irrational. In either case the point (x, y), being in L, will be in one of the triangles of the strip or on an edge separating two triangles in the strip. This proves what we wanted to prove.

To compute the infinite continued fraction $a_0 + {}^{1}\!/\!_{a_1} + {}^{1}\!/\!_{a_2} + {}^{1}\!/\!_{a_3} + \cdots$ for a given irrational number x we can follow the same procedure as for rational numbers, but it doesn't terminate after a finite number of steps. Recall the original example that we did:

$$\frac{67}{24} = 2 + \frac{19}{24} = 2 + \cfrac{1}{24/19} = 2 + \cfrac{1}{1 + 5/19} = 2 + \cfrac{1}{1 + \cfrac{1}{19/5}}$$

$$= 2 + \cfrac{1}{1 + \cfrac{1}{3 + 4/5}} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{5/4}}} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{4}}}}$$

The sequence of steps is the following:

(1) Write $x = a_0 + r_1$ where a_0 is an integer and $0 \le r_1 < 1$
(2) Write $1/r_1 = a_1 + r_2$ where a_1 is an integer and $0 \le r_2 < 1$
(3) Write $1/r_2 = a_2 + r_3$ where a_2 is an integer and $0 \le r_3 < 1$

and so on, repeatedly. Thus one first finds the largest integer $a_0 \le x$, with r_1 the 'remainder', then one inverts r_1 and finds the greatest integer $a_1 \le 1/r_1$, with r_2 the remainder, etc.

Here is how this works for $x = \sqrt{2}$:

(1) $\sqrt{2} = 1 + (\sqrt{2} - 1)$ where $a_0 = 1$ since $\sqrt{2}$ is between 1 and 2. Before going on to step (2) we have to compute $\frac{1}{r_1} = \frac{1}{\sqrt{2}-1}$. Multiplying numerator and denominator by $\sqrt{2} + 1$ gives $\frac{1}{\sqrt{2}-1} = \frac{1}{\sqrt{2}-1} \cdot \frac{\sqrt{2}+1}{\sqrt{2}+1} = \sqrt{2} + 1$. This is the number we use in the next step.

(2) $\sqrt{2} + 1 = 2 + (\sqrt{2} - 1)$ since $\sqrt{2} + 1$ is between 2 and 3.

Notice that something unexpected has happened: The remainder $r_2 = \sqrt{2} - 1$ is exactly the same as the previous remainder r_1. There is then no need to do the calculation of $\frac{1}{r_2} = \frac{1}{\sqrt{2}-1}$ since we know it will have to be $\sqrt{2} + 1$. This means that the next step (3) will be exactly the same as step (2), and the same will be true for all subsequent steps. Hence we get the continued fraction

$$\sqrt{2} = 1 + {}^{1}\!/\!_{2} + {}^{1}\!/\!_{2} + {}^{1}\!/\!_{2} + \cdots$$

We can check this calculation by finding the value of the continued fraction in the same way that we did earlier for ${}^{1}\!/\!_{1} + {}^{1}\!/\!_{1} + {}^{1}\!/\!_{1} + \cdots$. First we set $x = {}^{1}\!/\!_{2} + {}^{1}\!/\!_{2} + {}^{1}\!/\!_{2} + \cdots$.

Taking reciprocals gives $1/x = 2 + {}^1\!\diagup_2 + {}^1\!\diagup_2 + {}^1\!\diagup_2 + \cdots = 2 + x$. This leads to the quadratic equation $x^2 + 2x - 1 = 0$, which has roots $x = -1 \pm \sqrt{2}$. Since x is positive we can discard the negative root. Thus we have $-1 + \sqrt{2} = {}^1\!\diagup_2 + {}^1\!\diagup_2 + {}^1\!\diagup_2 + \cdots$. Adding 1 to both sides of this equation gives the formula for $\sqrt{2}$ as a continued fraction.

We can get good rational approximations to $\sqrt{2}$ by computing the convergents in its continued fraction $1 + {}^1\!\diagup_2 + {}^1\!\diagup_2 + {}^1\!\diagup_2 + \cdots$. It's a little easier to compute the convergents in $2 + {}^1\!\diagup_2 + {}^1\!\diagup_2 + {}^1\!\diagup_2 + \cdots = 1 + \sqrt{2}$ and then subtract 1 from each of these. For $2 + {}^1\!\diagup_2 + {}^1\!\diagup_2 + {}^1\!\diagup_2 + \cdots$ there is a nice pattern to the convergents:

$$\frac{2}{1}, \frac{5}{2}, \frac{12}{5}, \frac{29}{12}, \frac{70}{29}, \frac{169}{70}, \frac{408}{169}, \frac{985}{408}, \cdots$$

Notice that the sequence of numbers $1, 2, 5, 12, 29, 70, 169, \cdots$ is constructed in a way somewhat analogous to the Fibonacci sequence, except that each number is *twice* the preceding number plus the number before that. (It's easy to see why this has to be true, because each convergent is constructed from the previous one by inverting the fraction and adding 2.) After subtracting 1 from each of these fractions we get the convergents to $\sqrt{2}$:

$$\begin{aligned} \sqrt{2} &= 1.41421356\cdots \\ 1/1 &= 1.00000000\cdots \\ 3/2 &= 1.50000000\cdots \\ 7/5 &= 1.40000000\cdots \\ 17/12 &= 1.41666666\cdots \\ 41/29 &= 1.41379310\cdots \\ 99/70 &= 1.41428571\cdots \\ 239/169 &= 1.41420118\cdots \\ 577/408 &= 1.41421568\cdots \end{aligned}$$

We can compute the continued fraction for $\sqrt{3}$ by the same method as for $\sqrt{2}$, but something slightly different happens:

(1) $\sqrt{3} = 1 + (\sqrt{3} - 1)$ since $\sqrt{3}$ is between 1 and 2. Computing $\frac{1}{\sqrt{3}-1}$, we have $\frac{1}{\sqrt{3}-1} = \frac{1}{\sqrt{3}-1} \cdot \frac{\sqrt{3}+1}{\sqrt{3}+1} = \frac{\sqrt{3}+1}{2}$.

(2) $\frac{\sqrt{3}+1}{2} = 1 + (\frac{\sqrt{3}-1}{2})$ since the numerator $\sqrt{3}+1$ of $\frac{\sqrt{3}+1}{2}$ is between 2 and 3. Now we have a remainder $r_2 = \frac{\sqrt{3}-1}{2}$ which is different from the previous remainder $r_1 = \sqrt{3} - 1$, so we have to compute $\frac{1}{r_2} = \frac{2}{\sqrt{3}-1}$, namely $\frac{2}{\sqrt{3}-1} = \frac{2}{\sqrt{3}-1} \cdot \frac{\sqrt{3}+1}{\sqrt{3}+1} = \sqrt{3} + 1$.

(3) $\sqrt{3} + 1 = 2 + (\sqrt{3} - 1)$ since $\sqrt{3} + 1$ is between 2 and 3.

Now this remainder $r_3 = \sqrt{3} - 1$ is the same as r_1, so instead of the same step being repeated infinitely often, as happened for $\sqrt{2}$, the same two steps will repeat infinitely often. This means we get the continued fraction

$$\sqrt{3} = 1 + {}^1\!\diagup_1 + {}^1\!\diagup_2 + {}^1\!\diagup_1 + {}^1\!\diagup_2 + {}^1\!\diagup_1 + {}^1\!\diagup_2 + \cdots$$

Checking this takes a little more work than before. We begin by isolating the part of the continued fraction that repeats periodically, so we set

$$x = {}^1\!/\!_1 + {}^1\!/\!_2 + {}^1\!/\!_1 + {}^1\!/\!_2 + {}^1\!/\!_1 + {}^1\!/\!_2 + \cdots$$

Taking reciprocals, we get

$$\frac{1}{x} = 1 + {}^1\!/\!_2 + {}^1\!/\!_1 + {}^1\!/\!_2 + {}^1\!/\!_1 + {}^1\!/\!_2 + \cdots$$

Subtracting 1 from both sides gives

$$\frac{1}{x} - 1 = {}^1\!/\!_2 + {}^1\!/\!_1 + {}^1\!/\!_2 + {}^1\!/\!_1 + {}^1\!/\!_2 + \cdots$$

The next step will be to take reciprocals of both sides, so before doing this we rewrite the left side as $\frac{1-x}{x}$. Then taking reciprocals gives

$$\frac{x}{1-x} = 2 + {}^1\!/\!_1 + {}^1\!/\!_2 + {}^1\!/\!_1 + {}^1\!/\!_2 + \cdots$$

Hence

$$\frac{x}{1-x} - 2 = {}^1\!/\!_1 + {}^1\!/\!_2 + {}^1\!/\!_1 + {}^1\!/\!_2 + \cdots = x$$

Now we have the equation $\frac{x}{1-x} - 2 = x$ which can be simplified to the quadratic equation $x^2+2x-2 = 0$, with roots $x = -1 \pm \sqrt{3}$. Again the negative root is discarded, and we get $x = -1 + \sqrt{3}$. Thus $\sqrt{3} = 1 + x = 1 + {}^1\!/\!_1 + {}^1\!/\!_2 + {}^1\!/\!_1 + {}^1\!/\!_2 + {}^1\!/\!_1 + {}^1\!/\!_2 + \cdots$.

To simplify the notation we will write a bar over a block of terms in a continued fraction that repeat infinitely often, for example

$$\sqrt{2} = 1 + \overline{{}^1\!/\!_2} \qquad \text{and} \qquad \sqrt{3} = 1 + \overline{{}^1\!/\!_1 + {}^1\!/\!_2}$$

It is true in general that for every positive integer n that is not a square, the continued fraction for $\sqrt{n}$ has the form $a_0 + \overline{{}^1\!/\!_{a_1} + {}^1\!/\!_{a_2} + \cdots + {}^1\!/\!_{a_k}}$. The length of the period can be large, for example

$$\sqrt{46} = 6 + \overline{{}^1\!/\!_1 + {}^1\!/\!_3 + {}^1\!/\!_1 + {}^1\!/\!_1 + {}^1\!/\!_2 + {}^1\!/\!_6 + {}^1\!/\!_2 + {}^1\!/\!_1 + {}^1\!/\!_1 + {}^1\!/\!_3 + {}^1\!/\!_1 + {}^1\!/\!_{12}}$$

This example illustrates two other curious facts about the continued fraction for an irrational number $\sqrt{n}$:

(i) The last term of the period (12 in the example) is always twice the integer a_0 (the initial 6).

(ii) If the last term of the period is omitted, the preceding terms in the period form a palindrome, reading the same backwards as forwards.

We will see in Chapter 4 why these two properties have to be true.

It is natural to ask exactly which irrational numbers have continued fractions that are periodic, or at least *eventually* periodic, like for example

$${}^1\!/\!_2 + {}^1\!/\!_4 + \overline{{}^1\!/\!_3 + {}^1\!/\!_5 + {}^1\!/\!_7} = {}^1\!/\!_2 + {}^1\!/\!_4 + {}^1\!/\!_3 + {}^1\!/\!_5 + {}^1\!/\!_7 + {}^1\!/\!_3 + {}^1\!/\!_5 + {}^1\!/\!_7 + {}^1\!/\!_3 + {}^1\!/\!_5 + {}^1\!/\!_7 + \cdots$$

The answer is given by a theorem of Lagrange from around 1766:

Theorem 2.7 (Lagrange's Theorem). *The irrational numbers whose continued fractions are eventually periodic are exactly the numbers of the form $a + b\sqrt{n}$ where a and b are rational numbers, $b \neq 0$, and n is a positive integer that is not a square.*

These numbers $a + b\sqrt{n}$ are called *quadratic irrationals* because they are roots of quadratic equations with integer coefficients. The easier half of the theorem is the statement that the value of an eventually periodic infinite continued fraction is always a quadratic irrational. This can be proved by showing that the method we used for finding a quadratic equation satisfied by an eventually periodic continued fraction works in general. Rather than following this purely algebraic approach, however, we will develop a more geometric version of the procedure in the next chapter, so we will wait until then to give the argument that proves this half of Lagrange's Theorem. The more difficult half of the theorem is the assertion that the continued fraction expansion of every quadratic irrational is eventually periodic. It is not at all apparent from the examples of $\sqrt{2}$ and $\sqrt{3}$ why this should be true in general, but in Chapter 5 we will develop some theory that will make it clear.

What can be said about the continued fraction expansions of irrational numbers that are not quadratic, such as $\sqrt[3]{2}$, π, or e, the base for natural logarithms? It happens that e has a continued fraction whose terms have a very nice pattern, even though they are not periodic or eventually periodic:

$$e = 2 + \underbrace{{}^{1}\!\diagup_{1} + {}^{1}\!\diagup_{2} + {}^{1}\!\diagup_{1}} + \underbrace{{}^{1}\!\diagup_{1} + {}^{1}\!\diagup_{4} + {}^{1}\!\diagup_{1}} + \underbrace{{}^{1}\!\diagup_{1} + {}^{1}\!\diagup_{6} + {}^{1}\!\diagup_{1}} + \cdots$$

where the terms are grouped by threes with successive even numbers as middle denominators. Even simpler are the continued fractions for certain numbers built from e that have arithmetic progressions for their denominators:

$$\frac{e-1}{e+1} = {}^{1}\!\diagup_{2} + {}^{1}\!\diagup_{6} + {}^{1}\!\diagup_{10} + {}^{1}\!\diagup_{14} + \cdots$$

$$\frac{e^2-1}{e^2+1} = {}^{1}\!\diagup_{1} + {}^{1}\!\diagup_{3} + {}^{1}\!\diagup_{5} + {}^{1}\!\diagup_{7} + \cdots$$

The continued fractions for e and $(e-1)/(e+1)$ were discovered by Euler in 1737 while the formula for $(e^2-1)/(e^2+1)$ was found by Lambert in 1766 as a special case of a slightly more complicated formula for $(e^x-1)/(e^x+1)$.

For $\sqrt[3]{2}$ and π, however, the continued fractions have no known pattern. For π the continued fraction begins

$$\pi = 3 + {}^{1}\!\diagup_{7} + {}^{1}\!\diagup_{15} + {}^{1}\!\diagup_{1} + {}^{1}\!\diagup_{292} + \cdots$$

Here the first four convergents are 3, $22/7$, $333/106$, and $355/113$. We recognize $22/7$ as the familiar approximation $3\frac{1}{7}$ to π. The convergent $355/113$ is a particularly good approximation to π since its decimal expansion begins 3.14159282 whereas $\pi = 3.14159265\cdots$. It is no accident that the convergent $355/113$ obtained by truncating the continued fraction just before the 292 term gives a good approximation to π since it is a general fact that a convergent immediately preceding a large term in the continued fraction always gives an especially good approximation. This is because the next jump in the zigzag path in the Farey diagram will be rather small since it crosses a fan with a large number of triangles, and all succeeding jumps will of course be smaller still.

There are nice continued fractions for π if one allows numerators larger than 1, as in the following formula discovered by Euler:

$$\pi = 3 + {}^{1^2}\!\!\nearrow_{6} + {}^{3^2}\!\!\nearrow_{6} + {}^{5^2}\!\!\nearrow_{6} + {}^{7^2}\!\!\nearrow_{6} + \cdots$$

However, it is the continued fractions with numerator 1 that have the nicest properties, so we will not consider the more general sort in this book.

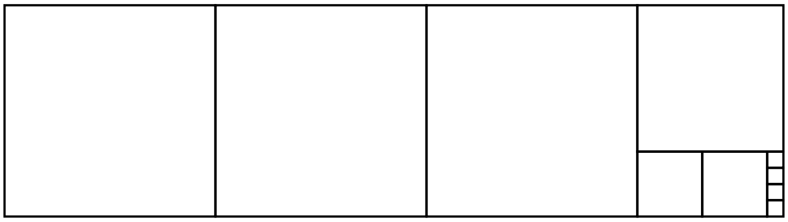
Exercises

1. (a) Compute the values of the continued fractions ${}^{1}\!\!\nearrow_{1} + {}^{1}\!\!\nearrow_{3} + {}^{1}\!\!\nearrow_{5} + {}^{1}\!\!\nearrow_{7}$ and ${}^{1}\!\!\nearrow_{1} + {}^{1}\!\!\nearrow_{1} + {}^{1}\!\!\nearrow_{1} + {}^{1}\!\!\nearrow_{1} + {}^{1}\!\!\nearrow_{1} + {}^{1}\!\!\nearrow_{2}$.
(b) Compute the continued fraction expansions of $19/44$ and $101/1020$.

2. (a) Compute the continued fraction for $38/83$ and display the steps of the Euclidean algorithm as a sequence of equations involving just integers.
(b) For the same number $38/83$ compute the associated strip of triangles (with large triangles subdivided into fans of smaller triangles), including the labeling of the vertices of all the triangles.
(c) Take the continued fraction ${}^{1}\!\!\nearrow_{a_1} + {}^{1}\!\!\nearrow_{a_2} + \cdots + {}^{1}\!\!\nearrow_{a_n}$ you got in part (a) and reverse the order of the numbers a_i to get a new continued fraction ${}^{1}\!\!\nearrow_{a_n} + {}^{1}\!\!\nearrow_{a_{n-1}} + \cdots + {}^{1}\!\!\nearrow_{a_1}$. Compute the value p/q of this continued fraction, and also compute the strip of triangles for this fraction p/q.

3. Let p_n/q_n be the value of the continued fraction ${}^{1}\!\!\nearrow_{a_1} + {}^{1}\!\!\nearrow_{a_2} + \cdots + {}^{1}\!\!\nearrow_{a_n}$ where each of the n terms a_i is equal to 2. For example, $p_1/q_1 = 1/2$ and $p_2/q_2 = {}^{1}\!\!\nearrow_{2} + {}^{1}\!\!\nearrow_{2} = 2/5$.
(a) Find equations expressing p_n and q_n in terms of p_{n-1} and q_{n-1}, and use these to write down the values of p_n/q_n for $n = 1, 2, 3, 4, 5, 6, 7$.
(b) Compute the strip of triangles for p_7/q_7.

4. (a) A rectangle whose sides have lengths 13 and 48 can be partitioned into squares in the following way:



Determine the lengths of the sides of all the squares, and relate the numbers of squares of each size to the continued fraction for $13/48$.

(b) Draw the analogous figure decomposing a rectangle of sides 19 and 42 into squares, and relate this to the continued fraction for $19/42$.

5. This exercise is intended to illustrate the proof of the first theorem in this chapter in the concrete case of the continued fraction ${}^1\!/_2 + {}^1\!/_3 + {}^1\!/_4 + {}^1\!/_5$.

(a) Write down the product $A_1A_2A_3A_4 = \begin{pmatrix} 0 & 1 \\ 1 & a_1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & a_2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & a_3 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & a_4 \end{pmatrix}$ associated to ${}^1\!/_2 + {}^1\!/_3 + {}^1\!/_4 + {}^1\!/_5$.

(b) Compute the four matrices A_1, A_1A_2, $A_1A_2A_3$, $A_1A_2A_3A_4$ and relate these to the edges of the zigzag path in the strip of triangles for ${}^1\!/_2 + {}^1\!/_3 + {}^1\!/_4 + {}^1\!/_5$.

(c) Compute the four matrices A_4, A_3A_4, $A_2A_3A_4$, $A_1A_2A_3A_4$ and relate these to the successive fractions that one gets when one computes the value of ${}^1\!/_2 + {}^1\!/_3 + {}^1\!/_4 + {}^1\!/_5$, namely ${}^1\!/_5$, ${}^1\!/_4 + {}^1\!/_5$, ${}^1\!/_3 + {}^1\!/_4 + {}^1\!/_5$, and ${}^1\!/_2 + {}^1\!/_3 + {}^1\!/_4 + {}^1\!/_5$.

6. (a) Find all integer solutions of the equations $40x + 89y = 1$ and $40x + 89y = 5$.

(b) Find another equation $ax + by = 1$ with integer coefficients a and b that has an integer solution in common with $40x + 89y = 1$. [Hint: use the Farey diagram.]

7. There is a close connection between the Diophantine equation $ax+by = n$ and the congruence $ax \equiv n \bmod b$, where the symbol $\equiv$ means "is congruent to". Namely, if one has a solution (x, y) to $ax + by = n$ then $ax \equiv n \bmod b$, and conversely, if one has a number x such that $ax \equiv n \bmod b$ then this means that $ax - n$ is a multiple of b, say k times b, so $ax - n = kb$ or equivalently $ax - kb = n$ so one has a solution of $ax + by = n$ with $y = -k$.

Using this viewpoint, find all integers x satisfying the congruence $31x \equiv 1 \bmod 71$, and then do the same for the congruence $31x \equiv 10 \bmod 71$. Are the solutions unique mod 71, i.e., unique up to adding multiples of 71?

8. Compute the values of the following infinite continued fractions:

(a) $\overline{{}^1\!/_4}$

(b) $\overline{{}^1\!/_k}$ for an arbitrary positive integer k.

(c) $\overline{{}^1\!/_2 + {}^1\!/_3}$ and ${}^1\!/_1 + \overline{{}^1\!/_2 + {}^1\!/_3}$

(d) $\overline{{}^1\!/_1 + {}^1\!/_2 + {}^1\!/_1 + {}^1\!/_6}$ and ${}^1\!/_1 + {}^1\!/_4 + \overline{{}^1\!/_1 + {}^1\!/_2 + {}^1\!/_1 + {}^1\!/_6}$

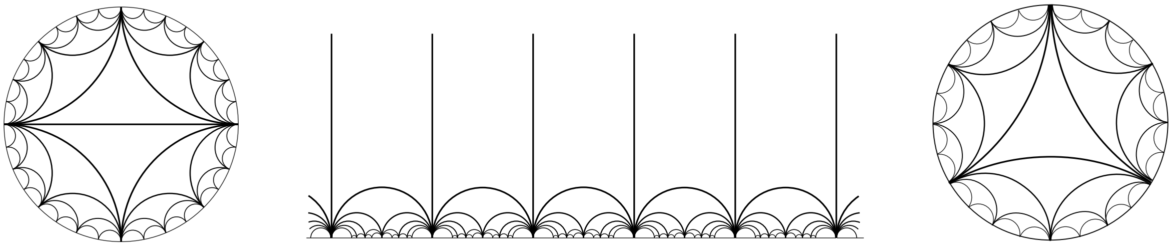
(e) $\overline{{}^1\!/_2 + {}^1\!/_3 + {}^1\!/_5}$

9. Compute the continued fractions for $\sqrt{5}$ and $\sqrt{23}$.

10. Compute the continued fractions for $\sqrt{n^2+1}$ and $\sqrt{n^2+n}$ where n is an arbitrary positive integer.

Chapter 3. Linear Fractional Transformations

One thing one notices about the various versions of the Farey diagram is their symmetry. For the circular Farey diagram the symmetries are the reflections across the horizontal and vertical axes and the 180 degree rotation about the center. For the standard Farey diagram in the upper halfplane there are symmetries that translate the diagram by any integer distance to the left or the right, as well as reflections across certain vertical lines, the vertical lines through an integer or half-integer point on the x-axis. The Farey diagram could also be drawn to have 120 degree rotational symmetry and three reflectional symmetries.



Our purpose in this chapter is to study all possible symmetries of the Farey diagram, where we interpret the word "symmetry" in a broader sense than the familiar meaning from Euclidean geometry. For our purposes, symmetries will be invertible transformations that take vertices to vertices, edges to edges, and triangles to triangles. There are simple algebraic formulas for these more general symmetries, and these formulas lead to effective means of calculation. One of the applications will be to computing the values of periodic or eventually periodic continued fractions.

From linear algebra one is familiar with the way in which 2×2 matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ correspond to linear transformations of the plane $\mathbb{R}^2$, transformations of the form

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

In our situation we are going to restrict $a,\ b,\ c,\ d,\ x,\ y$ to be integers. Then by associating to a pair (x, y) the fraction x/y one obtains a closely related transformation

$$T\left(\frac{x}{y}\right) = \frac{ax + by}{cx + dy} = \frac{a(\frac{x}{y}) + b}{c(\frac{x}{y}) + d}$$

If we set $z = x/y$ then T can also be written in the form

$$T(z) = \frac{az + b}{cz + d}$$

Such a transformation is called a *linear fractional transformation* since it is defined by a fraction whose numerator and denominator are linear functions.

In the formula $T(x/y) = (ax+by)/(cx+dy)$ there is no problem with allowing $x/y = \pm 1/0$ just by setting $(x, y) = (\pm 1, 0)$, and the result is that $T(\pm 1/0) = a/c$. The value $T(x/y) = (ax + by)/(cx + dy)$ can also be $\pm 1/0$, when $(x, y) = (d, -c)$ and the matrix has determinant $ad - bc = \pm 1$. This means that T defines a function from vertices of the Farey diagram to vertices of the Farey diagram. We would like T to take edges of the diagram to edges of the diagram, and the following result gives a condition for this to happen.

Proposition 3.1. *If the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ has determinant ± 1 then the associated linear fractional transformation T takes each pair of vertices in the Farey diagram that lie at the ends of an edge of the diagram to another such pair of vertices.*

Proof: We showed in Chapter 1 that two vertices labeled p/q and r/s are joined by an edge in the diagram exactly when $ps - qr = \pm 1$, or in other words when the matrix $\left(\begin{smallmatrix} p & r \\ q & s \end{smallmatrix}\right)$ has determinant ± 1. The two columns of the product matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} p & r \\ q & s \end{smallmatrix}\right)$ correspond to the two vertices $T(p/q)$ and $T(r/s)$, by the definition of matrix multiplication:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} p & r \\ q & s \end{pmatrix} = \begin{pmatrix} ap + bq & ar + bs \\ cp + dq & cr + ds \end{pmatrix}$$

The proposition can then be restated as saying that if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} p & r \\ q & s \end{smallmatrix}\right)$ each have determinant ± 1 then so does their product $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} p & r \\ q & s \end{smallmatrix}\right)$. But it is a general fact about determinants that the determinant of a product is the product of the determinants. (This is easy to prove by a direct calculation in the case of 2×2 matrices.) So the product of two matrices of determinant ± 1 has determinant ± 1. □

As notation, we will use $LF(\mathbb{Z})$ to denote the set of all linear fractional transformations $T(x/y) = (ax + by)/(cx + dy)$ with coefficients a, b, c, d in $\mathbb{Z}$ such that the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ has determinant ± 1. (Here $\mathbb{Z}$ is the set of all integers.)

Changing the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to its negative $\left(\begin{smallmatrix} -a & -b \\ -c & -d \end{smallmatrix}\right)$ produces the same linear fractional transformation since $(-ax - by)/(-cx - dy) = (ax + by)/(cx + dy)$. This is in fact the only way that different matrices can give the same linear fractional transformation T, as we will see later in this chapter. Note that changing $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to its negative $\left(\begin{smallmatrix} -a & -b \\ -c & -d \end{smallmatrix}\right)$ does not change the determinant. Thus each linear fractional transformation in $LF(\mathbb{Z})$ has a well-defined determinant, either $+1$ or -1. Later in this chapter we will also see how the distinction between determinant $+1$ and determinant -1 has a geometric interpretation in terms of orientations.

A useful fact about $LF(\mathbb{Z})$ is that each transformation T in $LF(\mathbb{Z})$ has an inverse T^{-1} in $LF(\mathbb{Z})$ because the inverse of a 2×2 matrix is given by the formula

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

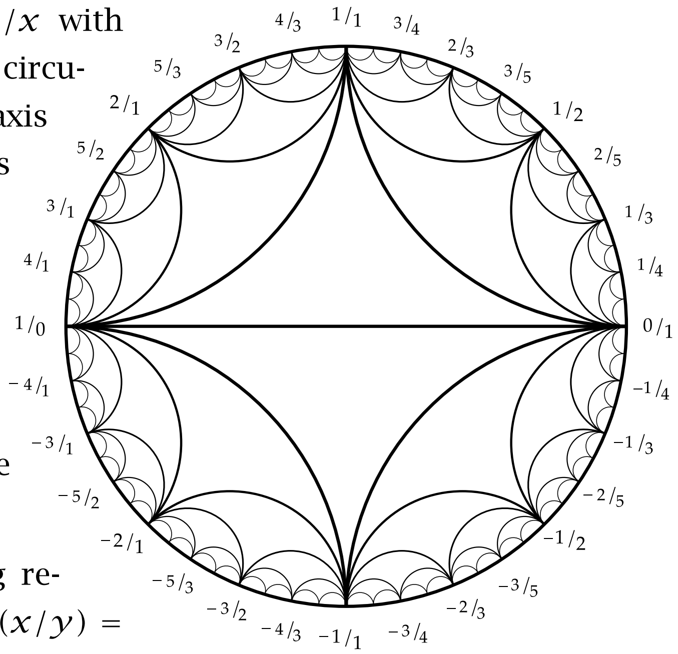
Thus if a, b, c, d are integers with $ad - bc = \pm 1$ then the inverse matrix also has integer entries and determinant ± 1. The factor $\frac{1}{ad-bc}$ is ± 1 so it can be ignored since the matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $-\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ determine the same linear fractional transformation, as we observed in the preceding paragraph.

The preceding proposition says that each linear fractional transformation T in $LF(\mathbb{Z})$ not only sends vertices of the Farey diagram to vertices, but also edges to edges. It follows that T must take triangles in the diagram to triangles in the diagram, since triangles correspond to sets of three vertices, each pair of which forms the endpoints of an edge. Since each transformation T in $LF(\mathbb{Z})$ has an inverse in $LF(\mathbb{Z})$, this implies that T gives a one-to-one (injective) and onto (surjective) transformation of vertices, and also of edges and triangles. For example, if two edges e_1 and e_2 have the same image $T(e_1) = T(e_2)$ then we must have $T^{-1}(T(e_1)) = T^{-1}(T(e_2))$ or in other words $e_1 = e_2$, so T cannot send two different edges to the same edge, which means it is one-to-one on edges. Also, every edge e_1 is the image $T(e_2)$ of some edge e_2 since we can write $e_1 = T(T^{-1}(e_1))$ and let $e_2 = T^{-1}(e_1)$. The same reasoning works with vertices and triangles as well as edges.

A useful property of linear fractional transformations that we will use repeatedly is that the way an element of $LF(\mathbb{Z})$ acts on the Farey diagram is uniquely determined by where a single triangle is sent. This is because once one knows where one triangle goes, this uniquely determines where the three adjacent triangles go, and this in turn determines where the six new triangles adjacent to these three go, and so on.

Seven Types of Transformations

We will now give examples illustrating seven different ways that elements of $LF(\mathbb{Z})$ can act on the Farey diagram.



(1) The transformation $T(x/y) = y/x$ with matrix $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ gives a reflection of the circular Farey diagram across its vertical axis of symmetry. This is a reflection across a line perpendicular to an edge of the diagram.

(2) The reflection across the horizontal axis of symmetry is the element $T(x/y) = -x/y$ with matrix $\left(\begin{smallmatrix}-1&0\\0&1\end{smallmatrix}\right)$. This is a reflection across an edge of the diagram.

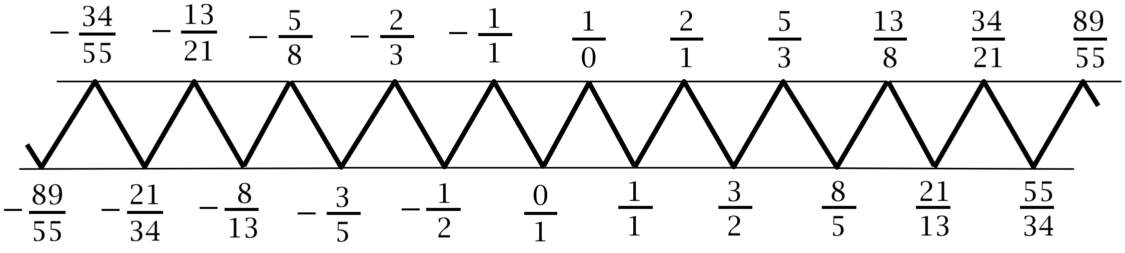
(3) If we compose the two preceding reflections we get the transformation $T(x/y) = -y/x$ with matrix $\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right)$. This rotates the Farey diagram 180 degrees about its center, interchanging $1/0$ and $0/1$ and also interchanging $1/1$ and $-1/1$. Thus it rotates the diagram 180 degrees about the centerpoint of an edge.

(4) Consider $T(x/y) = y/(y-x)$ corresponding to the matrix $\left(\begin{smallmatrix}0&1\\-1&1\end{smallmatrix}\right)$. This has the effect of "rotating" the triangle $\langle 1/0, 0/1, 1/1\rangle$ about its centerpoint, taking $1/0$ to

$0/1$, $0/1$ to $1/1$ and $1/1$ back to $1/0$. The whole Farey diagram is then “rotated” about the same point.

(5) Next let $T(x/y) = x/(x+y)$, corresponding to the matrix $\begin{pmatrix}1&0\\1&1\end{pmatrix}$. In particular $T(0/1) = 0/1$, so $0/1$ is a *fixed point* of T, a point satisfying $T(z) = z$. Also we have $T(1/0) = 1/1$ and more generally $T(1/n) = 1/(n+1)$. Thus the triangle $\langle 0/1, 1/0, 1/1\rangle$ is taken to the triangle $\langle 0/1, 1/1, 1/2\rangle$. This implies that T is a “rotation” of the Farey diagram about the vertex $0/1$, taking each triangle with $0/1$ as a vertex to the next triangle in the clockwise direction about this vertex.

(6) A different sort of behavior is exhibited by $T(x/y) = (2x+y)/(x+y)$ corresponding to $\begin{pmatrix}2&1\\1&1\end{pmatrix}$. To visualize T as a transformation of the Farey diagram let us look at the infinite strip



We claim that T translates the whole strip one unit to the right. To see this, notice first that since T takes $1/0$ to $2/1$, $0/1$ to $1/1$, and $1/1$ to $3/2$, it takes the triangle $\langle 1/0, 0/1, 1/1\rangle$ to the triangle $\langle 2/1, 1/1, 3/2\rangle$. This implies that T takes the triangle just to the right of $\langle 1/0, 0/1, 1/1\rangle$ to the triangle just to the right of $\langle 2/1, 1/1, 3/2\rangle$, and similarly each successive triangle is translated one unit to the right. The same argument shows that each successive triangle to the left of the original one is also translated one unit to the right. Thus the whole strip is translated one unit to the right.

(7) Using the same figure as in the preceding example, consider the transformation $T(x/y) = (x+y)/x$ corresponding to the matrix $\begin{pmatrix}1&1\\1&0\end{pmatrix}$. This sends the triangle $\langle 1/0, 0/1, 1/1\rangle$ to $\langle 1/1, 1/0, 2/1\rangle$ which is the next triangle to the right in the infinite strip. Geometrically, T translates the first triangle half a unit to the right and reflects it across the horizontal axis of the strip. It follows that the whole strip is translated half a unit to the right and reflected across the horizontal axis. Such a motion is sometimes referred to as a *glide-reflection.* Notice that performing this motion twice in succession yields a translation of the strip one unit to the right, the transformation in the preceding example.

Thus we have seven types of symmetries of the Farey diagram: reflections across an edge or a line perpendicular to an edge; rotations about the centerpoint of an edge or a triangle, or about a vertex; and translations and glide-reflections of periodic infinite strips. (Not all periodic strips have glide-reflection symmetries.) It is a true fact, though we won’t prove it here, that every element of $LF(\mathbb{Z})$ acts on the Farey diagram in one of these seven ways, except for the identity transformation $T(x/y) = x/y$ of course.

Specifying Where a Triangle Goes

As we observed earlier, the action of an element of $LF(\mathbb{Z})$ on the Farey diagram is completely determined by where it sends a single triangle. Now we will see that there always exists an element of $LF(\mathbb{Z})$ sending any triangle to any other triangle, and in fact, one can do this specifying where each individual vertex of the triangle goes.

As an example, suppose we wish to find an element T of $LF(\mathbb{Z})$ that takes the triangle $\langle 2/5, 1/3, 3/8\rangle$ to the triangle $\langle 5/8, 7/11, 2/3\rangle$, preserving the indicated ordering of the vertices, so $T(2/5) = 5/8$, $T(1/3) = 7/11$, and $T(3/8) = 2/3$. For this problem to even make sense we might want to check first that these really are triangles in the Farey diagram. In the first case, $\langle 2/5, 1/3\rangle$ is an edge since the matrix $\left(\begin{smallmatrix} 2 & 1 \\ 5 & 3 \end{smallmatrix}\right)$ has determinant 1, and there is a triangle joining this edge to $3/8$ since $3/8$ is the mediant of $2/5$ and $1/3$. For the other triangle, the determinant of $\left(\begin{smallmatrix} 5 & 2 \\ 8 & 3 \end{smallmatrix}\right)$ is -1 and the mediant of $5/8$ and $2/3$ is $7/11$.

As a first step toward constructing the desired transformation T we will do something slightly weaker: We construct a transformation T taking the edge $\langle 2/5, 1/3\rangle$ to the edge $\langle 5/8, 7/11\rangle$. This is rather easy if we first notice the general fact that the transformation $T(x/y) = (ax + by)/(cx + dy)$ with matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ takes $1/0$ to a/c and $0/1$ to b/d. Thus the transformation T_1 with matrix $\left(\begin{smallmatrix} 2 & 1 \\ 5 & 3 \end{smallmatrix}\right)$ takes $\langle 1/0, 0/1\rangle$ to $\langle 2/5, 1/3\rangle$, and the transformation T_2 with matrix $\left(\begin{smallmatrix} 5 & 7 \\ 8 & 11 \end{smallmatrix}\right)$ takes $\langle 1/0, 0/1\rangle$ to $\langle 5/8, 7/11\rangle$. Then the product

$$T_2T_1^{-1} = \begin{pmatrix} 5 & 7 \\ 8 & 11 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 5 & 3 \end{pmatrix}^{-1}$$

takes $\langle 2/5, 1/3\rangle$ first to $\langle 1/0, 0/1\rangle$ and then to $\langle 5/8, 7/11\rangle$. Doing the calculation, we get

$$\begin{pmatrix} 5 & 7 \\ 8 & 11 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 5 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 5 & 7 \\ 8 & 11 \end{pmatrix}\begin{pmatrix} 3 & -1 \\ -5 & 2 \end{pmatrix} = \begin{pmatrix} -20 & 9 \\ -31 & 14 \end{pmatrix}$$

This takes the edge $\langle 2/5, 1/3\rangle$ to the edge $\langle 5/8, 7/11\rangle$, but does it do the right thing on the third vertex of the triangle $\langle 2/5, 1/3, 3/8\rangle$, taking it to the third vertex of $\langle 5/8, 7/11, 2/3\rangle$? This is not automatic since there are always two triangles containing a given edge, and in this case the other triangle having $\langle 5/8, 7/11\rangle$ as an edge is $\langle 5/8, 7/11, 12/19\rangle$ since $12/19$ is the mediant of $5/8$ and $7/11$. In fact, if we compute what our T does to $3/8$ we get

$$\begin{pmatrix} -20 & 9 \\ -31 & 14 \end{pmatrix}\begin{pmatrix} 3 \\ 8 \end{pmatrix} = \begin{pmatrix} 12 \\ 19 \end{pmatrix}$$

so we don't have the right T yet. To fix the problem, notice that we have a little flexibility in the choice of a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ taking $1/0$ to a/c and $0/1$ to b/d since we can multiply either column by -1 without affecting the fractions a/b and c/d. It doesn't matter which column we multiply by -1 since multiplying both columns by -1 multiplies the whole matrix by -1 which doesn't change the associated element of $LF(\mathbb{Z})$, as noted earlier. In the case at hand, suppose we change the sign of the first column of $\left(\begin{smallmatrix} 5 & 7 \\ 8 & 11 \end{smallmatrix}\right)$. Then we get

$$\begin{pmatrix} -5 & 7 \\ -8 & 11 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 5 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} -5 & 7 \\ -8 & 11 \end{pmatrix}\begin{pmatrix} 3 & -1 \\ -5 & 2 \end{pmatrix} = \begin{pmatrix} -50 & 19 \\ -79 & 30 \end{pmatrix}$$

This fixes the problem since

$$\begin{pmatrix} -50 & 19 \\ -79 & 30 \end{pmatrix}\begin{pmatrix} 3 \\ 8 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$$

Here is a general statement summarizing what we saw in this one example:

Proposition 3.2. *(a) For any two triangles $\langle p/q, r/s, t/u\rangle$ and $\langle p'/q', r'/s', t'/u'\rangle$ in the Farey diagram there is a unique element T in $LF(\mathbb{Z})$ taking the first triangle to the second triangle preserving the ordering of the vertices, so $T(p/q) = p'/q'$, $T(r/s) = r'/s'$, and $T(t/u) = t'/u'$.*
(b) The matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ representing a given transformation T in $LF(\mathbb{Z})$ is unique except for replacing it by $\left(\begin{smallmatrix} -a & -b \\ -c & -d \end{smallmatrix}\right)$.

Proof: As we saw in the example above, there is a composition $T_2T_1^{-1}$ taking the edge $\langle p/q, r/s\rangle$ to $\langle p'/q', r'/s'\rangle$, where T_1 has matrix $\left(\begin{smallmatrix} p & r \\ q & s \end{smallmatrix}\right)$ and T_2 has matrix $\left(\begin{smallmatrix} p' & r' \\ q' & s' \end{smallmatrix}\right)$. If this composition $T_2T_1^{-1}$ does not take t/u to t'/u' we modify T_2 by changing the sign of one of its columns, say the first column. Thus we change $\left(\begin{smallmatrix} p' & r' \\ q' & s' \end{smallmatrix}\right)$ to $\left(\begin{smallmatrix} -p' & r' \\ -q' & s' \end{smallmatrix}\right)$, which equals the product $\left(\begin{smallmatrix} p' & r' \\ q' & s' \end{smallmatrix}\right)\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. The matrix $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ corresponds to the transformation $R(x/y) = -x/y$ reflecting the Farey diagram across the edge $\langle 1/0, 0/1\rangle$. Thus we are replacing $T_2T_1^{-1}$ by $T_2RT_1^{-1}$, inserting a reflection that interchanges the two triangles containing the edge $\langle 1/0, 0/1\rangle$. By inserting R we change where the composition $T_2T_1^{-1}$ sends the third vertex t/u of the triangle $\langle p/q, r/s, t/u\rangle$, so we can guarantee that t/u is taken to t'/u'. This proves part (a).

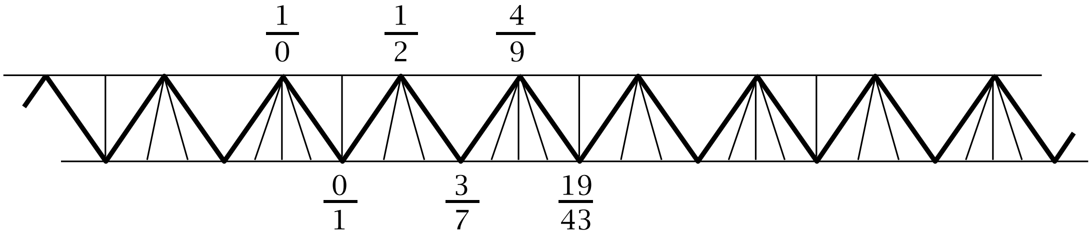
For part (b), note first that the transformation T determines the values $T(1/0) = a/c$ and $T(0/1) = b/d$. The fractions a/c and b/d are in lowest terms (because $ad - bc = \pm 1$) so this means that we know the two columns of the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ up to multiplying either or both columns by -1. We need to check that changing the sign of one column without changing the sign of the other column gives a different transformation. It doesn't matter which column we change since $\left(\begin{smallmatrix} -a & b \\ -c & d \end{smallmatrix}\right) = -\left(\begin{smallmatrix} a & -b \\ c & -d \end{smallmatrix}\right)$. As we saw in part (a), changing the sign in the first column amounts to replacing T by the composition TR, but this is a different transformation from T since it has a different effect on the triangles containing the edge $\langle 1/0, 0/1\rangle$. □

Continued Fractions Again

Linear fractional transformations can be used to compute the values of periodic or eventually periodic continued fractions, and to see that these values are always quadratic irrational numbers. To illustrate this, consider the periodic continued fraction

$$\overline{{}^{1}\!\diagup\!_{2}+{}^{1}\!\diagup\!_{3}+{}^{1}\!\diagup\!_{1}+{}^{1}\!\diagup\!_{4}}$$

The associated periodic strip in the Farey diagram is the following:



We would like to compute the element T of $LF(\mathbb{Z})$ that gives the rightward translation of this strip that exhibits the periodicity. A first guess is the T with matrix $\left(\begin{smallmatrix}4&19\\9&43\end{smallmatrix}\right)$ since this sends $\langle 1/0, 0/1\rangle$ to $\langle 4/9, 19/43\rangle$. This is actually the correct T since it sends the vertex $1/1$ just to the right of $1/0$, which is the mediant of $1/0$ and $0/1$, to the vertex $(4+19)/(9+43)$ just to the right of $4/9$, which is the mediant of $4/9$ and $19/43$. This is a general fact since $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)=\left(\begin{smallmatrix}a+b\\c+d\end{smallmatrix}\right)$.

The sequence of fractions labeling the vertices along the zigzag path in the strip moving toward the right are the convergents to $\overline{{}^{1}\!\diagup\!_{2}+{}^{1}\!\diagup\!_{3}+{}^{1}\!\diagup\!_{1}+{}^{1}\!\diagup\!_{4}}$. Call these convergents $z_1, z_2, \cdots$ and their limit z. When we apply the translation T we are taking each convergent to a later convergent in the sequence, so both the sequence $\{z_n\}$ and the sequence $\{T(z_n)\}$ converge to z. Thus we have

$$T(z) = T(\lim z_n) = \lim T(z_n) = z$$

where the middle equality uses the fact that T is continuous. (Note that a linear fractional transformation $T(z)=\frac{az+b}{cz+d}$ is defined for real values of z, not just rational values $z = x/y$, when $T(x/y) = (ax+by)/(cx+dy) = (a\frac{x}{y}+b)/(c\frac{x}{y}+d)$.)

In summary, what we have just argued is that the value z of the periodic continued fraction satisfies the equation $T(z) = z$, or in other words, $\frac{4z+19}{9z+43} = z$. This can be rewritten as $4z + 19 = 9z^2 + 43z$, which simplifies to $9z^2 + 39z - 19 = 0$. Computing the roots of this quadratic equation, we get

$$z = \frac{-39 \pm \sqrt{39^2 + 4\cdot 9\cdot 19}}{18} = \frac{-39 \pm 3\sqrt{13^2 + 4\cdot 19}}{18} = \frac{-13 \pm \sqrt{245}}{6} = \frac{-13 \pm 7\sqrt{5}}{6}$$

The positive root is the one that the right half of the infinite strip converges to, so we have

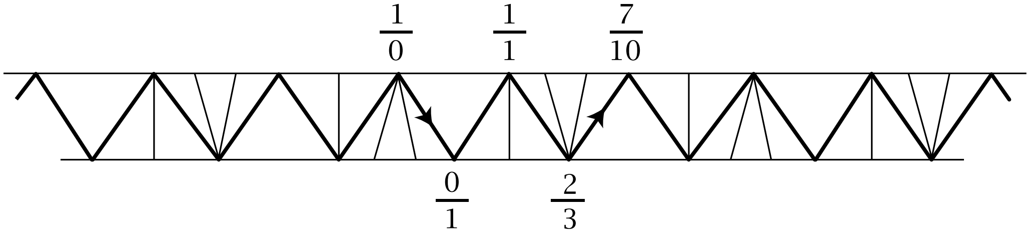
$$\frac{-13+7\sqrt{5}}{6} = \overline{{}^{1}\!\diagup\!_{2}+{}^{1}\!\diagup\!_{3}+{}^{1}\!\diagup\!_{1}+{}^{1}\!\diagup\!_{4}}$$

Incidentally, the other root $(-13 - 7\sqrt{5})/6$ has an interpretation in terms of the diagram as well: It is the limit of the numbers labeling the vertices of the zigzag path moving off to the left rather than to the right. This follows by the same sort of argument as above.

If a periodic continued fraction has period of odd length, the transformation giving the periodicity is a glide-reflection of the periodic strip rather than a translation. As an example, consider

$$\overline{{}^{1}\!\diagup\!\!\!\nearrow_{1} + {}^{1}\!\diagup\!\!\!\nearrow_{2} + {}^{1}\!\diagup\!\!\!\nearrow_{3}}$$

Here the periodic strip is



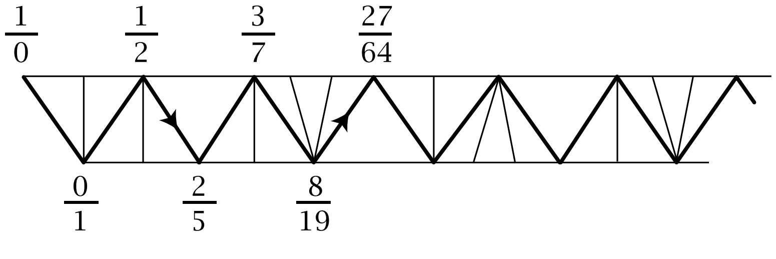
The transformation T with matrix $\begin{pmatrix} 2 & 7 \\ 3 & 10 \end{pmatrix}$ takes $\langle 1/0, 0/1 \rangle$ to $\langle 2/3, 7/10 \rangle$ and the mediant $1/1$ of $1/0$ and $0/1$ to the mediant $9/13$ of $2/3$ and $7/10$ so this transformation is a glide-reflection of the strip. The equation $T(z) = z$ becomes $\frac{2z+7}{3z+10} = z$ which simplifies to $3z^2 + 8z - 7 = 0$ with roots $(-4 \pm \sqrt{37})/3$. The positive root gives

$$\frac{-4 + \sqrt{37}}{3} = \overline{{}^{1}\!\diagup\!\!\!\nearrow_{1} + {}^{1}\!\diagup\!\!\!\nearrow_{2} + {}^{1}\!\diagup\!\!\!\nearrow_{3}}$$

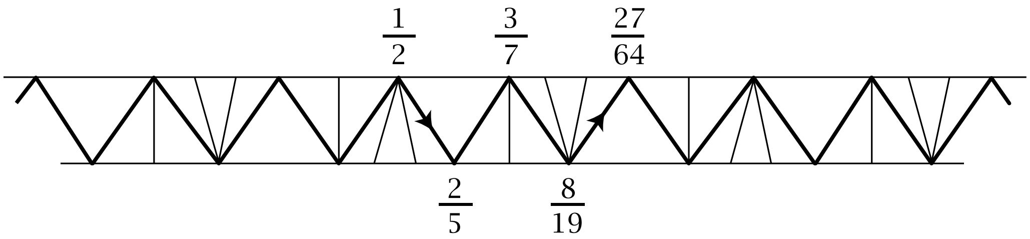
Continued fractions that are only eventually periodic can be treated in a similar fashion. For example, consider

$${}^{1}\!\diagup\!\!\!\nearrow_{2} + {}^{1}\!\diagup\!\!\!\nearrow_{2} + \overline{{}^{1}\!\diagup\!\!\!\nearrow_{1} + {}^{1}\!\diagup\!\!\!\nearrow_{2} + {}^{1}\!\diagup\!\!\!\nearrow_{3}}$$

The corresponding infinite strip is



In this case if we discard the triangles corresponding to the initial nonperiodic part of the continued fraction, ${}^{1}\!\diagup\!\!\!\nearrow_{2} + {}^{1}\!\diagup\!\!\!\nearrow_{2}$, and then extend the remaining periodic part in both directions, we obtain a periodic strip that is carried to itself by the glide-reflection T taking $\langle 1/2, 2/5 \rangle$ to $\langle 8/19, 27/64 \rangle$:



We can compute T as the composition $\langle 1/2, 2/5\rangle \to \langle 1/0, 0/1\rangle \to \langle 8/19, 27/64\rangle$ corresponding to the product

$$\begin{pmatrix} 8 & 27 \\ 19 & 64 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}^{-1} = \begin{pmatrix} 8 & 27 \\ 19 & 64 \end{pmatrix}\begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} -14 & 11 \\ -33 & 26 \end{pmatrix}$$

Since this transformation takes $3/7$ to the mediant $(8+27)/(19+64)$, it is the glide-reflection we want. Now we solve $T(z) = z$. This means $\frac{-14z+11}{-33z+26} = z$, which reduces to the equation $33z^2 - 40z + 11 = 0$ with roots $z = (20 \pm \sqrt{37})/33$. Both roots are positive, and we want the smaller one, $(20 - \sqrt{37})/33$, because along the top edge of the strip the numbers decrease as we move to the right, approaching the smaller root, and they increase as we move to the left, approaching the larger root. Thus we have

$$(20 - \sqrt{37})/33 = {}^1\!/_{2} + {}^1\!/_{2} + \overline{{}^1\!/_{1} + {}^1\!/_{2} + {}^1\!/_{3}}$$

Notice that $\sqrt{37}$ occurs in both this example and the preceding one where we computed the value of $\overline{{}^1\!/_{1} + {}^1\!/_{2} + {}^1\!/_{3}}$. This is not just an accident. It had to happen because to get from $\overline{{}^1\!/_{1} + {}^1\!/_{2} + {}^1\!/_{3}}$ to ${}^1\!/_{2} + {}^1\!/_{2} + \overline{{}^1\!/_{1} + {}^1\!/_{2} + {}^1\!/_{3}}$ one adds 2 and inverts, then adds 2 and inverts again, and each of these operations of adding an integer or taking the reciprocal takes place within the set $\mathbb{Q}(\sqrt{37})$ of all numbers of the form $a + b\sqrt{37}$ with a and b rational. More generally, this argument shows that any eventually periodic continued fraction whose periodic part is $\overline{{}^1\!/_{1} + {}^1\!/_{2} + {}^1\!/_{3}}$ has as its value some number in $\mathbb{Q}(\sqrt{37})$. However, not all irrational numbers in $\mathbb{Q}(\sqrt{37})$ have eventually periodic continued fractions with periodic part $\overline{{}^1\!/_{1} + {}^1\!/_{2} + {}^1\!/_{3}}$. For example, the continued fraction for $\sqrt{37}$ itself is $6 + \overline{{}^1\!/_{12}}$, with a different periodic part. (Check this by computing the value of this continued fraction.)

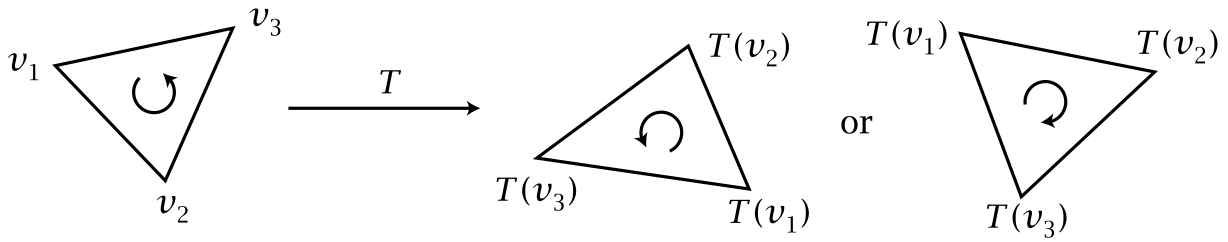
One Half of Lagrange's Theorem

The procedure we have used in these examples works in general for any irrational number z whose continued fraction is eventually periodic. From the periodic part of the continued fraction one constructs a periodic infinite strip in the Farey diagram, where the periodicity is given by a linear fractional transformation $T(z) = \frac{az+b}{cz+d}$ with integer coefficients, with T either a translation or a glide-reflection of the strip. As we argued in the first example, the number z satisfies the equation $T(z) = z$. This becomes the quadratic equation $az + b = cz^2 + dz$ with integer coefficients, or in simpler form, $cz^2 + (d-a)z - b = 0$. By the quadratic formula, the roots of this equation have the form $A + B\sqrt{n}$ for some rational numbers A and B and some integer n. We know that the real number z is a root of the equation so n can't be negative, and it can't be a square since z is irrational.

Thus we have an argument that proves one half of Lagrange's Theorem, the statement that a number whose continued fraction is periodic or eventually periodic is a quadratic irrational. There is one technical point that should be addressed, however. Could the leading coefficient c in the quadratic equation $cz^2 + (d - a)z - b = 0$ be zero? If this were the case then we couldn't apply the quadratic formula to solve for z, so we need to show that c cannot be zero. We do this in the following way. If c were zero the equation would become the linear equation $(d - a)z - b = 0$. If the coefficient of z in this equation is nonzero, we have only one root, $z = b/(d - a)$, a rational number contrary to the fact that z is irrational since its continued fraction is infinite. Thus we are left with the possibility that $c = 0$ and $a = d$, so the equation for z reduces to the equation $b = 0$. Then the transformation T would have the form $T(z) = \frac{az}{a} = z$ so it would be the identity transformation. However we know it is a genuine translation or a glide-reflection, so it is not the identity. We conclude from all this that c cannot be zero, and the technical point is taken care of.

Orientations

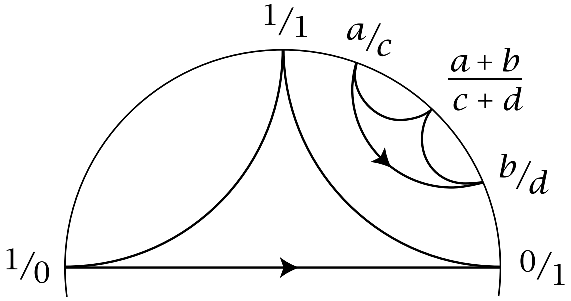
Elements of $LF(\mathbb{Z})$ are represented by integer matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of determinant ± 1. The distinction between determinant $+1$ and -1 has a very nice geometric interpretation in terms of orientations, which can be described in terms of triangles. A triangle in the Farey diagram can be oriented by choosing either the clockwise or counterclockwise ordering of its three vertices. An element T of $LF(\mathbb{Z})$ takes each triangle to another triangle in a way that either preserves the two possible orientations or reverses them.



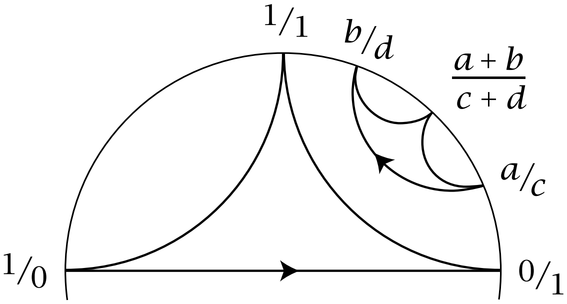
For example, among the seven types of transformations we looked at earlier, only reflections and glide-reflections reverse the orientations of triangles. Note that if a transformation T preserves the orientation of one triangle, it has to preserve the orientation of the three adjacent triangles, and then of the triangles adjacent to these, and so on for all the triangles. Similarly, if the orientation of one triangle is reversed by T, then the orientations of all triangles are reversed.

Proposition 3.3. *A transformation $T(x/y) = (ax + by)/(cx + dy)$ in $LF(\mathbb{Z})$ preserves orientations of triangles in the Farey diagram when the determinant $ad - bc$ is $+1$ and reverses the orientations when the determinant is -1.*

Proof: We will first prove a special case and then deduce the general case from the special case. The special case is that a, b, c, d are all positive or zero. The transformation T with matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ takes the edge $\langle 1/0, 0/1 \rangle$ in the circular Farey diagram to the edge $\langle a/c, b/d \rangle$, and if a, b, c, d are all positive or zero, this edge lies in the upper half of the diagram. Since $T(1/1) = (a+b)/(c+d)$, the triangle $\langle 1/0, 0/1, 1/1 \rangle$ is taken to the triangle $\langle a/c, b/d, (a+b)/(c+d) \rangle$ whose third vertex $(a+b)/(c+d)$ lies above the edge $\langle a/c, b/d \rangle$, by the way the Farey diagram was constructed using mediants, since we assume a, b, c, d are positive or zero. We know that the edge $\langle a/c, b/d \rangle$ is oriented to the right if $ad - bc = +1$ and to the left if $ad - bc = -1$. This means that T preserves the orientation of the triangle $\langle 1/0, 0/1, 1/1 \rangle$ if the determinant is $+1$ and reverses the orientation if the determinant is -1.



$ad - bc = +1$



$ad - bc = -1$

This proves the special case.

The general case can be broken into two subcases, according to whether the edge $\langle a/c, b/d \rangle$ lies in the upper or the lower half of the diagram. If $\langle a/c, b/d \rangle$ lies in the upper half of the diagram, then after multiplying one or both columns of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ by -1 if necessary, we will be in the special case already considered. Multiplying both columns by -1 doesn't affect T. Multiplying one column by -1 corresponds to first reflecting across the edge $\langle 1/0, 0/1 \rangle$, as we have seen earlier. Modifying T in this way changes the sign of the determinant and it also changes whether T preserves or reverses orientation, so the special case already proved implies the case that T takes $\langle 1/0, 0/1 \rangle$ to an edge in the upper half of the diagram.

The remaining possibility is that T takes the edge $\langle 1/0, 0/1 \rangle$ to an edge in the lower half of the diagram. In this case if we follow T by reflection across the edge $\langle 1/0, 0/1 \rangle$ we get a new transformation taking $\langle 1/0, 0/1 \rangle$ to an edge in the upper half of the diagram. As before, composing with this reflection changes T from orientation-preserving to orientation-reversing and vice versa, and it also changes the sign of the determinant since the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is changed to $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -a & -b \\ c & d \end{pmatrix}$, so this case follows from the previous case. □

As we noted in Chapter 2, to determine whether a matrix representing an element of $LF(\mathbb{Z})$ has determinant $+1$ or -1 it suffices to compute just the last digit of the determinant, and this can be done using just the last digit of the entries in the matrix. This is easy to do in one's head even if the entries in the matrix have many digits.

We will let $LF^{+}(\mathbb{Z})$ denote the elements of $LF(\mathbb{Z})$ corresponding to matrices of determinant $+1$.

Proposition 3.4. *For any two edges $\langle p/q, r/s\rangle$ and $\langle p'/q', r'/s'\rangle$ of the Farey diagram there exists a unique element $T \in LF^{+}(\mathbb{Z})$ taking the first edge to the second edge preserving the ordering of the vertices, so $T(p/q) = p'/q'$ and $T(r/s) = r'/s'$.*

Proof: We already know that there exists an element T in $LF(\mathbb{Z})$ with $T(p/q) = p'/q'$ and $T(r/s) = r'/s'$, and in fact there are exactly two choices for T which are distinguished by which of the two triangles containing $\langle p'/q', r'/s'\rangle$ a triangle containing $\langle p/q, r/s\rangle$ is sent to. One of these choices will make T preserve orientation and the other will make T reverse orientation. So there is only one choice where the determinant is $+1$. □

Exercises

1. Find a formula for the linear fractional transformation that rotates the triangle $\langle 0/1, 1/2, 1/1\rangle$ to $\langle 1/1, 0/1, 1/2\rangle$.

2. Find the linear fractional transformation that reflects the Farey diagram across the edge $\langle 1/2, 1/3\rangle$ (so in particular, the transformation takes $1/2$ to $1/2$ and $1/3$ to $1/3$).

3. Find a formula for the linear fractional transformation that reflects the upper half-plane version of the Farey diagram across the vertical line $x = 3/2$.

4. Find an infinite periodic strip of triangles in the Farey diagram such that the transformation $\left(\begin{smallmatrix}0&1\\1&2\end{smallmatrix}\right)$ is a glide-reflection along this strip and the transformation $\left(\begin{smallmatrix}0&1\\1&2\end{smallmatrix}\right)\left(\begin{smallmatrix}0&1\\1&2\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&2\\2&5\end{smallmatrix}\right)$ is a translation along this strip.

5. Let T be an element of $LF(\mathbb{Z})$ with matrix $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$. Show that the composition $T\left(\begin{smallmatrix}-1&0\\0&1\end{smallmatrix}\right)T^{-1}$ is the reflection across the edge $\langle a/c, b/d\rangle = T(\langle 1/0, 0/1\rangle)$.

For each of the remaining six problems, compute the value of the given periodic or eventually periodic continued fraction by first drawing the associated infinite strip of triangles, then finding a linear fractional transformation T in $LF(\mathbb{Z})$ that gives the periodicity in the strip, then solving $T(z) = z$.

6. $\overline{{}^{1}\!/_{2} + {}^{1}\!/_{5}}$

7. $\overline{{}^{1}\!/_{2} + {}^{1}\!/_{1} + {}^{1}\!/_{1}}$

8. $\overline{{}^{1}\!/_{1} + {}^{1}\!/_{1} + {}^{1}\!/_{1} + {}^{1}\!/_{1} + {}^{1}\!/_{1} + {}^{1}\!/_{2}}$

9. $2 + \overline{{}^{1}\!/_{1} + {}^{1}\!/_{1} + {}^{1}\!/_{4}}$

10. $2 + \overline{{}^{1}\!\nearrow\!{}_{1} + {}^{1}\!\nearrow\!{}_{1} + {}^{1}\!\nearrow\!{}_{1} + {}^{1}\!\nearrow\!{}_{4}}$

11. ${}^{1}\!\nearrow\!{}_{1} + {}^{1}\!\nearrow\!{}_{1} + \overline{{}^{1}\!\nearrow\!{}_{2} + {}^{1}\!\nearrow\!{}_{3}}$

Chapter 4. Quadratic Forms

Finding Pythagorean triples is answering the question, *When is the sum of two squares equal to a square*? More generally one can ask, *Exactly which numbers are sums of two squares*? In other words, when does an equation $x^2 + y^2 = n$ have integer solutions, and how can one find these solutions? The brute force approach of simply plugging in values for x and y leads to the following list of all solutions for $n \le 50$ (apart from interchanging x and y):

$$\mathbf{1} = 1^2 + 0^2,\ \mathbf{2} = 1^2 + 1^2,\ \mathbf{4} = 2^2 + 0^2,\ \mathbf{5} = 2^2 + 1^2,\ \mathbf{8} = 2^2 + 2^2,\ \mathbf{9} = 3^2 + 0^2,$$
$$\mathbf{10} = 3^2 + 1^2,\ \mathbf{13} = 3^2 + 2^2,\ \mathbf{16} = 4^2 + 0^2,\ \mathbf{17} = 4^2 + 1^2,\ \mathbf{18} = 3^2 + 3^2,$$
$$\mathbf{20} = 4^2 + 2^2,\ \mathbf{25} = 5^2 + 0^2 = 4^2 + 3^2,\ \mathbf{26} = 5^2 + 1^2,\ \mathbf{29} = 5^2 + 2^2,\ \mathbf{32} = 4^2 + 4^2,$$
$$\mathbf{34} = 5^2 + 3^2,\ \mathbf{36} = 6^2 + 0^2,\ \mathbf{37} = 6^2 + 1^2,\ \mathbf{40} = 6^2 + 2^2,\ \mathbf{41} = 5^2 + 4^2,$$
$$\mathbf{45} = 6^2 + 3^2,\ \mathbf{49} = 7^2 + 0^2,\ \mathbf{50} = 5^2 + 5^2 = 7^2 + 1^2$$

Notice that in some cases there is more than one solution for a given value of n. Our first goal will be to describe a more efficient way to find the integer solutions of $x^2 + y^2 = n$ and to display them graphically in a way that sheds much light on their structure. The technique for doing this will work not just for the function $x^2 + y^2$ but also for any function $Q(x,y) = ax^2 + bxy + cy^2$, where a, b, and c are integer constants. Such a function $Q(x,y)$ with at least one of the coefficients a, b, c nonzero is called a *quadratic form*, or sometimes just a *form* for short.

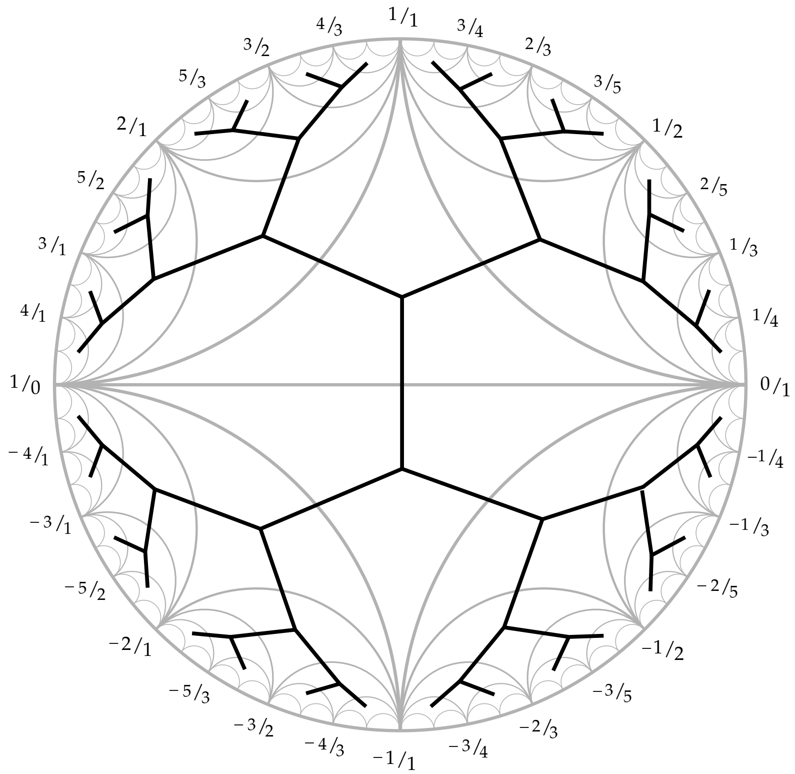
Solving $x^2 + y^2 = n$ amounts to representing n in the form of the sum of two squares. More generally, solving $Q(x,y) = n$ is called *representing n by the form* $Q(x,y)$. So the overall goal is to solve the *representation problem*: Which numbers n are represented by a given form $Q(x,y)$, and how does one find such representations.

Before starting to describe the method for displaying the values of a quadratic form graphically let us make a preliminary observation: If the greatest common divisor of two integers x and y is d, then $Q(x,y) = d^2Q(\frac{x}{d}, \frac{y}{d})$ where the greatest common divisor of $\frac{x}{d}$ and $\frac{y}{d}$ is 1. Hence it suffices to find the values of Q on *primitive* pairs (x,y), the pairs whose greatest common divisor is 1, and then multiply these values by arbitrary squares d^2. Thus the real problem is to find the primitive representations of a number n by a form $Q(x,y)$, or in other words, to find the primitive solutions of $Q(x,y) = n$.

Primitive pairs (x,y) correspond almost exactly to fractions x/y that are reduced to lowest terms, the only ambiguity being that both (x,y) and $(-x,-y)$ correspond to the same fraction x/y. However, this ambiguity does not affect the value of a quadratic form $Q(x,y) = ax^2 + bxy + cy^2$ since $Q(x,y) = Q(-x,-y)$. This means that we can regard $Q(x,y)$ as being essentially a function $f(x/y)$. Notice that we are not excluding the possibility $(x,y) = (1,0)$ which corresponds to the "fraction" $1/0$.

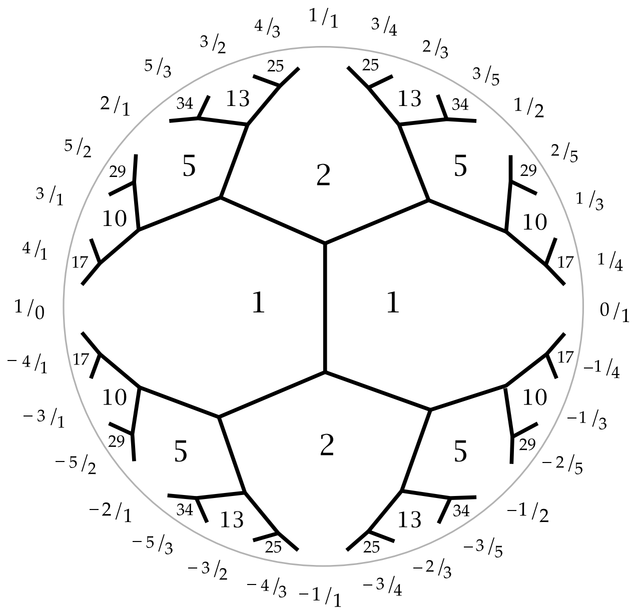
The Topograph

We already have a nice graphical representation of the rational numbers x/y and $1/0$ as the vertices in the Farey diagram. Here is a picture of the diagram with the so-called *dual tree* superimposed:



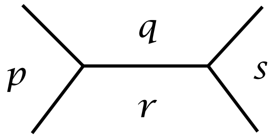
The dual tree has a vertex in the center of each triangle of the Farey diagram, and it has an edge crossing each edge of the Farey diagram. (The upper half of the dual tree actually looks like it could be the branch system of a real tree, with the lower half its reflection in still water or perhaps its root system.) As with the Farey diagram, we can only draw a finite part of the dual tree. The actual dual tree has branching that repeats infinitely often, an unending bifurcation process with smaller and smaller twigs.

The tree divides the interior of the large circle into regions, each of which is adjacent to one vertex of the original diagram. We can write the value $Q(x,y)$ in the region adjacent to the vertex x/y. This is shown in the figure below for the quadratic form $Q(x,y) = x^2 + y^2$, where to unclutter the picture we no longer draw the triangles of the original Farey diagram.



For example the 13 in the region adjacent to the fraction 2/3 represents the value $2^2 + 3^2$, and the 29 in the region adjacent to 5/2 represents the value $5^2 + 2^2$.

For a quadratic form Q this picture showing the values $Q(x, y)$ is called the *topograph* of Q. It turns out that there is a very simple method for computing the topograph from just a very small amount of initial data. This method is based on the following:

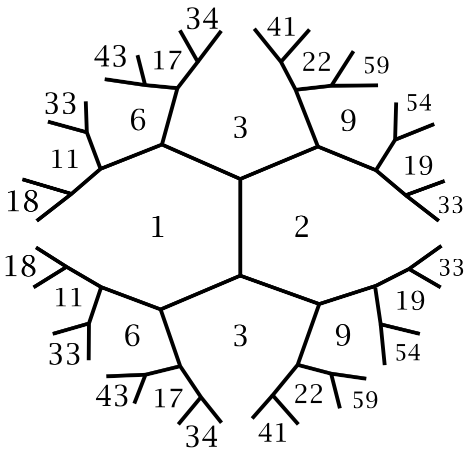


Arithmetic Progression Rule. If the values of $Q(x, y)$ in the four regions surrounding an edge in the tree are p, q, r, and s as indicated in the figure, then the three numbers p, $q + r$, s form an arithmetic progression.

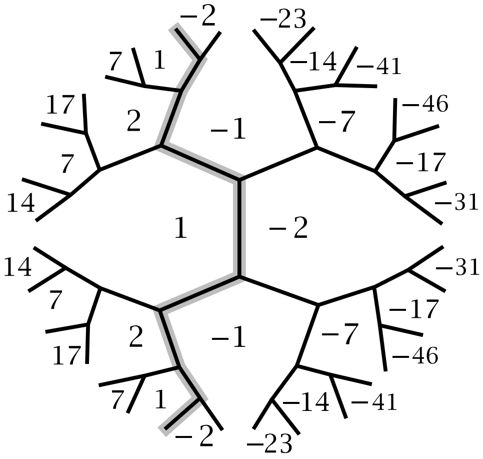
We can check this in the topograph of $x^2 + y^2$ shown above. Consider for example one of the edges separating the values 1 and 2. The values in the four regions surrounding this edge are $1, 1, 2, 5$ and the arithmetic progression is $1, 1 + 2, 5$. For an edge separating the values 1 and 5 the arithmetic progression is $2, 1 + 5, 10$. For an edge separating the values 5 and 13 the arithmetic progression is $2, 5 + 13, 34$. And similarly for all the other edges.

The arithmetic progression rule implies that the values of Q in the three regions surrounding a single vertex of the tree determine the values in all other regions, by starting at the vertex where the three adjacent values are known and working one's way outward in the dual tree. The easiest place to start for a quadratic form $Q(x, y) = ax^2 + bxy + cy^2$ is with the three values $Q(1, 0) = a$, $Q(0, 1) = c$, and $Q(1, 1) = a + b + c$ for the three fractions 1/0, 0/1, and 1/1. Here are two examples:

$Q(x,y) = x^2 + 2y^2$



$Q(x,y) = x^2 - 2y^2$



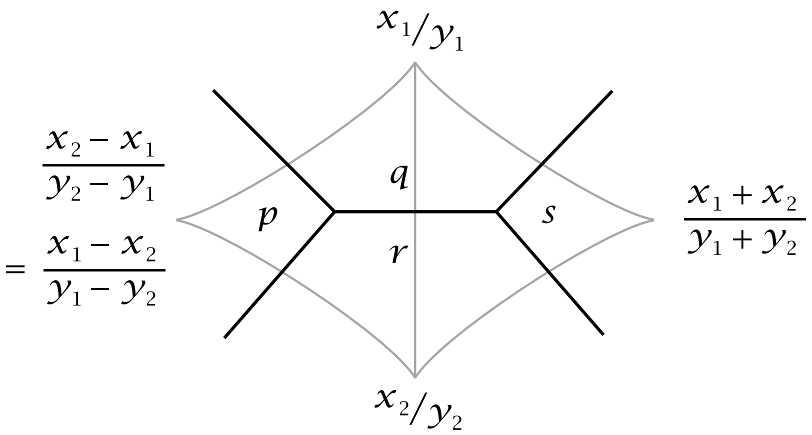
In the first case we start with the values 1 and 2 together with the 3 just above them. These determine the value 9 above the 2 via the arithmetic progression $1,\ 2+3,\ 9$. Similarly the 6 above the 1 is determined by the arithmetic progression $2,\ 1+3,\ 6$. Next one can fill in the 19 next to the 9 we just computed, using the arithmetic progression $3,\ 2+9,\ 19$, and so on for as long as one likes.

The procedure for the other form $x^2 - 2y^2$ is just the same, but here there are negative as well as positive values. The edges that separate positive values from negative values will be important later, so we have indicated these edges by special shading.

Perhaps the most noticeable thing in both the examples $x^2 + 2y^2$ and $x^2 - 2y^2$ is the fact that the values in the lower half of the topograph are the same as those in the upper half. We could have predicted in advance that this would happen because $Q(x,y) = Q(-x,y)$ whenever $Q(x,y)$ has the form $ax^2 + cy^2$, with no xy term. The topograph for $x^2 + y^2$ has even more symmetry since the values of $x^2 + y^2$ are unchanged when x and y are switched, so the topograph has left-right symmetry as well.

Here is a general observation: The three values around one vertex of the topograph can be specified arbitrarily. For if we are given three numbers a, b, c then the quadratic form $ax^2 + (c-a-b)xy + by^2$ takes these three values for (x,y) equal to $(1,0)$, $(0,1)$, $(1,1)$.

Proof of the Arithmetic Progression Rule: Let the two vertices of the Farey diagram corresponding to the values q and r have labels x_1/y_1 and x_2/y_2 as in the figure below. Then by the mediant rule for labeling vertices, the labels on the p and s regions are the fractions shown. Note that these labels are correct even when $x_1/y_1 = 1/0$ and $x_2/y_2 = 0/1$.


x_1/y_1
$\frac{x_2-x_1}{y_2-y_1}$
$= \frac{x_1-x_2}{y_1-y_2}$
q
p
s
r
$\frac{x_1+x_2}{y_1+y_2}$
x_2/y_2

For a quadratic form $Q(x,y) = ax^2 + bxy + cy^2$ we then have

$$\begin{aligned} s = Q(x_1+x_2, y_1+y_2) &= a(x_1+x_2)^2 + b(x_1+x_2)(y_1+y_2) + c(y_1+y_2)^2 \\ &= \underbrace{ax_1^2 + bx_1y_1 + cy_1^2}_{Q(x_1,y_1)=q} + \underbrace{ax_2^2 + bx_2y_2 + cy_2^2}_{Q(x_2,y_2)=r} + (\cdots) \end{aligned}$$

Similarly we have

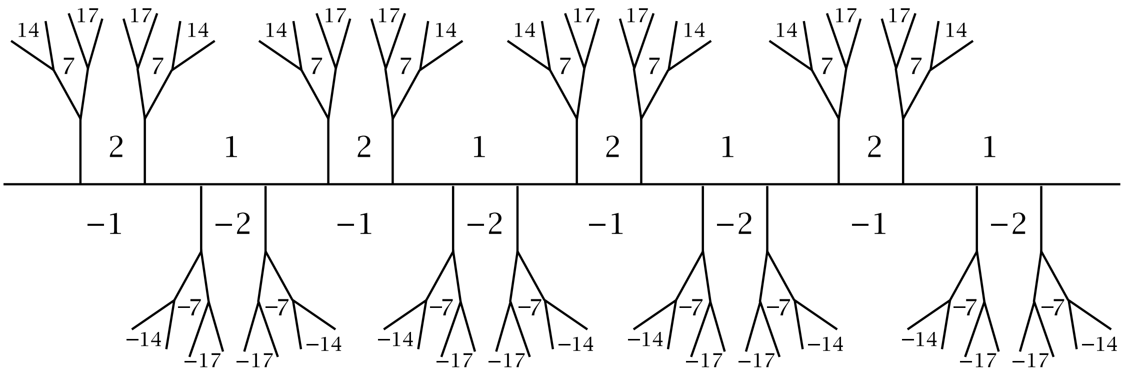
$$p = Q(x_1-x_2, y_1-y_2) = \underbrace{ax_1^2 + bx_1y_1 + cy_1^2}_{Q(x_1,y_1)=q} + \underbrace{ax_2^2 + bx_2y_2 + cy_2^2}_{Q(x_2,y_2)=r} - (\cdots)$$

The terms in $(\cdots)$ are the same in both cases, namely the terms involving both subscripts 1 and 2. If we compute $p+s$ by adding the two formulas together, the terms $(\cdots)$ will therefore cancel, leaving just $p+s = 2(q+r)$. This equation can be rewritten as $(q+r) - p = s - (q+r)$, which just says that $p, q+r, s$ forms an arithmetic progression. □

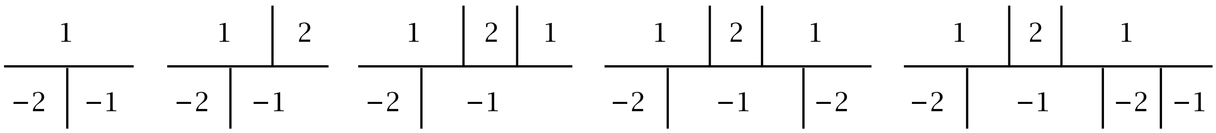
Periodic Separator Lines

For most quadratic forms that take on both positive and negative values, such as $x^2 - 2y^2$, there is another way of drawing the topograph that reveals some hidden and unexpected properties. For the form $x^2 - 2y^2$ there is a zigzag path of edges in the topograph separating the positive and negative values, and if we straighten this path out to be a line, called the *separator line*, what we see is the following infinitely repeated pattern:

$Q(x,y) = x^2 - 2y^2$

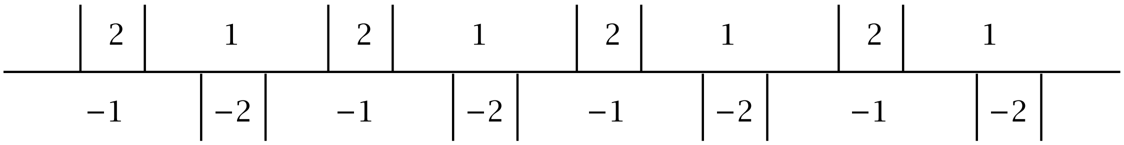


To construct this, one can first build the separator line starting with the three values $Q(1,0) = 1$, $Q(0,1) = -2$, and $Q(1,1) = -1$. Place these as shown in part (a) of the figure below, with a horizontal line segment separating the positive from the negative values.



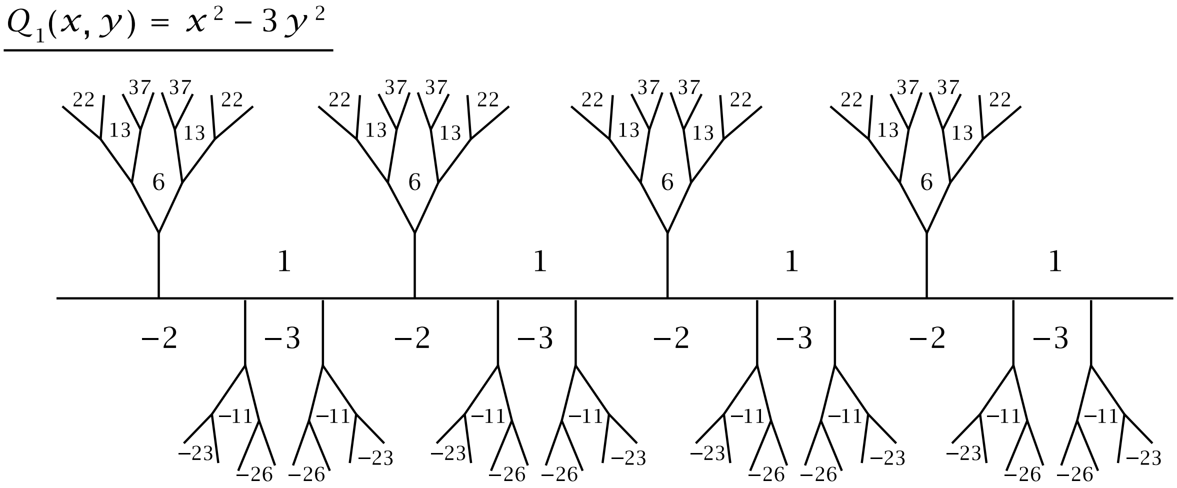
(a) (b) (c) (d) (e)

To extend the separator line one step farther to the right, apply the arithmetic progression rule to compute the next value 2 using the arithmetic progression $-2, 1 - 1, 2$. Since this value 2 is positive, we place it above the horizontal line and insert a vertical edge to separate this 2 from the 1 to the left of it, as in (b) of the figure. Now we repeat the process with the next arithmetic progression $1, 2 - 1, 1$ and put the new 1 above the horizontal line with a vertical edge separating it from the previous 2, as shown in (c). At the next step we compute the next value -2 and place it below the horizontal line since it is negative, giving (d). One more step produces (e) where we see that further repetitions will produce a pattern that repeats periodically as we move to the right. The arithmetic progression rule also implies that it repeats periodically to the left, so it is periodic in both directions:



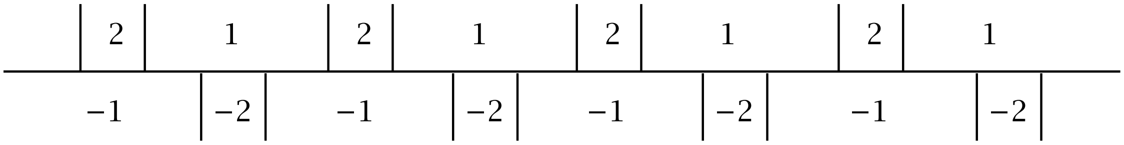
Thus we have the periodic separator line. To get the rest of the topograph we can then work our way upward and downward from the separator line, as shown in the original figure. As one moves upward from the separator line, the values of Q become larger and larger, approaching $+\infty$ monotonically, and as one moves downward the values approach $-\infty$ monotonically. The reason for this will become clear in the next chapter when we discuss something called the Monotonicity Property.

An interesting property of this form $x^2 - 2y^2$ that is evident from its topograph is that it takes on the same negative values as positive values. This would have been hard to predict from the formula $x^2 - 2y^2$. Indeed, for the similar-looking quadratic form $x^2 - 3y^2$ the negative values are quite different from the positive values, as one can see in its straightened-out topograph:

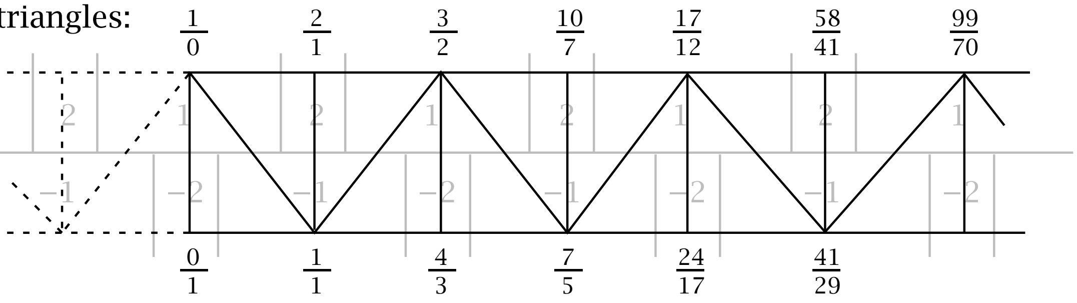


Continued Fractions Once More

There is a close connection between the topograph for a quadratic form $x^2 - dy^2$ and the infinite continued fraction for $\sqrt{d}$ when d is a positive integer that is not a square. In fact, we will see that the topograph can be used to compute the continued fraction for $\sqrt{d}$. As an example let us look at the case $d = 2$. The relevant portion of the topograph for $x^2 - 2y^2$ is the strip along the line separating the positive and negative values:

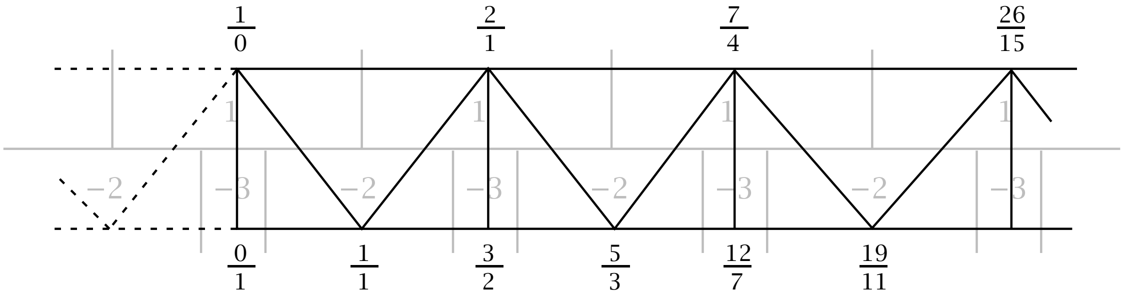


This is a part of the dual tree of the Farey diagram. If we superimpose the triangles of the Farey diagram corresponding to this part of the dual tree we obtain an infinite strip of triangles:

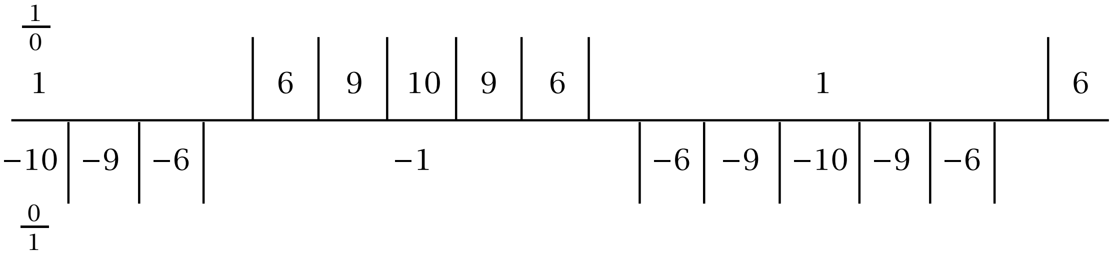


Ignoring the dotted triangles to the left, the infinite strip of triangles corresponds to the infinite continued fraction $1 + \overline{1/2}$. We could compute the value of this continued fraction by the method in Chapter 2, but there is an easier way using the quadratic form $x^2 - 2y^2$. For fractions $\frac{x}{y}$ labeling the vertices along the infinite strip, the corresponding values $n = x^2 - 2y^2$ are either ± 1 or ± 2. We can rewrite the equation $x^2 - 2y^2 = n$ as $(\frac{x}{y})^2 = 2 + \frac{n}{y^2}$. As we go farther and farther to the right in the infinite strip, both x and y are getting larger and larger while n only varies through finitely many values, namely ± 1 and ± 2, so the quantity $\frac{n}{y^2}$ is approaching 0. The equation $(\frac{x}{y})^2 = 2 + \frac{n}{y^2}$ then implies that $(\frac{x}{y})^2$ is approaching 2, so we see that $\frac{x}{y}$ is approaching $\sqrt{2}$. Since the fractions $\frac{x}{y}$ are also approaching the value of the infinite continued fraction $1 + \overline{{}^{1}\!\nearrow_{2}}$ that corresponds to the infinite strip, this implies that the value of the continued fraction $1 + \overline{{}^{1}\!\nearrow_{2}}$ is $\sqrt{2}$.

Here is another example, for the quadratic form $x^2 - 3y^2$, showing how $\sqrt{3} = 1 + \overline{{}^{1}\!\nearrow_{1} + {}^{1}\!\nearrow_{2}}$.

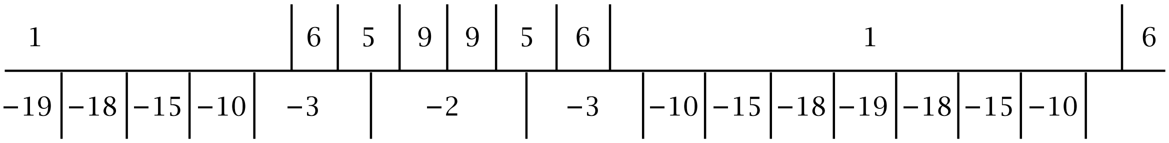


After looking at these two examples one can see that it is not really necessary to draw the strip of triangles, and one can just read off the continued fraction directly from the periodic separator line. Let us illustrate this by considering the form $x^2 - 10y^2$:



If one moves toward the right along the horizontal line starting at a point in the edge separating the $\frac{1}{0}$ region from the $\frac{0}{1}$ region, one first encounters 3 edges leading off to the right (downward), then 6 edges leading off to the left (upward), then 6 edges leading off to the right, and so on. This means that the continued fraction for $\sqrt{10}$ is $3 + \overline{{}^{1}\!\nearrow_{6}}$.

Here is a more complicated example showing how to compute the continued fraction for $\sqrt{19}$ from the form $x^2 - 19y^2$:

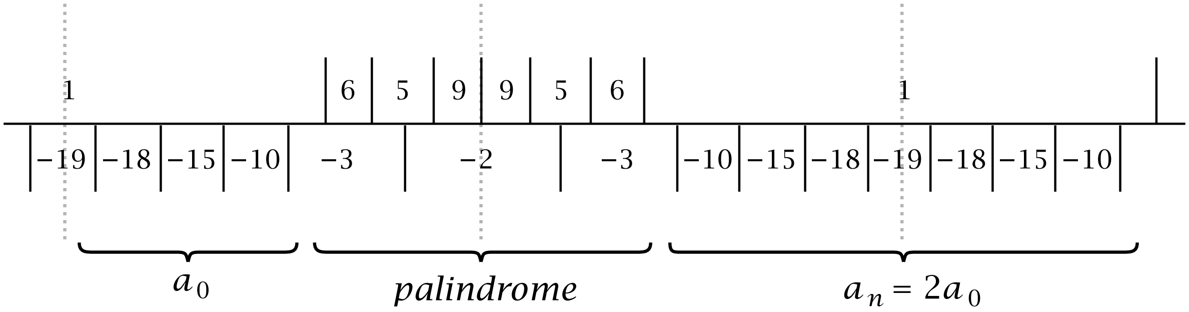


From this we read off that $\sqrt{19} = 4 + \overline{{}^1\!/_{2} + {}^1\!/_{1} + {}^1\!/_{3} + {}^1\!/_{1} + {}^1\!/_{2} + {}^1\!/_{8}}$.

In the next chapter we will prove that the topograph of the form $x^2 - dy^2$ always has a periodic separator line whenever d is a positive integer that is not a square. As in the examples above, this separator line always includes the edge of the dual tree separating the vertices $1/0$ and $0/1$ since the form takes the positive value $+1$ on $1/0$ and the negative value $-d$ on $0/1$. The periodicity then implies that the continued fraction for $\sqrt{d}$ has the form

$$\sqrt{d} = a_0 + \overline{{}^1\!/_{a_1} + {}^1\!/_{a_2} + \cdots + {}^1\!/_{a_n}}$$

with the periodic part starting immediately after the initial term a_0. In addition to being periodic, the separator line also has mirror symmetry with respect to reflection across the vertical line corresponding to the edge connecting $1/0$ to $0/1$ in the Farey diagram. This is because the form $x^2 - dy^2$ has no xy term, so replacing x/y by $-x/y$ does not change the value of the form. Once the separator line has symmetry with respect to this vertical line, the periodicity forces it to have mirror symmetry with respect to an infinite sequence of vertical lines, as illustrated in the following figure for the form $x^2 - 19y^2$:



In particular, these mirror symmetries imply that the continued fraction

$$\sqrt{d} = a_0 + \overline{{}^1\!/_{a_1} + {}^1\!/_{a_2} + \cdots + {}^1\!/_{a_n}}$$

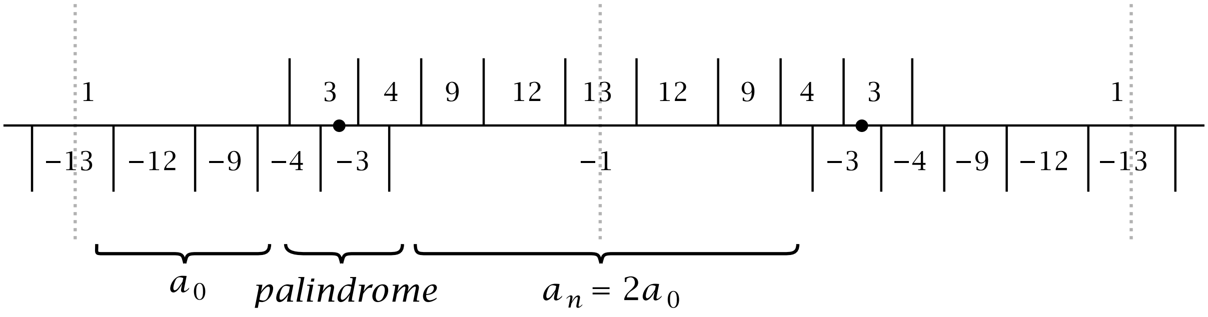
always has two special properties:

(a) $a_n = 2a_0$.

(b) The intermediate terms $a_1, a_2, \cdots, a_{n-1}$ form a palindrome, reading the same forward as backward.

Thus in $\sqrt{19} = 4 + \overline{{}^1\!/_{2} + {}^1\!/_{1} + {}^1\!/_{3} + {}^1\!/_{1} + {}^1\!/_{2} + {}^1\!/_{8}}$ the final 8 is twice the initial 4, and the intermediate terms $2, 1, 3, 1, 2$ form a palindrome. These special properties held also in the earlier examples, but were less apparent because there were fewer terms in the repeated part of the continued fraction.

In some cases there is an additional kind of symmetry along the separator line, as illustrated for the form $x^2 - 13y^2$:



As before there is a horizontal translation giving the periodicity and there are mirror symmetries across vertical lines, but now there is an extra glide-reflection along the strip that interchanges the positive and negative values of the form. Performing this glide-reflection twice in succession gives the translational periodicity. Notice that there are also 180 degree rotational symmetries about the points marked with dots on the separator line, and these rotations account for the palindromic middle part of the continued fraction

$$\sqrt{13} = 3 + \overline{{}^1\!/\!_1 + {}^1\!/\!_1 + {}^1\!/\!_1 + {}^1\!/\!_1 + {}^1\!/\!_6}$$

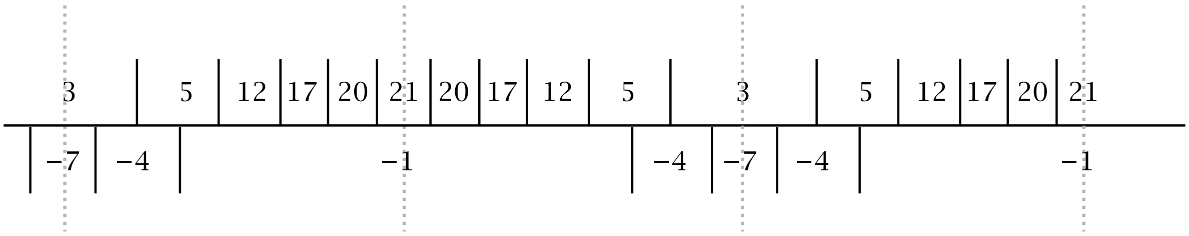
The fact that the periodic part has odd length corresponds to the separator strip having the glide-reflection symmetry. We could rewrite the continued fraction to have a periodic part of even length by doubling the period,

$$\sqrt{13} = 3 + \overline{{}^1\!/\!_1 + {}^1\!/\!_1 + {}^1\!/\!_1 + {}^1\!/\!_1 + {}^1\!/\!_6 + {}^1\!/\!_1 + {}^1\!/\!_1 + {}^1\!/\!_1 + {}^1\!/\!_1 + {}^1\!/\!_6}$$

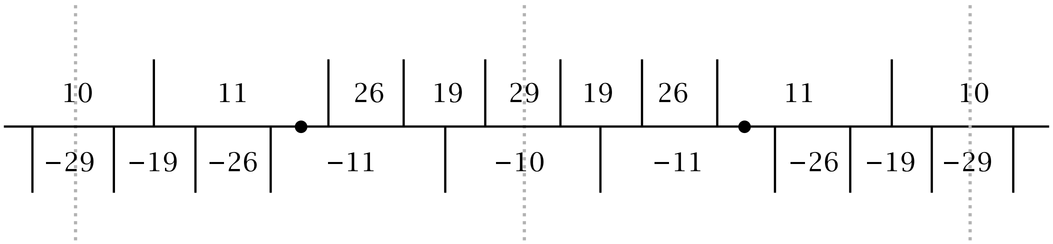
and this corresponds to ignoring the glide-reflection and just considering the translational periodicity.

We have been using quadratic forms $x^2 - dy^2$ to compute the continued fractions for irrational numbers $\sqrt{d}$, but everything works just the same for irrational numbers $\sqrt{p/q}$ if one uses the quadratic form $qx^2 - py^2$ in place of $x^2 - dy^2$. Following the same reasoning as before, if the equation $qx^2 - py^2 = n$ is rewritten as $q(\frac{x}{y})^2 = p + \frac{n}{y^2}$ then we see that as we move out along the periodic separator line the numbers x and y approach infinity while n cycles through finitely many values, so the term $\frac{n}{y^2}$ approaches 0 and the fractions $\frac{x}{y}$ approach a number z satisfying $qz^2 = p$, so $z = \sqrt{p/q}$. This argument depends of course on the existence of a periodic separator line, and we will prove in the next chapter that forms $qx^2 - py^2$ always have a periodic separator line, assuming that $\sqrt{p/q}$ is not a rational number, i.e., that p and q are not both squares.

Here are two examples. For the first one we use the form $3x^2 - 7y^2$ to compute the continued fraction for $\sqrt{7/3}$.



This gives $\sqrt{7/3} = 1 + \overline{{}^{1}\!/\!_{1} + {}^{1}\!/\!_{1} + {}^{1}\!/\!_{8} + {}^{1}\!/\!_{1} + {}^{1}\!/\!_{1} + {}^{1}\!/\!_{2}}$. For the second example we use $10x^2 - 29y^2$ to compute the continued fraction for $\sqrt{29/10}$,



with the result that $\sqrt{29/10} = 1 + \overline{{}^{1}\!/\!_{1} + {}^{1}\!/\!_{2} + {}^{1}\!/\!_{2} + {}^{1}\!/\!_{1} + {}^{1}\!/\!_{2}}$. The period of odd length here corresponds to the existence of the glide-reflection and 180 degree rotation symmetries.

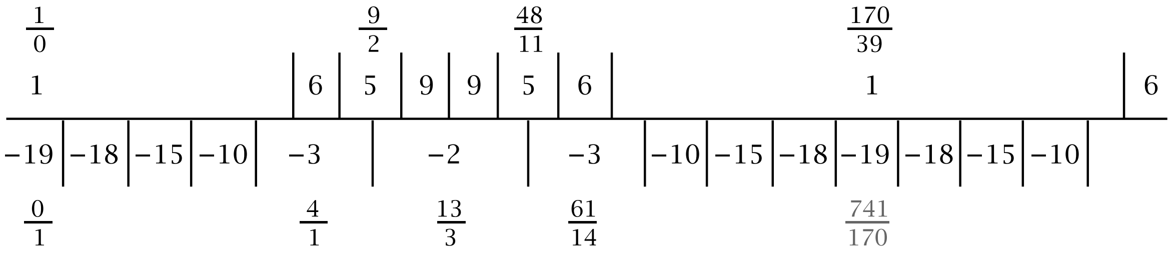
As one can see in these examples, the palindrome property and the relation $a_n = 2a_0$ still hold for the continued fractions for irrational numbers $\sqrt{p/q}$ assuming that $a_0 > 0$, which is equivalent to the condition $p/q > 1$ since a_0 is the integer part of $\sqrt{p/q}$. Fractions p/q less than 1 can easily be dealt with just by inverting them, interchanging p and q. Inverting a continued fraction $a_0 + \overline{{}^{1}\!/\!_{a_1} + {}^{1}\!/\!_{a_2} + \cdots + {}^{1}\!/\!_{a_n}}$ changes it to ${}^{1}\!/\!_{a_0} + \overline{{}^{1}\!/\!_{a_1} + {}^{1}\!/\!_{a_2} + \cdots + {}^{1}\!/\!_{a_n}}$. For example, from the earlier computation of $\sqrt{7/3}$ we obtain $\sqrt{3/7} = {}^{1}\!/\!_{1} + \overline{{}^{1}\!/\!_{1} + {}^{1}\!/\!_{1} + {}^{1}\!/\!_{8} + {}^{1}\!/\!_{1} + {}^{1}\!/\!_{1} + {}^{1}\!/\!_{2}}$.

One might ask whether the irrational numbers $\sqrt{p/q}$ are the only numbers having a continued fraction $a_0 + \overline{{}^{1}\!/\!_{a_1} + {}^{1}\!/\!_{a_2} + \cdots + {}^{1}\!/\!_{a_n}}$ or ${}^{1}\!/\!_{a_0} + \overline{{}^{1}\!/\!_{a_1} + {}^{1}\!/\!_{a_2} + \cdots + {}^{1}\!/\!_{a_n}}$ satisfying the palindrome property and the relation $a_n = 2a_0$. The answer is yes, and it would not be hard to prove this using the methods we are developing in this book.

Pell's Equation

We encountered the equation $x^2 - dy^2 = 1$ briefly in Chapter 0. It is traditionally called Pell's equation, and the similar equation $x^2 - dy^2 = -1$ is sometimes called Pell's equation as well, or else the negative Pell's equation. If d is a square then the equations are not very interesting since in this case d can be incorporated into the y^2 term, so one is looking at the equations $x^2 - y^2 = 1$ and $x^2 - y^2 = -1$, which have only the trivial solutions $(x, y) = (\pm 1, 0)$ for the first equation and $(x, y) = (0, \pm 1)$ for the second equation, since these are the only cases when the difference between two squares is ± 1. We will therefore assume that d is not a square in what follows.

As an example let us look at the equation $x^2 - 19y^2 = 1$. We drew a portion of the periodic separator line for the form $x^2 - 19y^2$ earlier, and here it is again with some of the fractional labels x/y shown as well.



Ignoring the label $741/170$ for the moment, the other fractional labels are the first few convergents for the continued fraction for $\sqrt{19}$ that we computed before, $4 + {}^1\!/\!_2 + {}^1\!/\!_1 + {}^1\!/\!_3 + {}^1\!/\!_1 + {}^1\!/\!_2 + {}^1\!/\!_8$. These fractional labels are the labels on the vertices of the zigzag path in the infinite strip of triangles in the Farey diagram, which we can imagine being superimposed on the separator line in the figure. The fractional label we are most interested in is the $170/39$ because this is the label on a region where the value of the form $x^2 - 19y^2$ is 1. This means exactly that $(x, y) = (170, 39)$ is a solution of $x^2 - 19y^2 = 1$. In terms of continued fractions, the fraction $170/39$ is the value of the initial portion $4 + {}^1\!/\!_2 + {}^1\!/\!_1 + {}^1\!/\!_3 + {}^1\!/\!_1 + {}^1\!/\!_2$ of the continued fraction for $\sqrt{19}$, with the final term of the period omitted.

Since the topograph of $x^2 - 19y^2$ is periodic along the separator line, there are infinitely many different solutions of $x^2 - 19y^2 = 1$ along the separator line. Going toward the left just gives the negatives $-x/y$ of the fractions x/y to the right, changing the signs of x or y, so it suffices to see what happens toward the right. One way to do this is to use the linear fractional transformation that gives the periodicity translation toward the right. This transformation sends the edge $\langle 1/0, 0/1\rangle$ of the Farey diagram to the edge $\langle 170/39, 741/170\rangle$. Here $741/170$ is the value of the continued fraction $4 + {}^1\!/\!_2 + {}^1\!/\!_1 + {}^1\!/\!_3 + {}^1\!/\!_1 + {}^1\!/\!_2 + {}^1\!/\!_4$ obtained from the continued fraction for $\sqrt{19}$ by replacing the final number 8 in the period by one-half of its value, 4. The figure above shows why this is the right thing to do. We get an infinite sequence of larger and larger positive solutions of $x^2 - 19y^2 = 1$ by applying the periodicity transformation with matrix $\left(\begin{smallmatrix}170 & 741\\ 39 & 170\end{smallmatrix}\right)$ to the vector $(1, 0)$. For example,

$$\begin{pmatrix}170 & 741\\ 39 & 170\end{pmatrix}\begin{pmatrix}170\\ 39\end{pmatrix} = \begin{pmatrix}57799\\ 13260\end{pmatrix}$$

so the next solution of $x^2 - 19y^2 = 1$ after $(170, 39)$ is $(57799, 13260)$, and we could compute more solutions if we wanted. Obviously they are getting large rather quickly.

The two 170's in the matrix $\left(\begin{smallmatrix}170 & 741\\ 39 & 170\end{smallmatrix}\right)$ can hardly be just a coincidence. Notice also that the entry 741 factors as $19 \cdot 39$ which hardly seems like it should be just a coincidence either. Let's check that these numbers had to occur. In general, for the form $x^2 - dy^2$ let us suppose that we have found the first solution $(x, y) = (p, q)$ after $(1, 0)$ for Pell's equation $x^2 - dy^2 = 1$, so $p^2 - dq^2 = 1$. Then based on the previous example we suspect that the periodicity transformation is the transformation

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

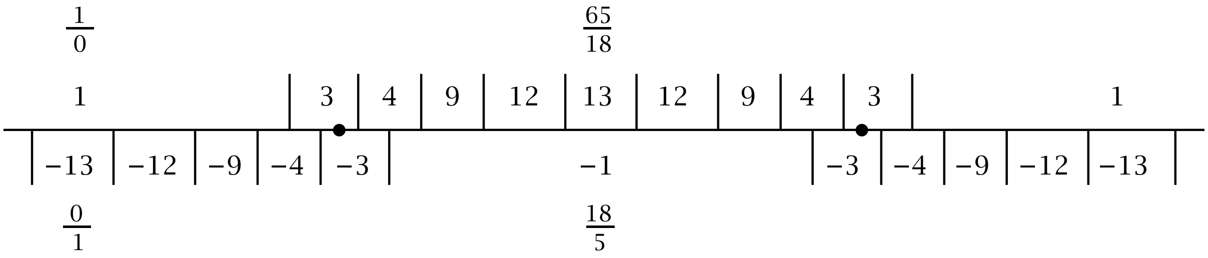
To check that this is correct the main thing to verify is that this transformation preserves the values of the quadratic form. When we plug in $(px + dqy, qx + dy)$ for (x, y) in $x^2 - dy^2$ we get

$$\begin{aligned}(px + dqy)^2 - d(qx + py)^2 &\\ &= p^2x^2 + 2pdqxy + d^2q^2y^2 - dq^2x^2 - 2pdqxy - dp^2y^2 \\ &= (p^2 - dq^2)x^2 - d(p^2 - dq^2)y^2 \\ &= x^2 - dy^2 \quad \text{since} \quad p^2 - dq^2 = 1\end{aligned}$$

so the transformation $\left(\begin{smallmatrix} p & dq \\ q & p \end{smallmatrix}\right)$ does preserve the values of the form. Also it takes $1/0$ to p/q, and its determinant is $p^2 - dq^2 = 1$, so it has to be the translation giving the periodicity along the separator line. (We haven't actually proved yet that periodic separator lines always exist for forms $x^2 - dy^2$, but we will do this in the next chapter.)

Are there other solutions of $x^2 - 19y^2 = 1$ besides the ones we have just described that occur along the separator line? The answer is No because we will see in the next chapter that as one moves away from the separator line in the topograph, the values of the quadratic form change in a monotonic fashion, steadily increasing toward $+\infty$ as one moves upward above the separator line, and decreasing steadily toward $-\infty$ as one moves downward below the separator line. Thus the value 1 occurs only along the separator line itself. Also we see that the value -1 never occurs, which means that the equation $x^2 - 19y^2 = -1$ has no integer solutions.

For an example where $x^2 - dy^2 = -1$ does have solutions, let us look again at the earlier example of $x^2 - 13y^2$.



The first positive solution $(x, y) = (p, q)$ of $x^2 - 13y^2 = -1$ corresponds to the value -1 in the middle of the figure. This is determined by the continued fraction $p/q = 3 + {}^{1}/_{1} + {}^{1}/_{1} + {}^{1}/_{1} + {}^{1}/_{1} = 18/5$, so we have $(p, q) = (18, 5)$. The matrix $\left(\begin{smallmatrix} p & dq \\ q & p \end{smallmatrix}\right)$ in this case is $\left(\begin{smallmatrix} 18 & 65 \\ 5 & 18 \end{smallmatrix}\right)$ with determinant $18^2 - 13 \cdot 5^2 = -1$ so this gives the glide-reflection along the periodic separator line taking $1/0$ to $18/5$ and $0/1$ to $65/18$. The smallest positive solution of $x^2 - 13y^2 = +1$ is obtained by applying this glide-reflection to $(18, 5)$, which gives

$$\begin{pmatrix} 18 & 65 \\ 5 & 18 \end{pmatrix} \begin{pmatrix} 18 \\ 5 \end{pmatrix} = \begin{pmatrix} 324 + 325 \\ 90 + 90 \end{pmatrix} = \begin{pmatrix} 649 \\ 180 \end{pmatrix}$$

Repeated applications of the glide-reflection will give solutions of $x^2 - 13y^2 = +1$ and $x^2 - 13y^2 = -1$ alternately.

Exercises

1. Draw the topograph for the form $Q(x,y) = 2x^2 + 5y^2$, showing all the values of $Q(x,y) \le 60$ in the topograph, with the associated fractional labels x/y. If there is symmetry in the topograph, you only need to draw one half of the topograph and state that the other half is symmetric.

2. Do the same for the form $Q(x,y) = 2x^2 + xy + 2y^2$, in this case displaying all values $Q(x,y) \le 40$ in the topograph.

3. Do the same for the form $Q(x,y) = x^2 - y^2$, showing all the values between $+30$ and -30 in the topograph, but omitting the labels x/y this time.

4. For the form $Q(x,y) = 2x^2 - xy + 3y^2$ do the following:
(a) Draw the topograph, showing all the values $Q(x,y) \le 30$ in the topograph, and including the labels x/y.
(b) List all the values $Q(x,y) \le 30$ in order, including the values when the pair (x,y) is not primitive.
(c) Find all the integer solutions of $Q(x,y) = 24$, both primitive and nonprimitive. (And don't forget that quadratic forms always satisfy $Q(x,y) = Q(-x,-y)$.)

5. Determine the periodic separator line in the topograph for each of the following quadratic forms (you do not need to include the fractional labels x/y):
(a) $x^2 - 7y^2$ (b) $3x^2 - 4y^2$ (c) $x^2 + xy - y^2$

6. Using your answers in the preceding problem, write down the continued fraction expansions for $\sqrt{7}$, $2\sqrt{3}/3$, and $(-1+\sqrt{5})/2$.

7. For the following quadratic forms, draw enough of the topograph, starting with the edge separating the $1/0$ and $0/1$ regions, to locate the periodic separator line, and include the separator line itself in your topograph.
(a) $x^2 + 3xy + y^2$ (b) $6x^2 + 18xy + 13y^2$ (c) $37x^2 - 104xy + 73y^2$

8. Use a quadratic form to compute continued fractions for the following pairs of numbers:
(a) $(3+\sqrt{6})/2$ and $(3-\sqrt{6})/2$ (b) $(11+\sqrt{13})/6$ and $(11-\sqrt{13})/6$
(c) $(14+\sqrt{7})/9$ and $(14-\sqrt{7})/9$

9. For the quadratic form $x^2 - 14y^2$ do the following things:
(a) Draw the separator line in the topograph and compute the continued fraction for $\sqrt{14}$.
(b) Find the smallest positive integer solutions of $x^2 - 14y^2 = 1$ and $x^2 - 14y^2 = -1$, if these equations have integer solutions.
(c) Find the linear fractional transformation that gives the periodicity translation along the separator line and use this to find a second positive solution of $x^2 - 14y^2 = 1$.
(d) Determine the integers n with $|n| \le 12$ such that the equation $x^2 - 14y^2 = n$ has

an integer solution. (Don't forget the possibility that there could be solutions (x, y) that aren't primitive.)

10. For the quadratic form $x^2 - 29y^2$ do the following things:
(a) Draw the separator line and compute the continued fraction for $\sqrt{29}$.
(b) Find the smallest positive integer solution of $x^2 - 29y^2 = -1$.
(c) Find a glide-reflection symmetry of the separator line and use this to find the smallest positive integer solution of $x^2 - 29y^2 = 1$.

11. Compute the periodic separator line for the form $x^2 - 43y^2$ and use this to find the continued fraction for $\sqrt{43}$.

Chapter 5. The Classification of Quadratic Forms

We can divide quadratic forms $Q(x,y) = ax^2+bxy+cy^2$ into four broad classes according to the signs of the values $Q(x,y)$, where as always we restrict x and y to integers. We will always assume at least one of the coefficients a,b,c is nonzero, so Q is not identically zero, and we will always assume (x,y) is not $(0,0)$. There are four possibilities:

(I) $Q(x,y)$ takes on both positive and negative values but not 0. In this case we call Q a *hyperbolic* form.

(II) $Q(x,y)$ takes on both positive and negative values and also 0. Then we call Q a 0-*hyperbolic* form.

(III) $Q(x,y)$ takes on only positive values or only negative values. Then we call Q *elliptic*.

(IV) Q takes on the value 0 and either positive or negative values, but not both. Then Q is called *parabolic*.

The hyperbolic-elliptic-parabolic terminology is motivated in part by what the level curves $ax^2 + bxy + cy^2 = k$ are, where we now allow x and y to take on all real values so that one gets actual curves. The level curves are hyperbolas in cases (I) and (II), and ellipses in case (III). In case (IV), however, the level curves are not parabolas as one might guess, but straight lines. Case (IV) will be the least interesting of the four cases.

There is an easy way to distinguish the four types of forms $ax^2 + bxy + cy^2$ in terms of their discriminants $\Delta = b^2 - 4ac$. As we will show later in the chapter:

(I) If Δ is positive but not a square then Q is hyperbolic.

(II) If Δ is positive and a square then Q is 0-hyperbolic.

(III) If Δ is negative then Q is elliptic.

(IV) If Δ is zero then Q is parabolic.

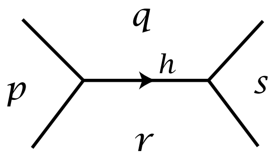
Discriminants turn out to play a central role in the theory of quadratic forms. A natural question to ask is whether every integer occurs as the discriminant of some form, and this is easy to answer. For a form $ax^2+bxy+cy^2$ we have $\Delta = b^2-4ac$, and this is congruent to b^2 mod 4. A square such as b^2 is always congruent to 0 or 1 mod 4, so the discriminant of a form is always congruent to 0 or 1 mod 4. Conversely, for every integer Δ congruent to 0 or 1 mod 4 there exists a form whose discriminant is Δ since:

$$x^2 - ky^2 \text{ has discriminant } \Delta = 4k$$
$$x^2 + xy - ky^2 \text{ has discriminant } \Delta = 4k + 1$$

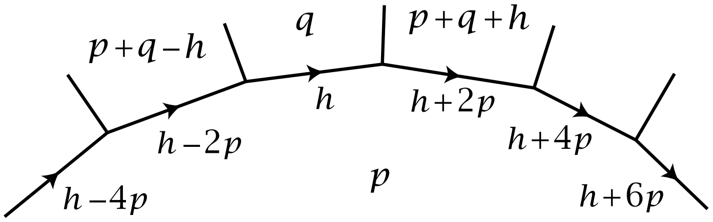
Here k can be positive, negative, or zero. The forms x^2-ky^2 and $x^2+xy-ky^2$ are called the *principal* quadratic forms of these discriminants.

We will analyze each of the four types of forms in turn, but before doing this let us make a few preliminary general comments.

In the arithmetic progression rule for labeling the four regions surrounding an edge of the topograph, we can label the edge by the common increment $h = (q + r) - p = s - (q + r)$ as in the figure at the right. The edge can be oriented by an arrow showing the direction in which the progression increases by h. Changing the sign of h corresponds to changing the orientation of the edge. In the special case that h happens to be 0 the orientation of the edge is irrelevant and can be omitted.

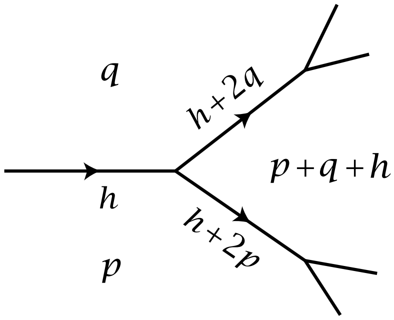


The values of the increment h along the boundary of a region in the topograph have the interesting property that they also form an arithmetic progression when all these edges are oriented in the same direction, and the amount by which h increases as we move from one edge to the next is $2p$ where p is the label on the region adjacent to all these edges:



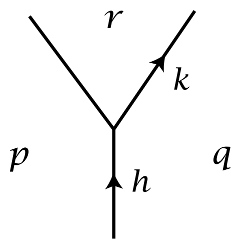
We will call this property the *Second Arithmetic Progression Rule.* To see why it is true, start with the edge labeled h in the figure, with the adjacent regions labeled p and q. The original Arithmetic Progression Rule then gives the value $p + q + h$ in the next region to the right. From this we can deduce that the label on the edge between the regions labeled p and $p + q + h$ must be $h + 2p$ since this is the increment from q to $p + (p + q + h)$. Thus the edge label increases by $2p$ when we move from one edge to the next edge to the right, so by repeated applications of this fact we see that we have an arithmetic progression of edge labels all along the border of the region labeled p.

Another thing worth noting at this point is something that we will refer to as the *Monotonicity Property*: If the three labels p, q, and h adjacent to an edge are all positive, then so are the three labels for the next two edges in front of this edge (orienting these edges as shown in the figure), and the new labels are larger than the old labels. It follows that when one continues forward out this part of the topograph, all the labels become monotonically larger the farther one goes. Similarly, when the original three labels are negative, all the labels become larger and larger negative, by the same principle applied to the negative $-Q(x, y)$ of the original form $Q(x, y)$.



Proposition 5.1. *If an edge in the topograph of $Q(x,y)$ is labeled h with adjacent regions labeled p and q, then the quantity $h^2 - 4pq$ is equal to the discriminant of $Q(x,y)$.*

Proof: For the given form $Q(x,y) = ax^2+bxy+cy^2$, the regions $1/0$ and $0/1$ in the topograph are labeled a and c, and the edge in the topograph separating these two regions has $h = b$ since the $1/1$ region is labeled $a+b+c$. So the statement of the proposition is correct for this edge. For other edges we proceed by induction, moving farther and farther out the tree. For the induction step suppose we have two adjacent edges labeled h and k as in the figure, and suppose inductively that the discriminant equals h^2-4pq. We have $r = p+q+h$, and from the second arithmetic progression rule we know that $k = h+2q$. Then we have $k^2-4qr = (h+2q)^2-4q(p+q+h) = h^2+4hq+4q^2-4pq-4q^2-4hq = h^2-4pq$, which means that the result holds for the edge labeled k as well. □



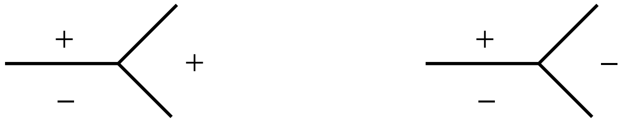
Hyperbolic Forms

Perhaps the most interesting of the four types of quadratic forms are the hyperbolic forms. We will show that these all have a periodic separator line as in the examples $x^2 - dy^2$ and $qx^2 - py^2$ that we looked at earlier.

Theorem 5.2. *For a hyperbolic form $Q(x,y)$ the edges of the topograph for which the two adjacent regions are labeled by numbers of opposite sign form a line which is infinite in both directions, and the topograph is periodic along this line.*

Proof: Since the form is hyperbolic, all regions of the topograph have labels that are either positive or negative, never zero. There must exist two regions of opposite sign since Q is hyperbolic, and by moving along a path in the topograph joining these two regions we will somewhere encounter two adjacent regions of opposite sign. Thus there must exist edges whose two adjacent regions have opposite sign. Let us call these edges *separating edges*. If we apply the discriminant formula $\Delta = h^2 - 4pq$ in preceding proposition to a separating edge, we see that Δ must be positive since p and q are nonzero and have opposite sign, so $-4pq$ is positive while h^2 is positive or zero. Thus a hyperbolic form must have positive discriminant.

At an end of a separating edge the value of Q in the next region must be either positive or negative since Q does not take the value 0:



This implies that exactly one of the two edges at the end of the first separating edge is also a separating edge. Repeating this argument, we see that each separating edge is part of a line of separating edges that is infinite in both directions (and the edges that lead off from this line are not separating edges).

As we move off this line of separating edges the values of Q are steadily increasing through positive integers on the positive side and steadily decreasing through negative integers on the negative side, by the monotonicity property, so there are no other separating edges that are not on this line.

It remains to prove that the topograph is periodic along the separator line. We can assume all the edges along the separator line are oriented in the same direction by changing the signs of the h values if necessary. For an edge of the separator line labeled h with adjacent regions labeled p and $-q$ with $p > 0$ and $q > 0$, we know that $h^2 + 4pq$ is equal to the discriminant Δ. From the equation $\Delta = h^2 + 4pq$ we obtain the inequalities $|h| < \sqrt{\Delta}$, $p \le \Delta/4$, and $q \le \Delta/4$. Thus there are only finitely many possible values for h, p, and q along the separator line. Hence there are only finitely many possible combinations of values h, p, and q at each edge on the separator line. Since the separator line is infinite, it follows that there must be two edges on the line that have the same values of h, p, and q. Since the topograph is uniquely determined by the three labels h, p, q at a single edge, the translation of the line along itself that takes one edge to another edge with the same three labels must preserve all the labels on the line. This shows that the separator line is periodic, including the values of Q along this line. □

Conceivably there might be just a single region on one side of the separator line, but this doesn't actually happen. There must be edges leading away from the separating line on both the side where the form is positive and on the side where it is negative, because if there was just a single region on one side of the line, the second arithmetic progression rule would say that the h labels along the line formed an infinite arithmetic progression, contradicting the fact that these values are periodic.

Here is an interesting consequence of the periodicity of the separator line:

Corollary 5.3. *For a hyperbolic form $Q(x,y) = ax^2 + bxy + cy^2$, if the equation $ax^2 + bxy + cy^2 = n$ has one integer solution then it has infinitely many integer solutions.*

Proof: Suppose (x,y) is a solution of $Q(x,y) = n$. If (x,y) is a primitive pair, then the number n appears in the topograph of Q infinitely many times, via the periodicity of the separator line, so there are infinitely many solutions in this case. If (x,y) is not primitive then it is m times a primitive pair (x',y') with $Q(x',y') = n/m^2$. This latter equation has infinitely many solutions as we just saw, so after replacing these solutions (x',y') by $(x,y) = (mx',my')$ we get infinitely many solutions of $Q(x,y) = n$. □

In Chapter 3 we gave an argument that showed that infinite continued fractions that are eventually periodic always represent quadratic irrational numbers. This is one half of Lagrange's Theorem, and now we can prove the other half, the converse statement:

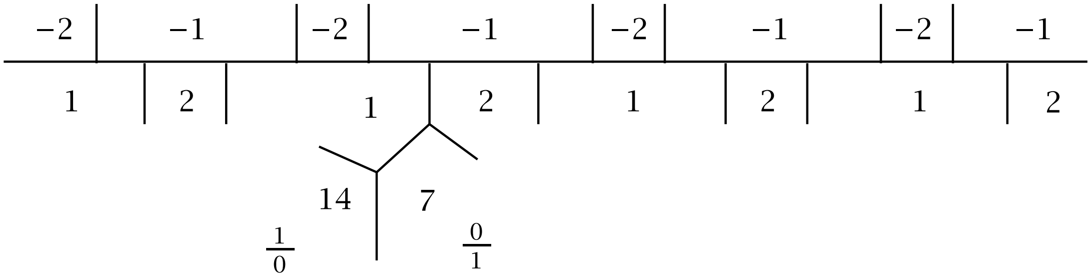
Theorem 5.4. *The continued fraction expansion of every quadratic irrational is eventually periodic.*

Proof: A quadratic irrational number α has the form $A + B\sqrt{n}$ where A and B are rational numbers and n is a positive integer that is not a square. Letting $\overline{\alpha}$ be the conjugate $A - B\sqrt{n}$ of α, we see that α and $\overline{\alpha}$ are roots of the quadratic equation $(x-\alpha)(x-\overline{\alpha}) = x^2 - (\alpha+\overline{\alpha})x + \alpha\overline{\alpha} = x^2 - 2Ax + (A^2 - nB^2) = 0$ whose coefficients are rational numbers. After multiplying through by a common denominator we can replace this equation by an equation $ax^2 + bx + c = 0$ with integer coefficients having α and $\overline{\alpha}$ as roots. The leading coefficient a is nonzero since it arose from a leading coefficient 1 by multiplying by a common denominator, which is not zero.

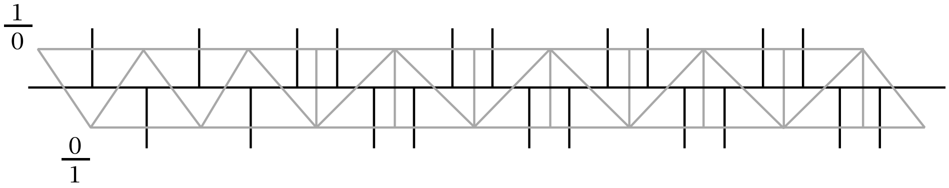
From the quadratic equation $ax^2 + bx + c = 0$ we obtain a quadratic form $Q(x,y) = ax^2 + bxy + cy^2$ with the same coefficients a, b, c. From the factorization of $ax^2 + bx + c$ as $a(x-\alpha)(x-\overline{\alpha})$ we see that $Q(x,y)$ can be factored as $a(x-\alpha y)(x-\overline{\alpha}y)$ since in both cases this just amounts to saying that $b = -a(\alpha+\overline{\alpha})$ and $c = a\alpha\overline{\alpha}$. Let us show that the quadratic form Q is hyperbolic. It cannot take on the value 0 at an integer pair $(x,y) \neq (0,0)$ since if $a(x-\alpha y)(x-\overline{\alpha}y) = 0$ then one of the factors would have to be zero, but we assume a is nonzero, and if one of the other two factors was zero we would have $\alpha = x/y$ or $\overline{\alpha} = x/y$ where x/y is rational, contradicting the assumption that α and $\overline{\alpha}$ are irrational. To see that Q takes on both positive and negative values we again use its factorization as $a(x-\alpha y)(x-\overline{\alpha}y)$. The two lines $x = \alpha y$ and $x = \overline{\alpha}y$ in the xy-plane divide the plane into four regions since $\alpha \neq \overline{\alpha}$, and the sign of $a(x-\alpha y)(x-\overline{\alpha}y)$ changes whenever we cross one of these two lines from one region to an adjacent region. Since each region contains points (x,y) with integer coordinates, this means that $Q(x,y)$ takes on both positive and negative values at integer pairs (x,y).

Since Q is hyperbolic, its topograph contains a periodic line separating the positive and negative values. This corresponds to a strip in the Farey diagram which is infinite in both directions. The fractions x_n/y_n labeling the vertices along this strip have both x_n and y_n approaching $\pm\infty$ as n goes to $\pm\infty$. (The only way this could fail for a path consisting of an infinite sequence of distinct edges in the dual tree would be if all the edges from some point onward bordered the $1/0$ or $0/1$ region, which is not the case here since periodic separator lines have only a finite number of their edges bordering a given region.) The values $Q(x_n, y_n) = ax_n^2 + bx_ny_n + cy_n^2 = k_n$ are bounded, ranging over a finite set along the strip. Thus the numbers $a(x_n/y_n)^2 + b(x_n/y_n) + c = k_n/y_n^2$ approach 0 as n goes to $\pm\infty$, so at one end of the strip we have x_n/y_n approaching one root α and at the other end we have x_n/y_n approaching the other root $\overline{\alpha}$. Joining either end of the strip to $1/0$ in the Farey diagram then gives infinite strips corresponding to infinite continued fractions for α and $\overline{\alpha}$ that are eventually periodic. □

Let us look at an example to illustrate the procedure in the proof of this theorem. We will use a quadratic form to compute the continued fractions for the two quadratic irrationals $\alpha = \frac{10+\sqrt{2}}{14}$ and $\overline{\alpha} = \frac{10-\sqrt{2}}{14}$. The equation $(x-\alpha)(x-\overline{\alpha}) = 0$ is then $x^2 - \frac{10}{7}x + \frac{1}{2} = 0$, so with integer coefficients this becomes $14x^2 - 20x + 7 = 0$. The associated quadratic form is $14x^2 - 20xy + 7y^2$. To compute the topograph we start with the three values at $1/0$, $0/1$, and $1/1$ and work toward the separator line:



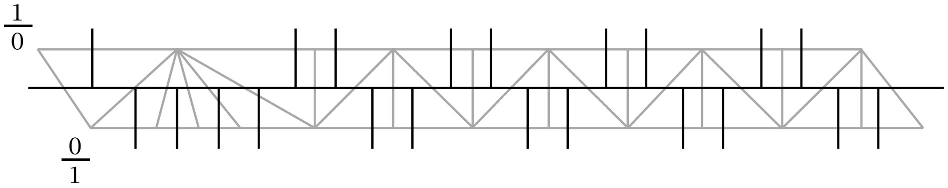
This figure lies in the upper half of the circular Farey diagram where the fractions x/y are positive, so if we follow the separator line out to the right we approach the smaller of the two roots of $14x^2 - 20x + 7 = 0$, which is $\frac{10-\sqrt{2}}{14}$, and if we follow the separator line to the left we approach the larger root, $\frac{10+\sqrt{2}}{14}$. To get the continued fraction for the smaller root we follow the path in the figure that starts with the edge between $1/0$ and $0/1$, then zigzags up to the separator line, then goes out this line to the right. If we straighten this path out it looks like the following:



The continued fraction is therefore

$$\frac{10-\sqrt{2}}{14} = {}^{1}\!\diagup_{1} + {}^{1}\!\diagup_{1} + {}^{1}\!\diagup_{1} + {}^{1}\!\diagup_{1} + \overline{{}^{1}\!\diagup_{2}}$$

It is not actually necessary to redraw the straightened-out path since in the original form of the topograph we can read off the sequence of left and right "side roads" as we go along the path, the sequence $LRLR\overline{LLRR}$ where L denotes a side road to the left and R a side road to the right. This sequence determines the continued fraction. For the other root $\frac{10+\sqrt{2}}{14}$ the straightened-out path has the following shape:

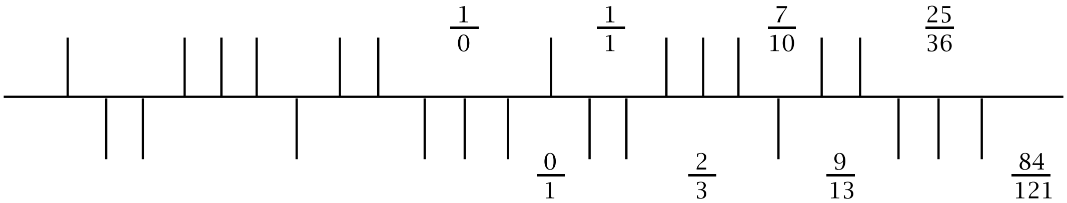


The sequence of side roads is $LRRRR\overline{LLRR}$ so the continued fraction is

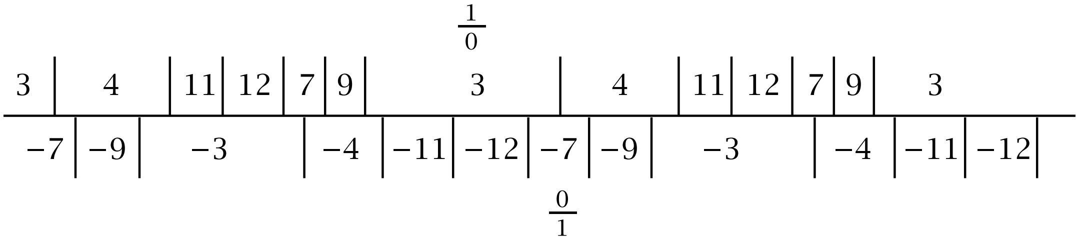
$$\frac{10+\sqrt{2}}{14} = 1\diagup 1 + 1\diagup 4 + \overline{1\diagup 2}$$

A natural question to ask is whether every periodic line in the dual tree of the Farey diagram is the separator line of some hyperbolic form. The answer is yes, and in fact the form is unique up to multiplication by a constant, which does not affect the separator line. We can compute the form by the following procedure. First compute a linear fractional transformation T that realizes the periodicity for the given periodic line. Next write down the equation $T(z) = z$ for the fixed points of T at the two ends of the periodic line. This equation simplifies to a quadratic equation $az^2+bz+c = 0$, and then the quadratic form $ax^2 + bxy + cy^2$ will be the form we want, with the given periodic line as its separator line.

To illustrate the procedure let us find a quadratic form whose periodic separator line is the following:



From the vertex labels we see that the translation giving the periodicity has matrix $\left(\begin{smallmatrix}25 & 84\\ 36 & 121\end{smallmatrix}\right)$ so it is the transformation $T(z) = (25z+84)/(36z+121)$. The fixed points of T are determined by setting this equal to z. The resulting equation simplifies to $25z + 84 = 36z^2 + 121z$ and then $36z^2 + 96z - 84 = 0$ or just $3z^2 + 8z - 7 = 0$. The roots α and $\overline{\alpha}$ of this equation are the fixed points, but we do not actually have to compute them since we know the quadratic form we want is $ax^2 + bxy + cy^2 = a(x-\alpha y)(x-\overline{\alpha}y)$ which in this example is just $3x^2+8xy-7y^2$. To check this we can compute the separator line of this form:



This provides a realization of the given periodic line as the separator line in the topograph of a quadratic form. Any constant multiple of this form would also have the same separator line.

We could have simplified the calculation slightly by noting that the periodic line we started with is taken to itself by a glide reflection that moves the line only half as far along itself as the translation T that we used. This glide reflection is $T'(z) = (2z+7)/(3z+10)$ and it has the same fixed points as T so we could use the equation

$T'(z) = z$ instead of $T(z) = z$. This gives $2z + 7 = 3z^2 + 10z$ which simplifies immediately to $3z^2 + 8z - 7 = 0$.

Notice that the separator line for $3x^2 + 8xy - 7y^2$ is not symmetric under reflection across any vertical line, unlike all the separator lines we have seen up to this point. This is the simplest example without this mirror symmetry property since the periodic strips associated to continued fractions $\overline{1/a_1}$ and $\overline{1/a_1 + 1/a_2}$ obviously have mirror symmetry, as do the strips for continued fractions $\overline{1/a_1 + 1/a_2 + 1/a_3}$ if two of the numbers a_1, a_2, a_3 are equal.

Now let us see why this construction always works. Starting with a periodic line in the dual tree of the Farey diagram, the construction produces a quadratic form $ax^2 + bxy + cy^2$ that factors as $a(x - \alpha y)(x - \overline{\alpha}y)$ where α and $\overline{\alpha}$ lie at the ends of the given periodic line. As we saw in the proof of Theorem 5.4, the form is hyperbolic and its separator line also has ends at α and $\overline{\alpha}$. The only thing remaining to verify is that this separator line is the same as the periodic line we started with. This is a consequence of the following general fact:

Lemma 5.5. *Given two irrational numbers α and β there is a unique line in the dual tree of the Farey diagram whose endpoints are α and β.*

Proof: To see that there is at least one line joining α and β let us look in the upper half-plane model of the Farey diagram, where the edges of the diagram are semicircles with their endpoints on the x axis. There is also such a semicircle with endpoints α and β. Call this semicircle S. Since we assume α and β are irrational, the endpoints of S are not vertices of the diagram. If S intersects some triangle in the diagram, it crosses this triangle from one edge of the triangle to another edge since it cannot intersect the same edge in more than one point. (If S intersected the edge in two points, this would mean the complete circle formed by S and its reflection across the x axis would intersect the complete circle containing the edge in at least four points, but if two circles in the plane intersect in more than two points, they must coincide, which would mean that S is an edge of the diagram, which it isn't.) The collection of all triangles in the diagram that are crossed by S forms an infinite strip in the diagram, infinite in both directions, converging to α and β at its two ends. This strip corresponds to a line in the dual tree joining α and β.

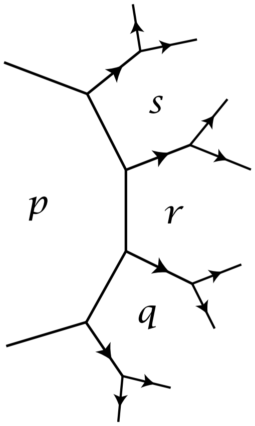
Suppose now that there are two different lines L_1 and L_2 in the dual tree that join α and β. Suppose first that L_1 and L_2 have no edges in common. Then there is an edge in the dual tree such that removing this edge from the tree produces two pieces, one containing L_1 and the other containing L_2. Dual to this removed edge of the tree is an edge E in the Farey diagram (we have in mind the circular Farey diagram now) with L_1 lying on one side of E and L_2 lying on the other side. Since the endpoints of E are rational numbers on the boundary circle of the Farey diagram, they must be distinct from the endpoints of L_1 and L_2 which are the irrational numbers α and β.

Since L_1 and L_2 lie on opposite sides of E, this means the endpoints of L_1 and L_2 must be four distinct points, two on each side of E. This contradicts the assumption that both L_1 and L_2 join α to β. Thus the possibility that L_1 and L_2 have no edges in common cannot occur.

The remaining possibility is that L_1 and L_2 have at least one edge in common. Since we assume L_1 is not equal to L_2 this implies that there is an edge e in the intersection of L_1 and L_2 where L_1 and L_2 diverge, so at one end of e the two abutting edges are e_1 lying in L_1 and e_2 lying in L_2. Dual to e, e_1, and e_2 are the three edges of one triangle of the Farey diagram. Complementary to this triangle are three pieces of the Farey diagram, each of which contains at least one end of one of the lines L_1 and L_2. This means that L_1 and L_2 together have at least three ends, but this contradicts our assumption that the ends of L_1 and L_2 are the two numbers α and β. □

Elliptic Forms

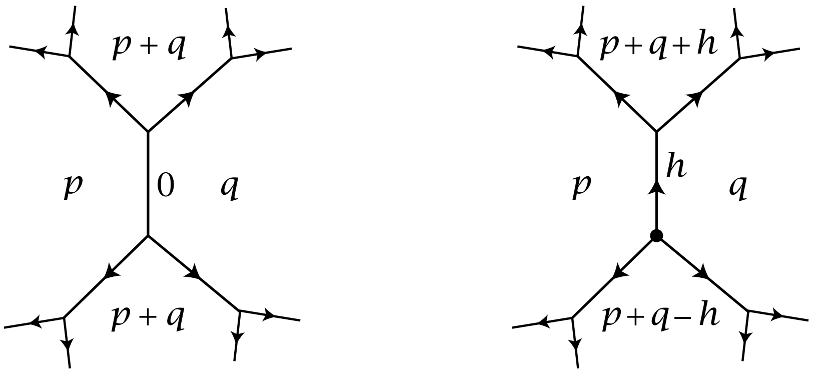
An elliptic quadratic form $Q(x,y)$ takes on only positive or only negative values at integer pairs $(x,y) \neq (0,0)$. The positive and negative cases are equivalent since one can switch from one to the other just by putting a minus sign in front of Q. Thus it suffices to consider the case that Q takes on only positive values, and we will assume we are in this case from now on. We will also generally assume when we look at topographs of elliptic forms that the orientations of the edges are chosen so as to give positive h-values, unless we state otherwise.



Let p be the minimum value taken on by Q, and consider a region of the topograph where Q takes the value p. All the edges having one endpoint at this region are oriented away from the region, by the arithmetic progression rule and the assumption that p is the minimum value of Q. The monotonicity property then implies that all edges farther away from the p region are also oriented away from the region, and the values of Q increase as one moves away from the region.

For the edges making up the border of the p region we know that the h-labels on these edges form an arithmetic progression with increment $2p$, provided that we temporarily re-orient these edges so that they all point in the same direction. There are two possibilities for this arithmetic progression:

(I) Some edge bordering the p region has the label $h = 0$. The topograph then has the form shown in the first figure below, with the orientations on edges that give positive h-labels. An example of such a form is $px^2 + qy^2$. We call the 0-labeled edge a *source edge* since all other edges are oriented away from this edge.

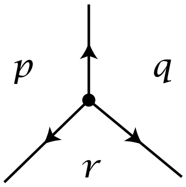


This takes care of the first case. The second case is:

(II) No edge bordering the p region has label $h = 0$. Since the labels on these edges form an arithmetic progression, there must be some vertex where the terms in the progression change sign. Then when we orient the edges to give positive h-labels, all three edges meeting at this vertex will be oriented away from the vertex, as in the second figure above. We call this a *source vertex* since all edges in the topograph are oriented away from this vertex.

The fact that the three edges leading from a source vertex all point away from the vertex is equivalent to the three triangle inequalities

$$p < q + r \qquad q < p + r \qquad r < p + q$$



In the case of a source edge one of these inequalities becomes an equality $r = p + q$.

Proposition 5.6. *Elliptic forms have negative discriminant.*

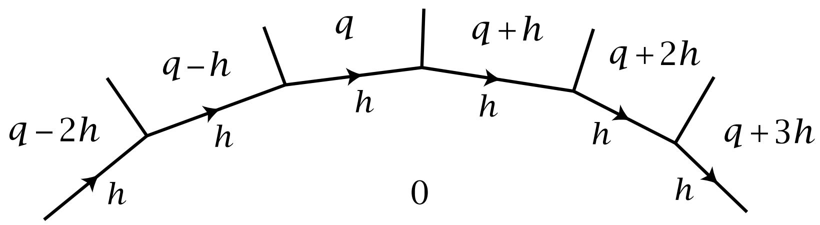
Proof: In the case of a source edge with the label $h = 0$ separating regions labeled p and q, the discriminant is $\Delta = h^2 - 4pq = -4pq$, which is negative. In the case of a source vertex with adjacent regions labeled p, q, r, the edge between the p and q regions is labeled $h = p + q - r$ so we have

$$\begin{aligned}\Delta = h^2 - 4pq &= (p + q - r)^2 - 4pq \\ &= p^2 + q^2 + r^2 - 2pq - 2pr - 2qr \\ &= p(p - q - r) + q(q - p - r) + r(r - p - q)\end{aligned}$$

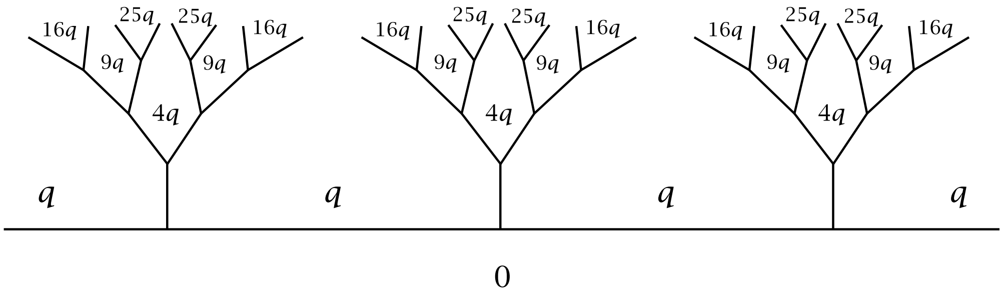
In the last line the three quantities in parentheses are negative by the triangle inequalities, so Δ is negative. □

Parabolic and 0-Hyperbolic Forms

These are the forms whose topograph has at least one region labeled 0. By the second arithmetic progression rule, each edge adjacent to the 0 region has the same label h, and the labels on the regions adjacent to the 0 region form an arithmetic progression. The discriminant is $\Delta = h^2$, a square.

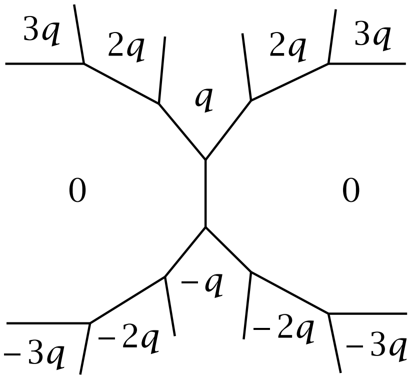


A special case is $h = 0$. Then the topograph is as shown in the next figure, and the form is parabolic with discriminant $\Delta = h^2 = 0$. Notice that the topograph is periodic along the 0 region since it consists of the same tree pattern repeated infinitely often.

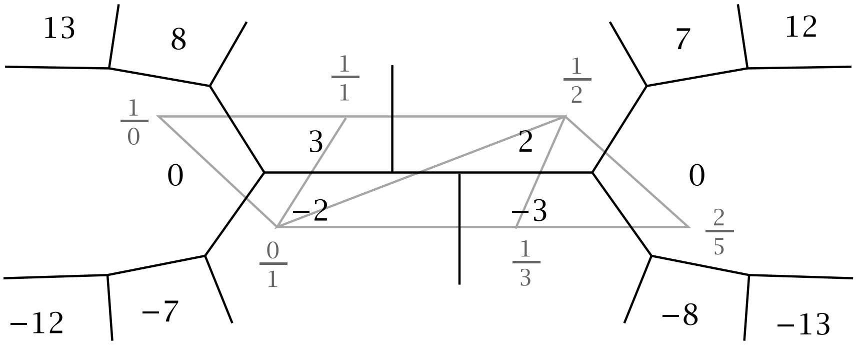


An example of a form with this topograph is $Q(x,y) = qx^2$. Notice that q is uniquely determined by the topograph since it is the value of the form closest to 0, both algebraically in terms of absolute value and geometrically in the topograph.

The remaining case is that h is nonzero, so the discriminant $\Delta = h^2$ is a positive square. The arithmetic progression of values of Q adjacent to the 0 region is not constant, so it includes both positive and negative numbers, and hence Q is 0-hyperbolic. If the arithmetic progression includes the value 0, this gives a second 0 region adjacent to the first one, and the topograph is as shown at the right. This is the topograph of the form $Q(x,y) = qxy$, with the two 0 regions at $x/y = 1/0$ and $0/1$.



If the arithmetic progression of values of Q adjacent to the 0 region does not include 0, there will be an edge separating the positive from the negative values in the progression. We can extend this separating edge to a line of separating edges as we did with hyperbolic forms, but the extension will eventually have to terminate with a second 0 region, otherwise the reasoning we used in the hyperbolic case would yield two edges along this line having the same h and the same positive and negative labels on the two adjacent regions, which would force the line to be periodic and hence extend infinitely far in both directions, which is impossible since it began at a 0 region at one end. Thus the topograph contains a finite separator line connecting two 0 regions. An example of such a form is $Q(x,y) = qxy - py^2 = (qx - py)y$ which has the value 0 at $x/y = 1/0$ and at $x/y = p/q$. Here we must have $|q| > 1$ for the two 0 regions to be nonadjacent. The separator line follows the strip of triangles in the Farey diagram corresponding to the continued fraction for p/q. For example, for $p/q = 2/5$ the topograph of the form $5xy - 2y^2 = (5x - 2y)y$ is the following:



This completes our description of what parabolic and 0-hyperbolic forms look like. As we have seen, the discriminants of these forms are squares. The converse is also true:

Proposition 5.7. *If the discriminant of a form $Q(x,y)$ is a square, then $Q(x,y) = 0$ for some pair of integers $(x,y) \neq (0,0)$ so Q is either parabolic or 0-hyperbolic.*

Proof: Suppose first that the form $Q(x,y) = ax^2 + bxy + cy^2$ happens to have $a = 0$. Then $Q(1,0) = 0$ so we are done in this case (and note that $\Delta = b^2$, a square). So we can assume that $a \neq 0$. The equation $aX^2 + bX + c = 0$ then has roots $X = (-b \pm \sqrt{b^2 - 4ac})/2a$. If $b^2 - 4ac$ is a square, this means the roots are rational. If $X = p/q$ is a rational root then $a(p/q)^2 + b(p/q) + c = 0$ and hence $ap^2 + bpq + cq^2 = 0$ so Q takes the value 0 at a pair (p,q) with $q \neq 0$. □

In particular, this shows the discriminant of a hyperbolic form is not a square. Since we showed earlier that a hyperbolic form has positive discriminant, this completes the characterization of the four types of forms in terms of their discriminants.

Equivalence of Forms

In the pictures of topographs we have drawn, we often omit the fractional labels x/y for the regions in the topograph since the more important information is often just the values $Q(x,y)$ of the form. This leads to the idea of considering two quadratic forms to be equivalent if their topographs "look the same" when the labels x/y are disregarded. For a precise definition, one can say that quadratic forms Q_1 and Q_2 are *equivalent* if there is a vertex v_1 in the topograph of Q_1 and a vertex v_2 in the topograph of Q_2 such that the values of Q_1 in the three regions surrounding v_1 are equal to the values of Q_2 in the three regions surrounding v_2. Since the three values around a vertex determine all the other values in a topograph, this guarantees that the topographs look the same everywhere, if the labels x/y are omitted.

An alternative definition of equivalence of forms would be to say that two forms are equivalent if there is a linear fractional transformation in $LF(\mathbb{Z})$ that takes the topograph of one form to the topograph of the other form. This is really the same as the first definition since there is a vertex of the topograph in the center of each triangle of the Farey diagram and we know that elements of $LF(\mathbb{Z})$ are determined by where they send a triangle, so if two topographs each have a vertex surrounded by the same triple of numbers, there is an element of $LF(\mathbb{Z})$ taking one topograph to the other, and conversely.

A topograph and its mirror image correspond to equivalent forms since the mirror image topograph has the same three labels around each vertex as at the corresponding vertex of the original topograph. For example, switching the variables x and y reflects the circular Farey diagram across its vertical axis and hence reflects the topograph of a form $Q(x,y)$ to the topograph of the equivalent form $Q(y,x)$. As another example, the forms $ax^2+bxy+cy^2$ and $ax^2-bxy+cy^2$ are equivalent since they are related by changing (x,y) to $(-x,y)$, reflecting the Farey diagram across its horizontal axis, with a corresponding reflection of the topograph.

For parabolic forms it is easy to describe what all the different equivalence classes are since we have seen exactly what their topographs look like: There is a single region labeled 0 and all the regions adjacent to this have the same label q, which can be any integer. The integer q thus determines the equivalence class, so there is one equivalence class of parabolic forms for each integer q, with the form qx^2 being one element of this equivalence class.

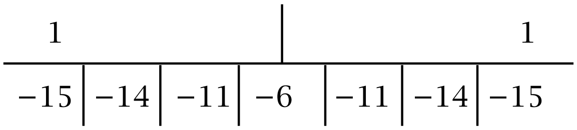
Parabolic forms are the ones with discriminant zero, but for the other three types of forms something different happens:

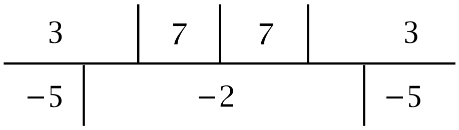
Theorem 5.8. *There are only a finite number of equivalence classes of forms with a given nonzero discriminant.*

Proof: Consider first the case of forms of positive discriminant. These are either hyperbolic or 0-hyperbolic. Hyperbolic forms have a separator line. For an edge in the separator line labeled h with adjacent regions labeled $p>0$ and $-q<0$ we have $\Delta = h^2+4pq$, so each of the quantities $|h|$, p, and q is bounded in size by Δ. This means that for fixed Δ there are only finitely many possibilities for h, p, and q for each edge of the separator line, hence just finitely many possible combinations of h, p, and $-q$ for each edge, so there are just finitely many possibilities for the form, up to equivalence. The same reasoning applies also to 0-hyperbolic forms that have a separating edge in their topograph. The only ones that do not have a separating edge are the ones with two adjacent regions labeled 0. In this case the edge separating these two regions has $h^2=\Delta$ since $p=q=0$ for this edge. Hence $h=\pm\sqrt{\Delta}$ and we can change the sign by changing the orientation of the edge. Thus the form is determined up to equivalence by Δ.

For forms of negative discriminant we can assume we are dealing with positive elliptic forms since a form Q and its negative $-Q$ have the same discriminant. If a positive elliptic form has a source edge in its topograph, this edge has $h = 0$ so $\Delta = -4pq$ where p and q are the values of Q in the adjacent regions. For fixed Δ there are only finitely many choices of p and q satisfying $\Delta = -4pq$. Hence, up to equivalence there are only finitely many positive elliptic forms of discriminant Δ having a source edge. In the other case of a source vertex surrounded by values p, q, r of the form, we obtained the formula $\Delta = p(p-q-r) + q(q-p-r) + r(r-p-q)$ with the three quantities in parentheses being negative, so $p + q + r \le |\Delta|$ and hence there are only finitely many possibilities for p, q, and r for each Δ. □

As an example, let us determine all the quadratic forms of discriminant 60, up to equivalence. Two obvious forms of discriminant 60 are $x^2 - 15y^2$ and $3x^2 - 5y^2$, whose separator lines consist of periodic repetitions of the following two patterns:





From the topographs it is apparent that these two forms are not equivalent, and also that the negatives of these two forms, $-x^2 + 15y^2$ and $-3x^2 + 5y^2$, give two more inequivalent forms, for a total of four equivalence classes so far. To see whether there are others we use the formula $\Delta = 60 = h^2 + 4pq$ relating the values p and $-q$ along an edge labeled h in the separator line, with $p > 0$ and $q > 0$. The various possibilities are listed in the table below. Note that the equation $60 = h^2 + 4pq$ implies that h has to be even. (In fact, the formula $\Delta = h^2 - 4ac$ implies that h and Δ always have the same parity.)

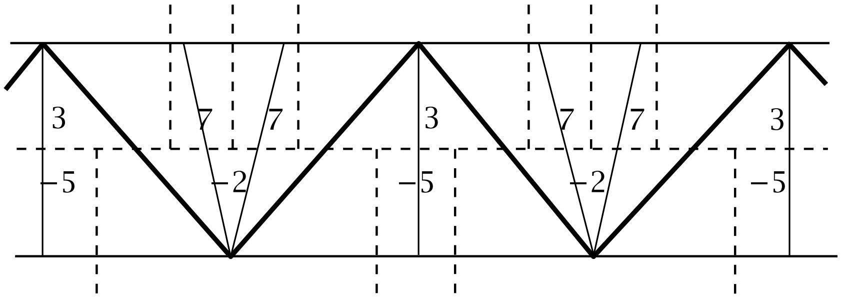
h	pq	(p,q)
0	15	$(1,15)$, $(3,5)$, $(5,3)$, $(15,1)$
2	14	$(1,14)$, $(2,7)$, $(7,2)$, $(14,1)$
4	11	$(1,11)$, $(11,1)$
6	6	$(1,6)$, $(2,3)$, $(3,2)$, $(6,1)$

Each pair of values for (p,q) in the table occurs at some edge along the separator line in one of the two topographs shown above, or the negatives of these topographs. Hence every form of discriminant 60 is equivalent to one of these four. If it had not been true that all the possibilities in the table occurred in the topographs of the forms we started with, we could have used these other possibilities for h, p, and q to generate new topographs and hence new forms, eventually exhausting all the finitely many possibilities.

The procedure in this example works for all hyperbolic forms. One makes a list of all the solutions of $\Delta = h^2 + 4pq$ with $p > 0$ and $q > 0$, then one constructs separator lines that realize all the resulting pairs (p,q). The different separator lines correspond exactly to the different equivalence classes of forms of discriminant Δ. Each solution (h,p,q) gives a form $px^2 + hxy - qy^2$. These are organized into "cycles" corresponding to the pairs $(p, -q)$ occurring along one of the periodic separator lines. Thus in the preceding example with $\Delta = 60$ the 14 pairs (p, q) in the table give rise to the four cycles along the four different separator lines.

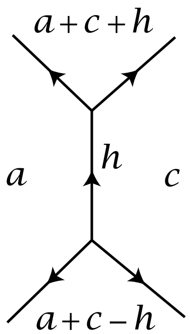
Note that a hyperbolic form $ax^2 + bxy + cy^2$ belongs to one of these cycles for the discriminant $\Delta = b^2 - 4ac$ exactly when $a > 0$ and $c < 0$ since a and c are the numbers p and $-q$ lying on opposite sides of an edge of the separator line (namely when $x/y = 1/0$ or $0/1$).

If we superimpose the separator line of a hyperbolic form on the associated infinite strip in the Farey diagram, we see that the forms within a cycle correspond to the edges of the Farey diagram that lie in the strip and join one border of the strip to the other. For example, for the form $3x^2 - 5y^2$ we obtain the following picture, with fans of two triangles alternating with fans of three triangles:



The number of forms within a given cycle can be fairly large in general. The situation can be improved somewhat by considering only the "most important" forms in the cycle, namely the forms that correspond to those edges in the strip that separate pairs of adjacent fans, indicated by heavier lines in the figure. In terms of the topograph itself these are the edges in the separator line whose two endpoints have edges leading away from the separator line on opposite sides. The forms corresponding to these edges are traditionally called the *reduced* forms within the given equivalence class. In the example of discriminant 60 these are the forms with $(p, q) = (1, 6)$, $(6, 1)$, $(3, 2)$, and $(2, 3)$. These are the forms $x^2 + 6xy - 6y^2$, $6x^2 + 6xy - y^2$, $3x^2 + 6xy - 2y^2$, and $2x^2 + 6xy - 3y^2$.

Now let us consider the analogous problem of finding all the equivalence classes of positive elliptic quadratic forms of a given discriminant. This turns out to be a simpler process since it can be done without drawing any topographs. At a source vertex or edge in the topograph for such a form Q let the smaller two of the three adjacent values of Q be $a \le c$, with the edge between them labeled $h \ge 0$, so that the third adjacent value of Q is $a + c - h$. The form is then equivalent to the form $ax^2 + hxy + cy^2$. Since a and c are the smallest values of Q we have $a \le c \le a + c - h$, and the latter inequality implies that $h \le a$. Thus we have the inequalities $0 \le h \le a \le c$. Note that these inequalities



imply the three triangle inequalities at the source vertex or edge: $a+c-h \le a+c$, $a < c+(a+c-h)$, and $c < a+(a+c-h)$. For the discriminant $\Delta = -D$ we have $D = 4ac - h^2$, so we are seeking solutions of

$$4ac = h^2 + D \qquad \text{with} \quad 0 \le h \le a \le c$$

The number h must have the same parity as D, and we can bound the choices for h by the inequalities $4h^2 \le 4a^2 \le 4ac = D + h^2$ which imply $3h^2 \le D$, or $h^2 \le D/3$. Thus every positive elliptic form is equivalent to a form $ax^2+hxy+cy^2$ with $4ac = h^2+D$ and $0 \le h \le a \le c$. An elliptic form satisfying these conditions is called *reduced.* Two different reduced elliptic forms with the same discriminant are never equivalent since a and c are the labels on the two regions in the topograph where the form takes its smallest values, and h is determined by a, c, and D via the formula $4ac = h^2 + D$.

As an example, when $D = 260$ we must have h even and $h^2 \le 260/3$ so h must be $0, 2, 4, 6,$ or 8. The corresponding values of a and c that are possible can then be computed from the equation $4ac = 260+h^2$, always keeping in mind the requirement that $h \le a \le c$. The possibilities are shown in the following table:

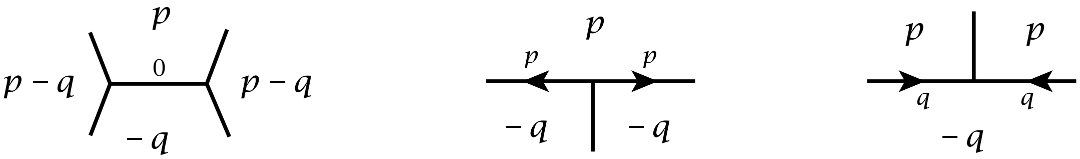
h	ac	(a,c)
0	65	$(1,65)$, $(5,13)$
2	66	$(2,33)$, $(3,22)$, $(6,11)$
4	69	—
6	74	—
8	81	$(9,9)$

Thus every positive elliptic form of discriminant -260 is equivalent to one of the reduced forms x^2+65y^2, $5x^2+13y^2$, $2x^2+2xy+33y^2$, $3x^2+2xy+22y^2$, $6x^2+2xy+11y^2$, or $9x^2+8xy+9y^2$, and no two of these reduced forms are equivalent to each other.

Symmetries

We have observed that some topographs are symmetric in various ways. To give a precise meaning to this term, let us say that a *symmetry* of a form Q (or its topograph) is a transformation T in $LF(\mathbb{Z})$ that leaves all the values of Q unchanged, so $Q(T(x,y)) = Q(x,y)$ for all pairs (x,y). For example, every hyperbolic form has a periodic separator line, which means there is a symmetry that translates the separator line along itself. If T is the symmetry translating by one period in either direction, then all the positive and negative powers of T are also translational symmetries. Strictly speaking, the identity transformation is always a symmetry but we will often ignore this trivial symmetry.

Some hyperbolic forms also have mirror symmetry, where the symmetry is reflection across a line perpendicular to the separator line. This reflector line could contain one of the edges leading off the separator line, or it could be halfway between two consecutive edges leading off the separator line on the same side. If a reflector line lies halfway between two adjacent edges leading off the separator line for a form $px^2 + hxy - qy^2$ this corresponds to having $h = 0$ as in the first figure below, so the form is just $px^2 - qy^2$.

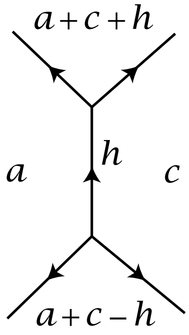


On the other hand if the reflector line contains an edge leading off the separator line then either $h = p$ or $h = q$ as in the second and third figures, so the form is $px^2 + pxy - qy^2$ or $px^2 + qxy - qy^2$. In the earlier example with discriminant $\Delta = 60$ there were fourteen forms occurring along the separator lines, and eight of these correspond to mirror symmetries: the four with $h = 0$ and the four with $(p, q) = (2, 7)$, $(7, 2)$, $(1, 6)$, and $(6, 1)$. Each of the four equivalence classes of forms contains two forms exhibiting the mirror symmetries.

For hyperbolic forms these two types of symmetries, the periodicity translations and the mirror symmetries across lines perpendicular to the separator line, are the only possible types of symmetries. This is because every symmetry must take positive values of the form to positive values, and negative values to negative values, so the symmetry must carry the separator line to itself, and it is a fairly obvious fact that all symmetries of a line are either translations along the line or reflections across some point on the line, exchanging the two ends of the line and reversing its orientation.

If the separator line has a mirror symmetry then because of periodicity there has to be at least one reflector line in each period, but in fact there are two reflector lines in each period. To see this, let τ denote the translation by one period and let ρ be a reflection across a reflector line L. If x is the point on the separator line halfway between L and $\tau(L)$, then $\tau(\rho(x)) = x$. Since $\tau\rho$ reverses orientation it must therefore be a reflection across the line through x perpendicular to the separator line, halfway between L and $\tau(L)$. Thus there are at least two reflector lines in each period. There cannot be more than two since the composition of the reflections across two adjacent reflector lines is a translation through twice the distance between the separator lines, so the distance between adjacent reflector lines must be half a period.

Some elliptic forms also have symmetries. The source vertex or edge must be taken to itself by any symmetry since the smallest values of the form occur around this one vertex or edge. It is easy to determine the symmetries of an elliptic form $ax^2 + hxy + cy^2$ that is reduced, so $0 \le h \le a \le c$. As one can see by looking at the figure to the right, symmetries occur when one or more of these three inequalities become equalities. When $h = 0$ one has a source edge and this has a mirror symmetry across the line perpendicular



to the source edge. When $a = c$ one has a mirror symmetry across the central edge. And when $h = a$ we have $a + c - h = c$ so there is a mirror symmetry across the edge separating the two regions with these labels.

Certain combinations of these equalities are also possible. If $h = 0$ and $a = c$ so the form is $a(x^2 + y^2)$ there are mirror symmetries across the source edge as well as across the line perpendicular to this edge, and the composition of these two reflections is a 180 degree rotational symmetry about the midpoint of the edge. Another possibility is that $h = a = c$ so the form is $a(x^2 + xy + y^2)$ and all three values of the form around the lower vertex in the diagram are equal. Then there is a 120 degree rotational symmetry about this source vertex as well as mirror symmetries across the three adjacent edges. These are the only combinations that can occur since we must have $0 < a$ so $0 = h = a$ is impossible.

For elliptic forms this exhausts all the possible symmetries since if we have strict inequalities $0 < h < a < c$ then the values of the form in the four regions shown in the diagram above are all distinct.

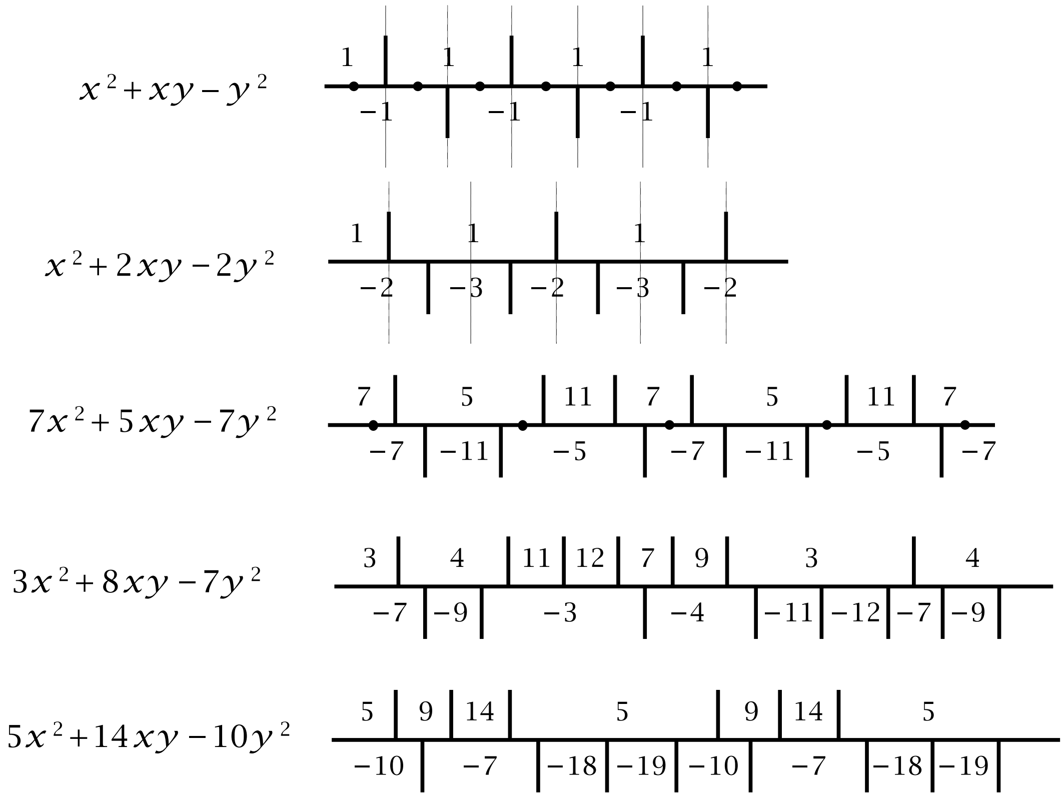
One conclusion that can be drawn from the preceding analysis is that mirror symmetries in a topograph do not occur at just a random place in the topograph. For a hyperbolic form they must occur at an edge in the separator line, and for an elliptic form they can only occur at the source vertex or edge.

Traditionally, a form whose topograph has mirror symmetry is called “ambiguous” although there is really nothing about the form that is ambiguous in the usual sense of the word, unless perhaps it is the fact that such a form is indistinguishable from its mirror image.

Among the examples of hyperbolic forms we have considered there were some whose topograph had a “symmetry” which was a glide-reflection along the separator line that had the effect of changing each value to its negative rather than preserving the values. These are not actual symmetries according to the definition above, so let us call such a transformation that takes each value of a form to its negative a *skew symmetry*. (Compare this with skew-symmetric matrices in linear algebra which equal the negative of their transpose.) Skew symmetries might also be called “anti-symmetries”.

There is one other type of skew symmetry, a 180 degree rotation about a point of the separator line. Examples of forms with this sort of skew symmetry also occurred in Chapter 4, the forms $x^2 - 13y^2$ and $10x^2 - 29y^2$.

The following pictures show forms whose separator lines have all the possible combinations of symmetries and skew symmetries. The first form has all four types: translations, mirror symmetries, glide-reflections, and rotations. The next three forms have only one type of symmetry besides translations, while the last form has only translational symmetries.



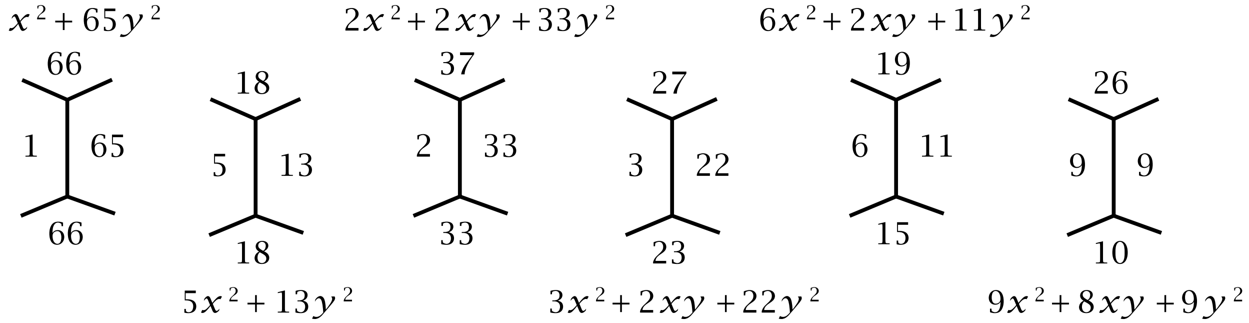
It is not possible to have two of the three non-translational symmetries without having the third since the composition of two of these symmetry types gives the third type. One can see this by considering the effect of a symmetry or skew symmetry on the orientation of the plane and the orientation of the separator line. The four possible combinations distinguish the four types of transformations according to the following chart, where + denotes orientation-preserving and − denotes orientation-reversing.

	plane orientation	line orientation
translation	+	+
rotation	+	−
glide reflection	−	+
reflection	−	−

The Class Number

If the topographs of two forms are mirror images of each other, then the forms are equivalent, according to the definitions we have given. Of course, if a topograph has mirror symmetry then it is the same as its mirror image, but when there is no mirror symmetry it is sometimes desirable to distinguish a topograph from its mirror image. In order to do this one uses a more refined notion of equivalence in which two forms are considered equivalent only if there is an orientation-preserving transformation in $LF(\mathbb{Z})$ taking the topograph of one form to the topograph of the other. In this case the forms are called *properly equivalent*. This more refined notion might also be called “oriented equivalence”. For forms with mirror symmetry, an equivalence that reverses orientation can always be converted to one that preserves orientation by composing it with a mirror symmetry, so there is no distinction between the two concepts in this case. But a form without mirror symmetry is not properly equivalent to its mirror image.

To illustrate the distinction, let us look at the earlier example of discriminant $\Delta = -260$ where we saw that there were six equivalence classes of forms. Small portions of the topographs of these six elliptic forms are shown below.



In the first two topographs the central edge is a source edge, and in the other four the lower vertex is a source vertex. Whenever there is a source edge the topograph has a mirror symmetry across a line perpendicular to the source edge. When there is source vertex there is a mirror symmetry only when at least two of the three surrounding values of the form are equal, as in the third and sixth topographs above, but not the fourth or fifth topographs. Thus the mirror images of the fourth and fifth topographs correspond to two more quadratic forms which are not equivalent to them under any orientation-preserving transformation. To obtain an explicit formula for the mirror image forms we can just interchange the a and c terms in $ax^2+bxy+cy^2$, which corresponds to interchanging x and y, reflecting the topograph across a vertical line. Alternatively we could change the sign of b, corresponding to changing the sign of either x or y and thus reflecting the topograph across a horizontal line.

The net result of all this is that with the more refined notion of proper equivalence there are eight proper equivalence classes of forms of discriminant -260. In general, if the number of equivalence classes in a given discriminant whose topographs do not have mirror symmetry is r, then the number of proper equivalence classes is r more than the number of equivalence classes.

Another refinement in the classification of quadratic forms is to restrict attention just to forms that are not multiples of other forms. In other words, one considers only the forms $ax^2+bxy+cy^2$ for which a, b, and c have no common divisor greater than 1. Such forms are called *primitive*. Multiplying a form by a constant d multiplies its discriminant by d^2, so non-primitive forms of discriminant Δ exist exactly when Δ is a square times another discriminant. For example, when $\Delta = -12 = 4(-3)$ one has the primitive form x^2+3y^2 as well as the non-primitive form $2x^2+2xy+2y^2$.

A discriminant which is not equal to a square times another discriminant is called a *fundamental discriminant*. For example, 8 is a fundamental discriminant even though it is divisible by a square, 4, since the other factor 2 is not the discriminant of any form, as it is not congruent to 0 or 1 mod 4. Fundamental discriminants are those for which every form is primitive.

The number of proper equivalence classes of primitive forms of a given discriminant is called the *class number* for that discriminant, where in the case of elliptic forms one considers only those with positive values. The class number equals the number of (non-proper) equivalence classes if every form of that discriminant has mirror symmetry and there are no non-primitive forms. In particular, if all forms of the given discriminant are equivalent, then the class number is 1 since in this case all forms are equivalent to the principal form, and this is primitive and has mirror symmetry. For fundamental discriminants the converse is also true: class number 1 implies all forms of that discriminant are equivalent since they are all properly equivalent. An example when the class number is 1 but not all forms are equivalent is the non-fundamental discriminant $\Delta = -12$, where all forms are equivalent to either $x^2 + 3y^2$ or $2x^2 + 2xy + 2y^2$.

The question of which discriminants have class number 1 has been much studied. For elliptic forms the following nine fundamental discriminants have class number 1:

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

In addition there are four more which are not fundamental: $-12,\ -16,\ -27,\ -28$. It was conjectured by Gauss around 1800 that there are no other negative discriminants of class number 1. Over a century later in the 1930s it was shown that there is at most one more, and then in the 1950s and 60s Gauss's conjecture was finally proved completely.

The situation for positive discriminants with class number 1 is not as well understood. Computations show that there are many more such discriminants, even among fundamental discriminants, and the evidence seems to suggest there are in fact infinitely many. However, this has not been proved.

For each of the negative discriminants of class number 1 listed above it is very easy to check that all forms are equivalent. For example when $\Delta = -163$ we must have h odd with $h^2 \le 163/3$ so the only possibilities are $h = 1, 3, 5, 7$. From the equation $4ac = 163 + h^2$ the corresponding values of ac are $41, 43, 47, 53$ which all happen to be primes, and since $a \le c$ this forces a to be 1 in each case. But since $h \le a$ this means h must be 1, and we obtain the single quadratic form $x^2 + xy + 41y^2$.

The corresponding polynomial $x^2 + x + 41$ has a curious property discovered by Euler: For each $x = 0, 1, 2, 3, \cdots, 39$ the value of $x^2 + x + 41$ is a prime number. Here are these forty primes:

41 43 47 53 61 71 83 97 113 131 151 173 197 223 251 281 313 347 383 421
461 503 547 593 641 691 743 797 853 911 971 1033 1097 1163 1231 1301
1373 1447 1523 1601

Notice that the successive differences between these numbers are $2, 4, 6, 8, 10, \cdots$. The next number in the sequence after 1601 would be $1681 = 41^2$, not a prime. (Write $x^2 + x + 41$ as $x(x+1) + 41$ to see why $x = 40$ must give a nonprime value.) A similar thing happens for the other values of D. The nontrivial cases are listed in the table below.

D		
7	$x^2 + x + 2$	2
11	$x^2 + x + 3$	3 5
19	$x^2 + x + 5$	5 7 11 17
43	$x^2 + x + 11$	11 13 17 23 31 41 53 67 83 101
67	$x^2 + x + 17$	17 19 23 29 37 47 59 73 89 107 127 149 173 199 227 257

It is interesting that these lists, including the one for $x^2 + x + 41$, account for all primes less than 100 except 79.

Just for fun, suppose one asks about the next 40 values of $x^2 + x + 41$ after the value 41^2 when $x = 40$. The next value, when $x = 41$, is $1763 = 41 \cdot 43$, also not a prime. After this the next two values are primes, then comes $2021 = 43 \cdot 47$, then four primes, then $2491 = 47 \cdot 53$, then six primes, then $3233 = 53 \cdot 61$, then eight primes, then $4331 = 61 \cdot 71$, then ten primes, then $5893 = 71 \cdot 83$. This last number was for $x = 76$, and the next four values are prime as well for $x = 77,\ 78,\ 79,\ 80$, completing the second forty values. But then the pattern breaks down when $x = 81$ where one gets the value $6683 = 41 \cdot 163$. Thus, before the breakdown, not only were we getting sequences of 2, 4, 6, 8, 10 primes but the non-prime values were the products of two successive terms in the original sequence of prime values $41,\ 43,\ 47,\ 53,\ 61,\ \cdots$. All this seems quite surprising, even if the nice patterns do not continue forever.

We usually focus on elliptic and hyperbolic forms since their behavior is much more interesting than for the other two types. Parabolic forms are extremely simple since they are all equivalent to one-variable forms ax^2, and different values of a give different equivalence classes since a is the value closest to 0. Just slightly more subtle are 0-hyperbolic forms, whose classification we now describe.

As we saw in our initial discussion of 0-hyperbolic forms, their topographs contain two regions labeled 0 and the labels on the regions adjacent to each 0-region form an arithmetic progression with increment q, where the discriminant is $\Delta = q^2$. These arithmetic progressions can also be thought of as congruence classes mod q. The sign of q does not affect the arithmetic progression, so we may assume it is positive. Either one of the two arithmetic progressions adjacent to a 0-region determines the form up to equivalence since two successive terms in the progression together with the 0 in the adjacent region give the three values of the form around a vertex in the topograph.

The form $qxy - py^2$ has discriminant q^2 and has $-p$ as one term of the arithmetic progression adjacent to the 0-region $x/y = 1/0$, namely in the region $x/y =$

$0/1$. Thus every 0-hyperbolic form of discriminant q^2 is equivalent to one of these forms $qxy - py^2$. Since only the mod q value of p affects the arithmetic progression, we may assume $0 \le p < q$. The number of equivalence classes of 0-hyperbolic forms of discriminant q^2 is therefore at most q. However, the number of equivalence classes could be smaller since each form has two 0-regions and hence two arithmetic progressions, which could be the same or different. Since either arithmetic progression determines the form, if the two progressions are the same then the topograph must have a mirror symmetry interchanging the two 0-regions. This always happens if the two 0-regions touch, for example, which is the case $p = 0$ so the form is qxy. If we let r denote the number of forms without mirror symmetry then the number of equivalence classes of 0-hyperbolic forms of discriminant q^2 is $q - r$. On the other hand, the number of proper equivalence classes is simply q.

It is possible to figure out exactly when there is a mirror symmetry interchanging the 0-regions. As we observed in the earlier discussion of 0-hyperbolic forms, the second 0-region for $qxy - py^2$ is at $x/y = p/q$ and the separator line (in the cases when the 0-regions do not touch) runs down the middle of the strip in the Farey diagram for the continued fraction for p/q. Mirror symmetry in the topograph is equivalent to mirror symmetry in this strip, which is equivalent in turn to the terms in the continued fraction forming a palindrome with an odd number of terms (since the strip must have an odd number of fans if it has mirror symmetry). As we saw in Chapter 2, reversing the order of the terms in a continued fraction for p/q changes p to p' where $pp' \equiv \pm 1 \bmod q$, with the sign being $+$ when the continued fraction has an odd number of terms. This is assuming that p and q are coprime so that p/q is in lowest terms. Thus in these cases the condition for mirror symmetry is $p^2 \equiv 1 \bmod q$. This always has the solutions $p \equiv \pm 1 \bmod q$, and if q is prime these are the only solutions. For nonprime q there can be other solutions. For example when $q = 15$ the solutions are $p \equiv \pm 1, \pm 4 \bmod 15$.

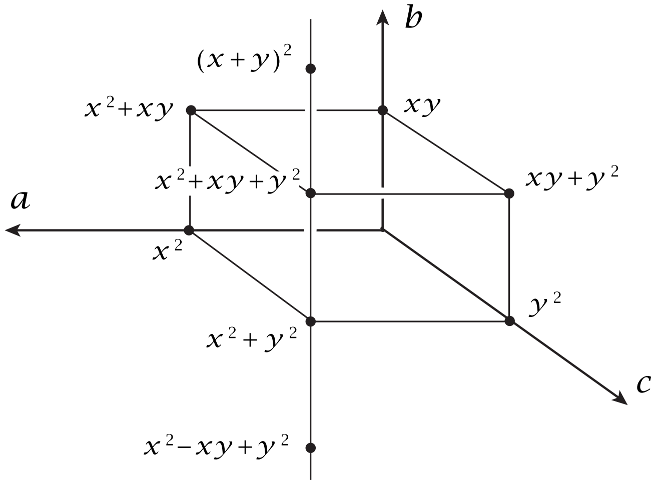
In the cases that p and q have greatest common divisor $d > 1$ we can factor d out of the form $qxy - py^2$ to get a 0-hyperbolic form of smaller discriminant q^2/d^2 which can be checked for mirror symmetry in the same way.

It is possible for a 0-hyperbolic form to have a 180 degree rotational skew symmetry. This happens when the strip along the separating line is palindromic and has an even number of fans, which means $p^2 \equiv -1 \bmod q$. The only time the same form has both a mirror symmetry and a rotational skew symmetry is when $1 \equiv -1 \bmod q$ so q must be 1 or 2.

Charting All Forms

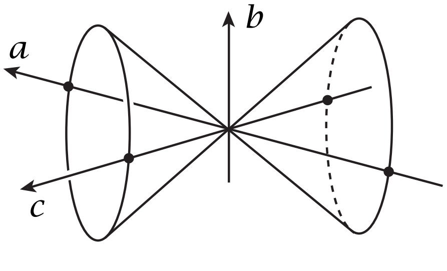
We have used the Farey diagram to study individual quadratic forms through their topographs, but the diagram also appears in another way when one seeks a global picture of all forms simultaneously, as we will now see.

Quadratic forms are defined by formulas $ax^2+bxy+cy^2$, and our point of view will be to regard the coefficients a, b, and c as parameters that vary over all integers independently. It is natural to consider the triples (a,b,c) as points in 3-dimensional Euclidean space $\mathbb{R}^3$, and more specifically as points in the integer lattice $\mathbb{Z}^3$ consisting of points (a,b,c) whose coordinates are integers. We will exclude the origin $(0,0,0)$ since this corresponds to the trivial form that is identically zero. Instead of using the traditional (x,y,z) as coordinates for $\mathbb{R}^3$ we will use (a,b,c), but since a and c play a symmetric role as the coefficients of the squared terms x^2 and y^2 in a form $ax^2+bxy+cy^2$ we will position the a and c axes in a horizontal plane, with the b axis vertical, perpendicular to the ac plane. Here is a figure showing the location of a few forms:



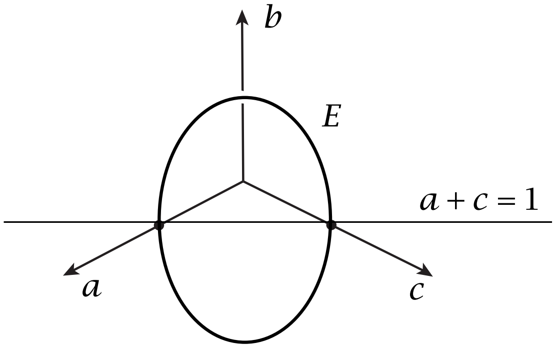
Along each ray starting at the origin and passing through a lattice point (a,b,c) there are infinitely many lattice points (ka,kb,kc) for positive integers k. If a, b, and c have a common divisor greater than 1 we can first cancel this common divisor to get a primitive triple (a,b,c) corresponding to a primitive form $ax^2+bxy+cy^2$, with all the other lattice points on the ray through (a,b,c) being the positive integer multiples of this. Thus primitive forms correspond exactly to rays from the origin passing through lattice points. These are the same as rays passing through points (a,b,c) with rational coordinates since denominators can always be eliminated by multiplying the coordinates by the least common multiple of the denominators.

Since the discriminant $\Delta = b^2-4ac$ plays such an important role in the classification of forms, let us see how this fits into the picture in (a,b,c) coordinates. When b^2-4ac is zero we have the special class of parabolic forms, and the points in $\mathbb{R}^3$ satisfying the equation $b^2-4ac=0$ form a double cone with the common vertex of the two cones at the origin. The double cone intersects the ac plane in the a and c axes. The central axis of the double cone itself is the line $a=c$ in the ac plane. Points (a,b,c) inside either cone



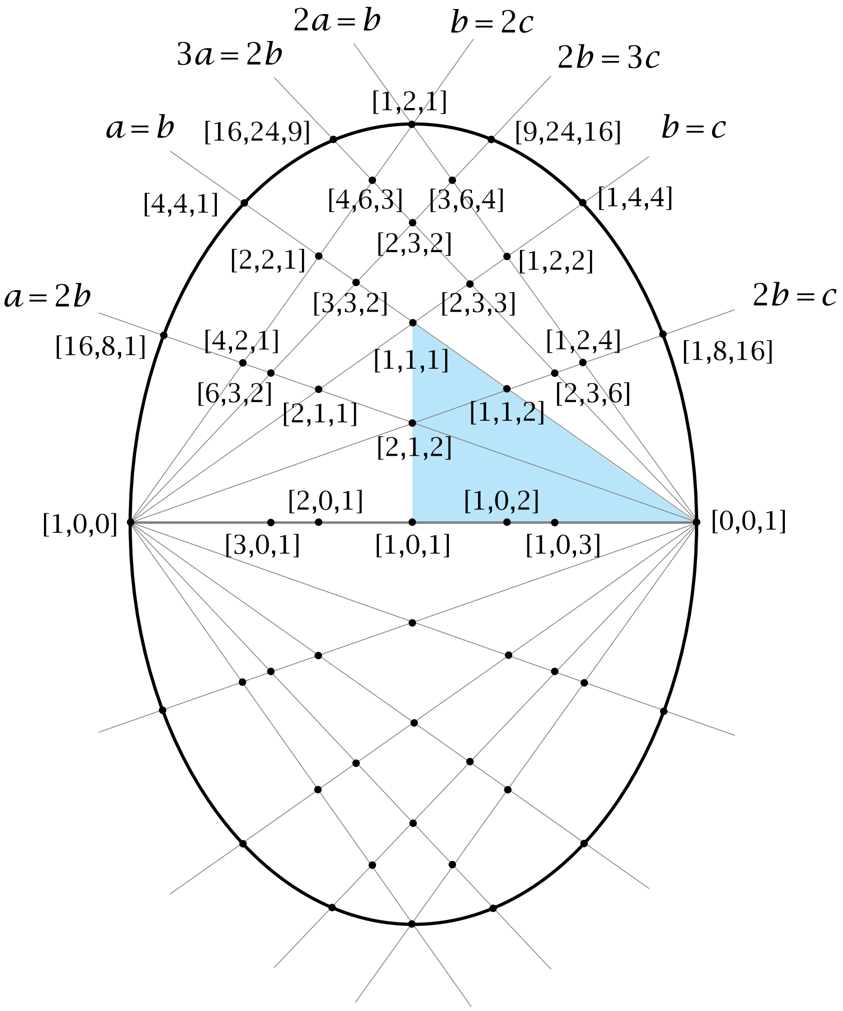
have $b^2 - 4ac < 0$ so the lattice points inside the cones correspond to elliptic forms. Positive elliptic forms have $a > 0$ and $c > 0$ so they lie inside the cone projecting to the first quadrant of the ac plane. We call this the *positive cone*. Inside the other cone are the negative elliptic forms, those with $a < 0$ and $c < 0$. Outside the cones is a single region consisting of points with $b^2 - 4ac > 0$ so the lattice points here correspond to hyperbolic forms and 0-hyperbolic forms.

If one slices the positive cone via a vertical plane perpendicular to the axis of the cone such as the plane $a + c = 1$, then the intersection of the cone with this plane is an ellipse which we denote E.



The top and bottom points of E are $(a, b, c) = (\frac{1}{2}, \pm 1, \frac{1}{2})$ so its height is 2. The left and right points of E are $(1, 0, 0)$ and $(0, 0, 1)$ so its width is $\sqrt{2}$. Thus E is somewhat elongated vertically. If we wanted, we could compress the vertical coordinate to make E a circle, but there is no special advantage to doing this.

When we project a lattice point (a, b, c) corresponding to a primitive positive elliptic form along the ray to the origin passing through (a, b, c), this ray intersects the plane $a + c = 1$ in the point $(a/(a + c), b/(a + c), c/(a + c))$ since the sum of the first and third coordinates of this point is 1. This point lies inside the ellipse E and has rational coordinates. Conversely, every point inside E with rational coordinates is the radial projection of a unique primitive positive elliptic form, obtained by multiplying the coordinates of the point by the least common multiple of their denominators. Thus the rational points inside E parametrize primitive positive elliptic forms. We shall use the notation $[a, b, c]$ to denote both the form $ax^2 + bxy + cy^2$ and the corresponding rational point $(a/(a + c), b/(a + c), c/(a + c))$ inside E. The figure below shows some examples, including a few parabolic forms on E itself.

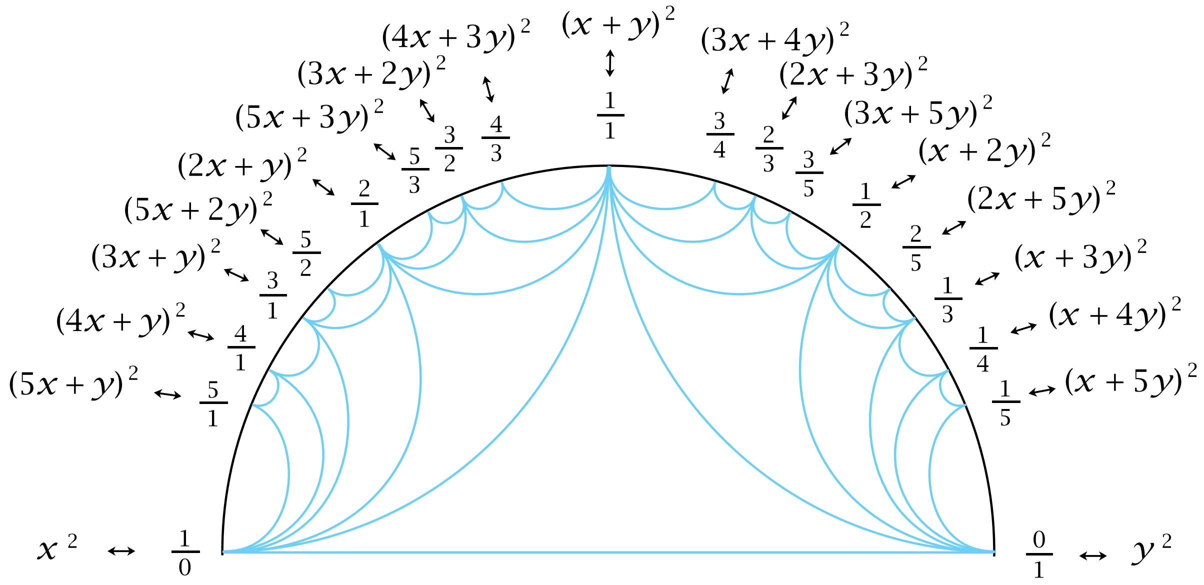


In this figure the lines radiating out from the points $[1,0,0]$ and $[0,0,1]$ consist of the points $[a,b,c]$ with a fixed ratio a/b or b/c. The ratios a/c are fixed along vertical lines. Two out of three of these ratios determine the third since $\frac{a}{b} \cdot \frac{b}{c} = \frac{a}{c}$.

Of special interest are the reduced primitive elliptic forms $[a,b,c]$, which are those satisfying $0 \le b \le a \le c$ where a, b, and c have no common divisor. These correspond to the points inside the ellipse lying in the triangle with vertices $[1,1,1]$, $[1,0,1]$, and $[0,0,1]$, whose edges correspond to one of the three inequalities $0 \le b \le a \le c$ becoming an equality, so $b = 0$ for the lower edge, $a = c$ for the vertical edge, and $a = b$ for the hypotenuse.

Just as rational points inside the ellipse E correspond to primitive positive elliptic forms, the rational points on E itself correspond to primitive positive parabolic forms. As we know, every parabolic form is equivalent to the form ax^2 for some nonzero integer a. For this to be primitive means that $a = \pm 1$, so every positive primitive parabolic form is equivalent to x^2. Equivalent forms are those that can be obtained from each other by a change of variable replacing (x,y) by $(px+qy, rx+sy)$ for some integers p,q,r,s satisfying $ps-qr = \pm 1$. For the form x^2 this means that the primitive positive parabolic forms are the forms $(px+qy)^2 = p^2x^2+2pqxy+q^2y^2$ for any pair of coprime integers p and q. In $[a,b,c]$ notation this is $[p^2, 2pq, q^2]$, defining a point on the ellipse E.

More concisely, we could label the rational point on E corresponding to the form $(px+qy)^2$ just by the fraction p/q. Thus at the left and right sides of E we have the fractions $1/0$ and $0/1$ corresponding to the forms x^2 and y^2, while at the top and bottom of E we have $1/1$ and $-1/1$ corresponding to $(x+y)^2$ and $(x-y)^2 = (-x+y)^2$.


$(4x+3y)^2$
$(x+y)^2$
$(3x+4y)^2$
$(3x+2y)^2$
$(2x+3y)^2$
$(5x+3y)^2$
$(3x+5y)^2$
$(2x+y)^2$
$(x+2y)^2$
$(5x+2y)^2$
$(2x+5y)^2$
$(3x+y)^2$
$(x+3y)^2$
$(4x+y)^2$
$(x+4y)^2$
$(5x+y)^2$
$(x+5y)^2$
$\frac{4}{3}$ $\frac{3}{2}$ $\frac{5}{3}$ $\frac{2}{1}$ $\frac{5}{2}$ $\frac{3}{1}$ $\frac{4}{1}$ $\frac{5}{1}$
$\frac{1}{1}$
$\frac{3}{4}$ $\frac{2}{3}$ $\frac{3}{5}$ $\frac{1}{2}$ $\frac{2}{5}$ $\frac{1}{3}$ $\frac{1}{4}$ $\frac{1}{5}$
$x^2 \leftrightarrow \frac{1}{0}$
$\frac{0}{1} \leftrightarrow y^2$

Note that changing the signs of both p and q does not change the form $(px+qy)^2$ or the fraction p/q. In the first quadrant of the ellipse the fractions p/q increase monotonically from $0/1$ to $1/1$ since the ratio b/c equals $2p/q$ and b is increasing while c is decreasing so $2p/q$ is increasing, and hence also p/q. Similarly in the second quadrant the values of p/q increase from $1/1$ to $1/0$ since we have $b/a = 2q/p$ which decreases as b decreases and a increases. In the lower half of the ellipse we have just the negatives of the values in the upper half since the sign of b has changed from plus to minus.

Thus the labeling of the rational points of E by fractions p/q seems very similar to the labeling of vertices in the circular Farey diagram. As we saw near the end of Chapter 1, if the Farey diagram is drawn with $1/0$ at the top of the unit circle in the xy plane, then the point labeled p/q has coordinates $(x,y) = ((2pq/(p^2+q^2),(p^2-q^2)/(p^2+q^2))$. After rotating the circle to put $1/0$ on the left side by replacing (x,y) by $(-y,x)$ this becomes $((q^2-p^2)/(p^2+q^2), 2pq/(p^2+q^2))$. Here the y-coordinate $2pq/(p^2+q^2)$ is the same as the b-coordinate of the point of E labeled p/q, namely the point $(a,b,c) = (p^2/(p^2+q^2), 2pq/(p^2+q^2), q^2/(p^2+q^2))$. Since the vertical coordinates of points in either the left or right half of the circle or the ellipse E determine the horizontal coordinates uniquely, this means that the labeling of points of E by fractions p/q is really the same as in the circular Farey diagram.

Let us return now to the general picture of how forms $ax^2+bxy+cy^2$ are represented by points (a, b, c) in $\mathbb{R}^3$. As we know, a change of variables by a linear transformation T sending (x, y) to $T(x, y) = (px + qy, rx + sy)$ where p, q, r, s are integers with $ps - qr = \pm 1$ transforms each form into another equivalent form. To see the effect of this change of variables on the coefficients (a, b, c) of a form $Q(x, y) = ax^2 + bxy + cy^2$ we do a simple calculation:

$$\begin{aligned} Q(px + qy, rx + sy) &= a(px + qy)^2 + b(px + qy)(rx + sy) + c(rx + sy)^2 \\ &= (ap^2 + bpr + cr^2)x^2 + (2apq + bps + bqr + 2crs)xy \\ &\qquad + (aq^2 + bqs + cs^2)y^2 \end{aligned}$$

This means that the (a, b, c) coordinates of points in $\mathbb{R}^3$ are transformed by T^* according to the formula

$$T^*(a, b, c) = (p^2a + prb + r^2c, 2pqa + (ps + qr)b + 2rsc, q^2a + qsb + s^2c)$$

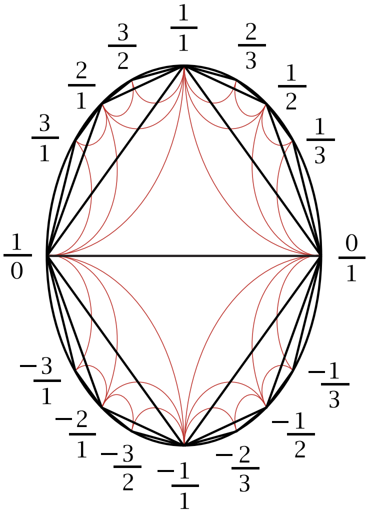
For fixed values of p, q, r, s this T^* is a linear transformation of the variables a, b, c. Its matrix is

$$\begin{pmatrix} p^2 & pr & r^2 \\ 2pq & ps + qr & 2rs \\ q^2 & qs & s^2 \end{pmatrix}$$

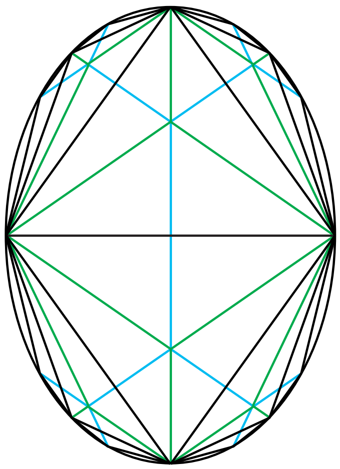
Since T^* is a linear transformation, it takes lines to lines and planes to planes, but T^* also has another special geometric property. Since equivalent forms have the same discriminant, this means that each surface defined by an equation $b^2 - 4ac = k$ for k a constant is taken to itself by T^*. In particular, the double cone $b^2 - 4ac = 0$ is taken to itself, and in fact each of the two cones separately is taken to itself since one cone consists of positive parabolic forms and the other cone of negative parabolic forms (as one can see just by looking at the coefficients a and c), and positive parabolic forms are never equivalent to negative parabolic forms. When $k > 0$ the surface $b^2 - 4ac = k$ is a hyperboloid of one sheet and when $k < 0$ it is a hyperboloid of two sheets. In the case of two sheets the lattice points on one sheet give positive elliptic forms and those on the other sheet give negative elliptic forms.

Since T^* takes lines through the origin to lines through the origin and it takes the double cone $b^2 - 4ac = 0$ to itself, this means that T^* gives a transformation of the ellipse E to itself, taking rational points to rational points since rational points on E correspond to lattice points on the cones. Regarding E as the boundary circle of the Farey diagram, we know that linear fractional transformations give symmetries of the Farey diagram, also taking rational points on the boundary circle to rational boundary points. And in fact, the transformation of this circle defined by T^* is exactly one of these linear fractional transformations. This is because T^* takes the parabolic form $(dx + ey)^2$ to the form $(d(px + qy) + e(rx + sy))^2 = ((dp + er)x + (dq + es)y)^2$ so in the fractional labeling of points of E this says $T^*(d/e) = (pd + re)/(qd + se)$ which is a linear fractional transformation. If we write this using the variables x and y instead of d and e it would be $T^*(x/y) = (px + ry)/(qx + sy)$. This is not quite the same as the linear fractional transformation $T(x/y) = (px + qy)/(rx + sy)$ defined by the original change of variables $T(x, y) = (px + qy, rx + sy)$, but rather T^* is obtained from T by transposing the matrix of T, interchanging the off-diagonal terms q and r.

Via radial projection, the transformation T^* determines a transformation not just of E but of the interior of E in the plane $a + c = 1$ as well. This transformation, which we still call T^* for simplicity, takes lines inside E to lines inside E since T^* takes planes through the origin to planes through the origin. This leads us to consider a "linear" version of the Farey diagram in which each circular arc of the original Farey diagram is replaced by a straight line segment joining the two endpoints of the circular arc. These line segments divide the interior of E into triangles, just as the original Farey diagram divides the disk into curvilinear triangles. The transformation T^* takes each of these triangles onto another triangle, analogous to the way that linear fractional transformations provide symmetries of the original Farey diagram.

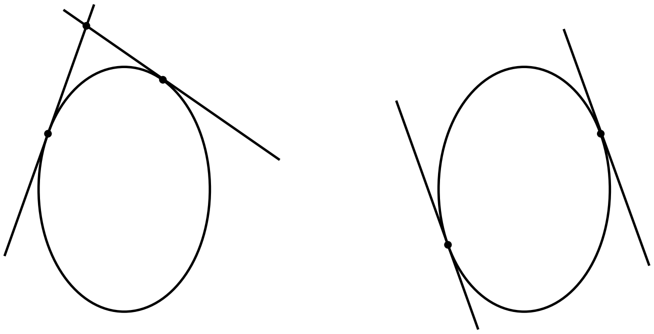


Suppose we divide each triangle of the linear Farey diagram into six smaller triangles as in the figure at the right. The transformation T^* takes each of these small triangles onto another small triangle since it takes lines to lines. One of these small triangles is the triangle defined by the inequalities $0 \le b \le a \le c$ that we considered earlier. The fact that every positive primitive elliptic form is equivalent to exactly one reduced form, corresponding to a rational point in this special triangle, is now visible geometrically as the fact that there is always exactly one transformation T^* taking a given small triangle in the subdivided linear Farey diagram to this one special small triangle.



Elliptic forms whose topograph contains a source edge are equivalent to forms $ax^2 + cy^2$ so these are the forms corresponding to rational points on the edges of the linear Farey diagram, shown in black in the figure above. These are the forms whose topograph has a symmetry reflecting across a line perpendicular to the source edge. (This line is just the edge in the Farey diagram containing the given form.) The other type of reflectional symmetry in the topograph of an elliptic form is reflection across an edge of the topograph. Forms with this sort of symmetry correspond to rational points in the blue and green edges in the preceding figure, the edges we added to subdivide the Farey diagram into the smaller triangles. The blue and green edges are distinguished by whether the two equal values of the form in the three regions surrounding the source vertex occur for the smallest value of the form (blue edges) or the next-to-smallest value (green edges). Note that the blue edges form the dual tree of the Farey diagram.

Let us now turn our attention to hyperbolic and 0-hyperbolic forms, which correspond to integer lattice points that lie outside the two cones. As a preliminary observation, note that for a point (a,b,c) outside the double cone there are exactly two planes in $\mathbb{R}^3$ that are tangent to the double cone and pass through (a,b,c). Each of these planes is tangent to the double cone along a whole line through the origin. The two tangent planes through (a,b,c) are determined by their intersection with the plane $a+c=1$, which consists of two lines tangent to the ellipse E. These two lines can either intersect or be parallel. The latter possibility occurs when the point (a,b,c) lies in the plane $a+c=0$, so the two tangent planes intersect in a line in this plane.



As a simple example, if the point (a,b,c) we start with happens to lie on the b axis, then the tangent planes are the ab plane and the bc plane. These intersect the plane $a+c=1$ in the two vertical tangent lines to the ellipse E.

Our goal will be to show the following:

Proposition 5.9. *Let $Q(x,y)=ax^2+bxy+cy^2$ be a form of positive discriminant, either hyperbolic or 0-hyperbolic. Then the two points where the tangent lines to E determined by (a,b,c) touch E are the points diametrically opposite the two points that are the endpoints of the separator line in the topograph of Q in the case that Q is hyperbolic, or the two points labeling the regions in the topograph of Q where Q takes the value zero in the case that Q is 0-hyperbolic.*

Proof: We begin with a few preliminary remarks that will allow us to treat both the hyperbolic and 0-hyperbolic cases in the same way. A form $Q(x,y)=ax^2+bxy+cy^2$ of positive discriminant can always be factored as $(px+qy)(rx+sy)$ since if $a=0$ we have the factorization $y(bx+cy)$ and if $a\neq 0$ then the associated quadratic equation $ax^2+bx+c=0$ has positive discriminant so it has two distinct real roots α and β, leading to the factorization $ax^2+bxy+cy^2=a(x-\alpha y)(x-\beta y)$ which can be rewritten as $(px+qy)(rx+sy)$ by incorporating a into either factor. If Q is hyperbolic then the discriminant is not a square and hence the factorization $(px+qy)(rx+sy)$ will involve coefficients that are quadratic irrationals. If Q is

0-hyperbolic then the discriminant is a square so the roots α and β are rational and we obtain a factorization of Q as $(px+qy)(rx+sy)$ with rational coefficients. In fact we can take p,q,r,s to be integers in this case since we know every 0-hyperbolic form is equivalent to a form $y(bx+cy)$ so we can obtain the given form Q from $y(bx+cy)$ by replacing x and y by certain linear combinations $dx+ey$ and $fx+gy$ with integer coefficients d,e,f,g.

The points where the tangent planes touch the double cone correspond to forms of discriminant zero, with coefficients that may not be integers or even rational. A simple way to construct two such forms from a given form $Q=(px+qy)(rx+sy)$ is just to take the squares of the two linear factors, so we obtain the two forms $(px+qy)^2$ and $(rx+sy)^2$, each of discriminant zero. We will show that each of these two forms lies on the line of tangency for one of the two tangent planes determined by Q.

To do this for the case of $(px+qy)^2$ we consider the line L in $\mathbb{R}^3$ passing through the two points corresponding to the forms $(px+qy)(rx+sy)$ and $(px+qy)^2$. We claim that L consists of the forms

$$Q_t=(px+qy)\Big[(1-t)(rx+sy)+t(px+qy)\Big]$$

as t varies over all real numbers. When $t=0$ or $t=1$ we obtain the two forms $Q_0=(px+qy)(rx+sy)$ and $Q_1=(px+qy)^2$ so these forms lie on L. Also, we can see that the forms Q_t do form a straight line in $\mathbb{R}^3$ by rewriting the formula for Q_t in (a,b,c) coordinates, where it becomes:

$$(a,b,c)=\big(pr(1-t)+p^2t,(ps+qr)(1-t)+2pqt,qs(1-t)+q^2t\big)$$

This defines a line since p,q,r,s are constants, so each coordinate is a linear function of t. Since the forms Q_t factor as the product of two linear factors, they have nonnegative discriminant for all t. This means that L does not go into the interior of either cone. It also does not pass through the origin since if it did, it would have to be a subset of the double cone since it contains the form Q_1 which lies in the double cone. From these facts we deduce that L must be a tangent line to the double cone. Hence the plane containing L and the origin must be tangent to the double cone along the line containing the origin and Q_1. The same reasoning shows that the other tangent plane that passes through $(px+qy)(rx+sy)$ intersects the double cone along the line containing the origin and $(rx+sy)^2$.

The labels of the points of E corresponding to the forms $(px+qy)^2$ and $(rx+sy)^2$ are p/q and r/s according to the convention we have adopted. On the other hand, when the form $(px+qy)(rx+sy)$ is hyperbolic the ends of the separator line in its topograph are at the two points where this form is zero, which occur when x/y is $-q/p$ and $-s/r$. These are the negative reciprocals of the previous two points p/q and r/s so they are the diametrically opposite points in E. Similarly when $(px+qy)(rx+sy)$ is 0-hyperbolic the vertices of the Farey diagram where it is zero are at $-q/p$ and $-s/r$, again diametrically opposite p/q and r/s. $\square$

It might have been nicer if the statement of the previous Proposition did not involve passing to diametrically opposite points, but to achieve this we would have had to use a different rule for labeling the points of E, with the label p/q corresponding to the form $(qx - py)^2$ instead of $(px + qy)^2$. This 180 degree rotation of the labels would put the negative labels in the upper half of E rather than the lower half, which doesn't seem like such a good idea.

Next let us investigate how hyperbolic and 0-hyperbolic forms are distributed over the lattice points outside the double cone $b^2 - 4ac$. This is easier to visualize if we project such points radially into the plane $a + c = 1$. This only works for forms $ax^2 + bxy + cy^2$ with $a + c > 0$, but the forms with $a + c < 0$ are just the negatives of these so they give nothing essentially new. The forms with $a + c = 0$ will be covered after we deal with those with $a + c > 0$.

Forms with $a + c > 0$ that are hyperbolic or 0-hyperbolic correspond via radial projection to points in the plane $a + c = 1$ outside the ellipse E. Each such point determines a pair of tangent lines to E intersecting at the given point.

For a 0-hyperbolic form $(px + qy)(rx + sy)$ the points of tangency in E have rational labels p/q and r/s. We know that every 0-hyperbolic form is equivalent to a form $y(rx + sy)$ with $a = 0$, so $p/q = 0/1$ and one line of tangency is the vertical line tangent to E on the right side. The form $y(rx + sy)$ corresponds to the point $(0, r, s)$ in the plane $a = 0$ tangent to the double cone. Projecting radially into the vertical tangent line to E, we obtain the points $(0, r/s, 1)$, where r/s is an arbitrary rational number. Thus 0-hyperbolic forms are dense in this vertical tangent line to E. Choosing any rational number r/s, the other tangent line for the form $y(rx + sy)$ is tangent to E at the point labeled r/s.

An arbitrary 0-hyperbolic form $(px + qy)(rx + sy)$ is obtained from one with $p/q = 0/1$ by applying a linear fractional transformation T taking $0/1$ to p/q, so the vertical tangent line to E at $0/1$ is taken to the tangent line at p/q, and the dense set of 0-hyperbolic forms in the vertical tangent line is taken to a dense set of 0-hyperbolic forms in the tangent line at p/q. Thus we see that the 0-hyperbolic forms in the plane $a + c = 1$ consist of all the rational points on all the tangent lines to E at rational points p/q of E.

In the case of a hyperbolic form $ax^2 + bxy + cy^2$ with $a + c > 0$ the two tangent lines intersect E at a pair of conjugate quadratic irrationals, the negative reciprocals of the roots α and $\overline{\alpha}$ of the equation $ax^2 + bx + c = 0$. Since α determines $\overline{\alpha}$ uniquely, one tangent line determines the other uniquely, unlike the situation for 0-hyperbolic forms whose rational tangency points p/q and r/s can be varied independently. A consequence of this uniqueness for hyperbolic forms is that each of the two tangent lines contains only one rational point, the intersection point of the two lines, since any other rational point would correspond to another form having one of its tangent lines the same as for $ax^2 + bxy + cy^2$ and the other tangent line different, contradicting the previous observation that each tangent line for a hyperbolic form determines the other. (The hypothetical second form would also be hyperbolic since the common tangency point for the two forms is not a rational point on E.)

The points in the plane $a + c = 1$ that correspond to 0-hyperbolic forms are dense in the region of this plane outside E since for an arbitrary point in this region we can first take the two tangent lines to E through this point and then take a pair of nearby lines that are tangent at rational points of E since points in E with rational labels are dense in E. It is also true that points in the plane $a+c = 1$ that correspond to hyperbolic forms are dense in the region outside E. To see this we can proceed in two steps. First consider the case of a point in this region whose two tangent lines to E are tangent at irrational points of E. These two irrational points are the endpoints of an infinite strip in the Farey diagram that need not be periodic. However we can approximate this strip by a periodic strip by taking a long finite segment of the infinite strip and then repeating this periodically at each end. This means that the given point in the region outside E lies arbitrarily close to points corresponding to hyperbolic forms. Finally, a completely arbitrary point in the region outside E can be approximated by points whose tangent lines to E touch E at irrational points since irrational numbers are dense in real numbers.

It remains to consider hyperbolic and 0-hyperbolic forms $(px + qy)(rx + sy)$ corresponding to points (a, b, c) in the plane $a + c = 0$. Such a form determines a line through the origin in this plane, and the tangent planes to the double cone that intersect in this line intersect the plane $a + c = 1$ in two parallel lines tangent to E at two diametrically opposite points p/q and $-q/p$. Thus the form is $(px + qy)(qx - py)$, up to a constant multiple. If p/q is rational this is a 0-hyperbolic form. Examples are:

— xy with vertical tangents to E at $1/0$ and $0/1$.
— $x^2 - y^2 = (x + y)(x - y)$ with horizontal tangents to E at $1/1$ and $-1/1$.
— $2x^2 - 3xy - 2y^2 = (2x + y)(x - 2y)$ with parallel tangents at $2/1$ and $-1/2$.

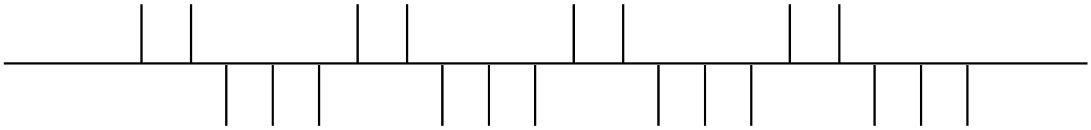
If p/q and $-q/p$ are conjugate quadratic irrationals then we have a hyperbolic form $ax^2 + bxy + cy^2 = a(x - \alpha)(x - \overline{\alpha})$ where $\alpha\overline{\alpha} = -1$ since $c = -a$ when $a + c = 0$. Thus α and $\overline{\alpha}$ are negative reciprocals of each other that are interchanged by 180 degree rotation of E. As examples we have:

$$x^2 + xy - y^2 = \Big(x - \frac{-1+\sqrt{5}}{2}y\Big)\Big(x - \frac{-1-\sqrt{5}}{2}y\Big)$$
$$2x^2 + xy - 2y^2 = 2\Big(x - \frac{-1+\sqrt{17}}{4}y\Big)\Big(x - \frac{-1-\sqrt{17}}{4}y\Big)$$

One can consider a pair of parallel tangent lines to E as the limit of a pair of intersecting tangents where the point of intersection moves farther and farther away from E in a certain direction which becomes the direction of the pair of parallel tangents.

Exercises

1. Find a hyperbolic quadratic form whose periodic separator line has the following pattern:



2. (a) Find two elliptic forms $ax^2 + cy^2$ that have the same discriminant but take on different sets of values. Draw enough of the topographs of the two forms to make it apparent that they do not have exactly the same sets of values. Include the source vertex or source edge in the topographs. (Remember that the topograph only shows the values $Q(x, y)$ for primitive pairs (x, y).)
(b) Do the same thing with hyperbolic forms $ax^2 + cy^2$. Include the separator lines in their topographs.

3. (a) Show the quadratic form $Q(x, y) = 92x^2 - 74xy + 15y^2$ is elliptic by computing its discriminant.
(b) Find the source vertex or edge in the topograph of this form.
(c) Using the topograph of this form, find all the integer solutions of $92x^2 - 74xy + 15y^2 = 60$, and explain why your list of solutions is a complete list. (There are exactly four pairs of solutions $\pm(x, y)$, three of which will be visible in the topograph.)

4. (a) Show that if a quadratic form $Q(x, y) = ax^2 + bxy + cy^2$ can be factored as a product $(Ax + By)(Cx + Dy)$ with A, B, C, D integers, then Q takes the value 0 at some pair of integers $(x, y) \neq (0, 0)$, hence Q must be either 0-hyperbolic or parabolic. Show also, by a direct calculation, that the discriminant of this form is a square.
(b) Find a 0-hyperbolic form $Q(x, y)$ such that $Q(1, 5) = 0$ and $Q(7, 2) = 0$ and draw a portion of the topograph of Q that includes the two regions where $Q = 0$.

5. Determine the number of equivalence classes of quadratic forms of discriminant $\Delta = 120$ and list one form from each equivalence class.

6. Do the same thing for $\Delta = 61$.

7. (a) Find the smallest positive nonsquare discriminant for which there is more than one equivalence class of forms of that discriminant. (In particular, show that all smaller discriminants have only one equivalence class.)
(b) Find the smallest positive nonsquare discriminant for which there are two inequivalent forms of that discriminant, neither of which is simply the negative of the other.

8. (a) For positive elliptic forms of discriminant $\Delta = -D$, verify that the smallest value of D for which there are at least two inequivalent forms of discriminant $-D$ is $D = 12$.

(b) If we add the requirement that all forms under consideration are primitive, then what is the smallest D?

9. Determine all the equivalence classes of positive elliptic forms of discriminants -67, -104, and -347.

10. (a) Determine all the equivalence classes of 0-hyperbolic forms with discriminant 49.

(b) Determine which equivalence class in part (a) each of the forms $Q(x,y) = 7xy - py^2$ for $p = 0,1,2,3,4,5,6$ belongs to.

11. Show that the principal forms $x^2 - dy^2$ and $x^2 + xy - dy^2$ of discriminants $4d$ and $4d + 1$ have topographs with mirror symmetry.

12. Show that if a form takes the same value on two adjacent regions of its topograph, then these regions are both adjacent to the source vertex or edge when the form is elliptic, or both lie along the separator line when the form is hyperbolic.

13. In this extended exercise the goal will be to show that the only negative even discriminants with class number 1 are -4, -8, -12, -16, and -28. (Note that of these, only -4 and -8 are fundamental discriminants.) The strategy will be to exhibit an explicit reduced primitive form Q different from the principal form $x^2 + dy^2$ for each discriminant $-4d$ with $d > 4$ except $d = 7$. This will be done by breaking the problem into several cases, where in each case a form Q will be given and you are to show that this form has the desired properties, namely it is of discriminant $-4d$, primitive, reduced, and different from the principal form. You should also check that the cases considered cover all possibilities.

(a) Suppose d is not a prime power. Then it can be factored as $d = ac$ where $1 < a < c$ and a and c are coprime. In this case let Q be the form $ax^2 + cy^2$.

(b) The form $ax^2 + 2xy + cy^2$ will work provided that $d + 1$ factors as $d + 1 = ac$ where a and c are coprime and $1 < a < c$. If d is odd, for example a power of an odd prime, then $d + 1$ is even so it has such a factorization $d + 1 = ac$ unless $d + 1 = 2^n$.

(c) If $d = 2^n$ the cases we need to consider are $n \geq 3$ since we assume $d > 4$. When $n = 3$ take Q to be $3x^2 + 2xy + 3y^2$ and when $n \geq 4$ take Q to be $4x^2 + 4xy + (2^{n-2} + 1)y^2$.

(d) When $d + 1 = 2^n$ the cases of interest are $n \geq 3$. When $n = 3$ we have $d = 7$ which is one of the allowed exceptions with class number 1. When $n = 4$ we have $d = 15$ and $3x^2 + 5y^2$ works as in part (a). When $n = 5$ we have $d = 31$ and we take the form $5x^2 + 4xy + 7y^2$. When $n \geq 6$ we use the form $8x^2 + 6xy + (2^{n-3} + 1)y^2$.

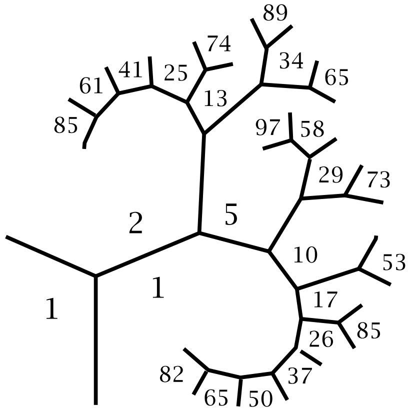
Chapter 6. Representations by Quadratic Forms

With the various things we have learned about quadratic forms so far, let us return to the basic representation problem of determining what values a given form $Q(x,y) = ax^2 + bxy + cy^2$ can take on when x and y are integers, or in other words, which numbers can be represented in the form $ax^2 + bxy + cy^2$. Remember that it suffices to restrict attention to the values in the topograph since these are the values for primitive pairs (x,y), and to get all other values one just multiplies the values in the topograph by arbitrary squares. We focus on the forms that are either elliptic or hyperbolic, as these are the most interesting cases.

As we will see through a series of examples, the type of answer one gets for the representation problem varies from quite simple to slightly complicated to quite complicated indeed.

Three Levels of Complexity

As a first example let us try to find a general pattern in the values of the form $x^2 + y^2$. In view of the symmetry of the topograph for this form it suffices to look just in the first quadrant of the topograph. A piece of this quadrant is shown in the figure at the right, somewhat distorted to squeeze more numbers into the picture. What is shown is all the numbers in the topograph that are less than 100. At first glance it may be hard to detect any patterns here. Both even and odd numbers occur, but none of the even numbers are divisible by 4 so they are all twice an odd number, and in fact an odd number that appears in the topograph. Considering the odd numbers, one notices they are all congruent to 1 mod 4 and not 3 mod 4, which is the other possibility for odd numbers. On the other hand, not all odd numbers congruent to 1 mod 4 appear in the topograph. Up to 100, the ones that are missing are 9, 21, 33, 45, 49, 57, 69, 77, 81, and 93. Each of these has at least one prime factor congruent to 3 mod 4, while all the odd numbers that do appear have all their prime factors congruent to 1 mod 4. Conversely, all products of primes congruent to 1 mod 4 are in the topograph.



This leads us to guess that the following statements might be true:

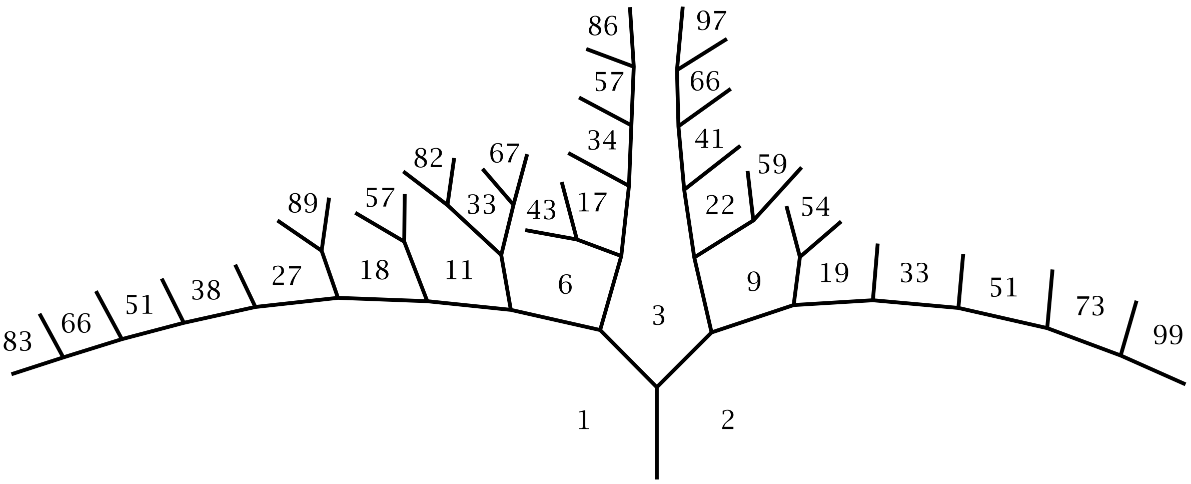
Conjecture. *The numbers that appear in the topograph of $x^2 + y^2$ are precisely the numbers $n = 2^a p_1 p_2 \cdots p_k$ where $a \le 1$ and each p_i is a prime congruent to 1 mod 4. Consequently the values of the quadratic form $Q(x,y) = x^2 + y^2$ as x and y range over all integers (not just the primitive pairs) are exactly the numbers $n = m^2 p_1 p_2 \cdots p_k$ where m is an arbitrary integer and each p_i is either 2 or a prime congruent to 1 mod 4.*

In both statements the index k denoting the number of prime factors p_i is allowed to be zero as well as any positive integer. The restriction $a \le 1$ in the first statement disappears in the second statement since for nonprimitive representations we can multiply by arbitrary squares which allows us to realize all powers of 2.

We will prove the conjecture later in the chapter. A weaker form of the conjecture can be proved just by considering congruences mod 4 as follows. An even number squared is congruent to 0 mod 4 and an odd number squared is congruent to 1 mod 4, so $x^2 + y^2$ must be congruent to 0, 1, or 2 mod 4. Moreover, the only way that $x^2 + y^2$ can be 0 mod 4 is for both x and y to be even, which cannot happen for primitive pairs. Thus all numbers in the topograph must be congruent to 1 or 2 mod 4. This says that the odd numbers in the topograph are congruent to 1 mod 4 and the even numbers are each twice an odd number.

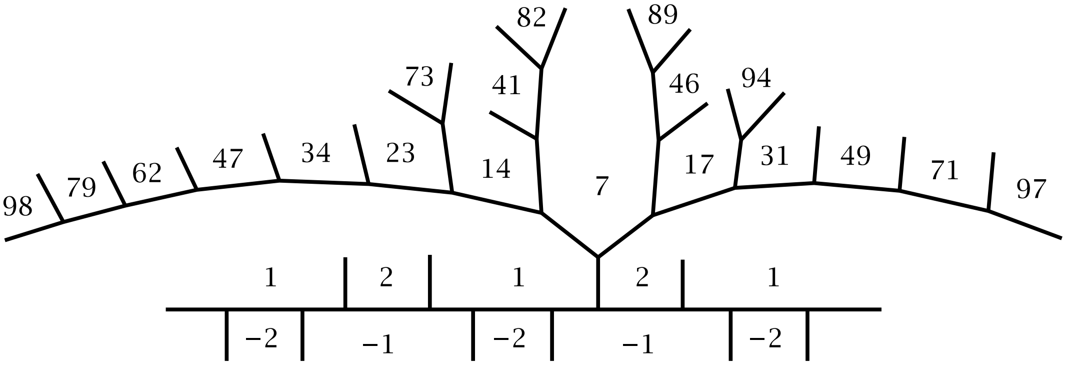
However, these simple observations say nothing about the role played by primes and prime factorizations, nor do they include any positive assertions about which numbers actually are represented by $x^2 + y^2$. It definitely takes more work to show for example that every prime $p = 4k+1$ can be represented as the sum of two squares.

Let us look at a second example to see whether the same sorts of patterns occur, this time for the form $Q(x, y) = x^2 + 2y^2$. Here is a portion of its topograph showing all values less than 100:



Again the even values are just the doubles of the odd values. The odd prime values are $3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97$ and the other odd values are all possible products of these primes. The odd prime values are not determined by their values mod 4 in this case, but instead by their values mod 8 since these values are all congruent to 1 or 3 mod 8. Apart from this change, the answer to the representation problem for $x^2 + 2y^2$ is completely analogous to the answer for $x^2 + y^2$. Namely, the numbers represented primitively by $x^2 + 2y^2$ are the numbers $n = 2^a p_1 p_2 \cdots p_k$ with $a \le 1$ and each p_i a prime congruent to 1 or 3 mod 8. Using congruences mod 8 we could easily prove the weaker statement that all numbers represented primitively by $x^2 + 2y^2$ must be congruent to $1, 2, 3$, or 6 mod 8, so all odd numbers in the topograph must be congruent to 1 or 3 mod 8 and all even numbers must be twice an odd number.

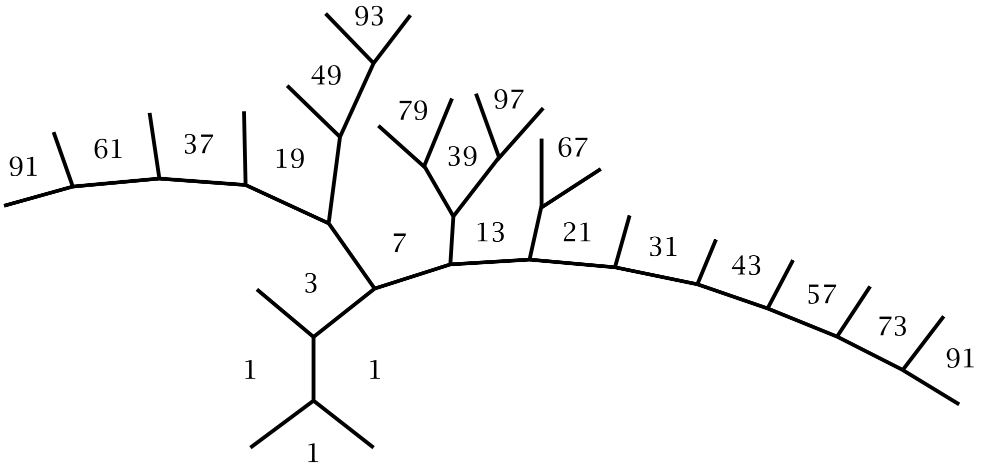
These two examples were elliptic forms, but the same sort of behavior can occur for hyperbolic forms as we see in the next example, the form $x^2 - 2y^2$. The negative values of this form happen to be just the negatives of the positive values, so we need only show the positive values in the topograph:



Here the primes that occur are 2 and primes congruent to ±1 modulo 8. The nonprime values that occur are the products of primes congruent to ±1 modulo 8 and twice these products. Again there is a weaker statement that can be proved using just congruences mod 8.

In these three examples the guiding principle was to look at prime factorizations and at primes modulo certain numbers, the numbers 4, 8, and 8 in the three cases. Notice that these numbers are just the absolute values of the discriminants −4, −8, and 8. Looking at primes modulo $|\Delta|$ turns out to be a key idea for all quadratic forms.

Another example of the same sort is the form $x^2 + xy + y^2$ of discriminant −3. This time it is the prime 3 that plays a special role rather than 2.



We only have to draw one-sixth of the topograph because of all the symmetries. Notice that all the values are odd, so the prime 2 plays no role here. Since the discriminant is −3 we are led to consider congruences mod 3. The primes in the topograph are

3 and the primes congruent to 1 mod 3 (which in particular excludes the prime 2), namely the primes $7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97$. The nonprime values are the products of these primes with the restriction that the prime 3 never has an exponent greater than 1. This is analogous to the prime 2 never having an exponent greater than 1 in the preceding examples. In all four examples the "special" primes whose exponents are restricted are just the prime divisors of the discriminant. This is a general phenomenon, that primes dividing the discriminant behave differently from those that do not.

A special feature of the discriminants -4, -8, 8, and -3 is that in each case all forms of that discriminant are equivalent. We will see that the representation problem always has the same type of answer for discriminants with a single equivalence class of forms.

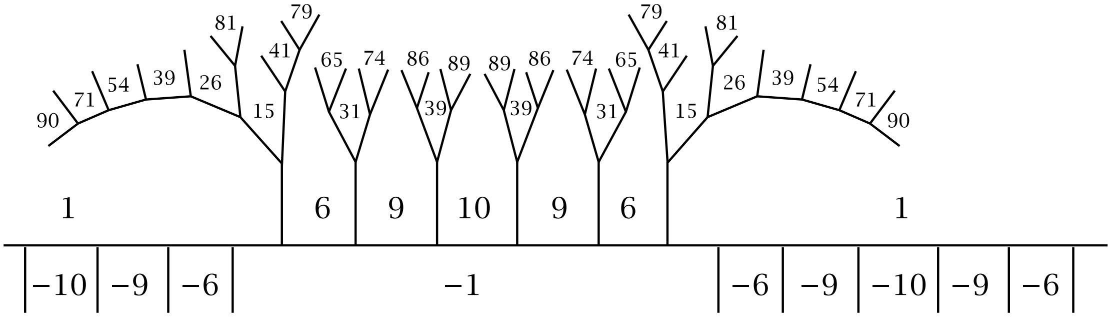
Before going on to the next level of complexity let us digress to describe a nice property that forms of the first level of complexity have. As we know, if a form $Q(x, y)$ represents an integer n then it also represents any multiple m^2n. The converse is not always true however. For example the form $2x^2 + 7y^2$ represents 9 (when x and y both equal 1) but obviously does not represent 1. Nevertheless, this converse property does hold for forms such as those in the preceding four examples where the numbers represented (primitively or not) by the form are exactly the numbers n that can be factored as $n = m^2p_1p_2 \cdots p_k$ for primes p_i satisfying certain conditions and m an arbitrary integer. This is because if a number n has a factorization of this type then we can cancel any square factor of n and the result still has a factorization of the same type.

Let us apply this "square-cancellation" property in the case of the form x^2+y^2 to determine the numbers n such that the circle $x^2 + y^2 = n$ contains a rational point, and hence, as in Chapter 0, an infinite dense set of rational points. Suppose first that the circle $x^2 + y^2 = n$ contains a rational point, so after putting the two coordinates over a common denominator the point is $(x, y) = (\frac{a}{c}, \frac{b}{c})$. The equation $x^2 + y^2 = n$ then becomes $a^2 + b^2 = c^2n$. This means that the equation $x^2 + y^2 = c^2n$ has an integer solution. Then the square-cancellation property implies that the original equation $x^2 + y^2 = n$ has an integer solution. Thus we see that if there are rational points on the circle $x^2 + y^2 = n$ then there are integer points on it. This is not something that is true for all quadratic curves, as shown again by the example of the ellipse $2x^2 + 7y^2 = 1$ which has rational points such as $(\frac{1}{3}, \frac{1}{3})$ but no integer points.

From the solution to the representation problem for $x^2 + y^2$ we deduce that the circle $x^2 + y^2 = n$ contains rational points exactly when $n = m^2p_1p_2 \cdots p_k$ where m is an arbitrary integer and each p_i is either 2 or a prime congruent to 1 mod 4. The first few values of n satisfying this condition are $1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, \cdots$.

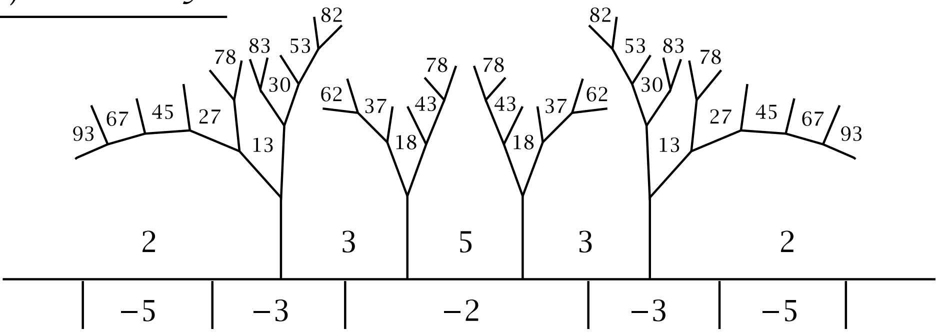
Now let us consider some examples with a second level of complexity. First consider the form $x^2 - 10y^2$ whose positive values less than 100 are shown in the following topograph:

$Q_1(x, y) = x^2 - 10y^2$



There is no need to show any more of the negative values since these will just be the negatives of the positive values. The prime values less than 100 are $31, 41, 71, 79, 89$. These are the primes congruent to ± 1 or ± 9 modulo 40, the discriminant. However, in contrast to what happened in the previous examples, there are many nonprime values that are not products of these prime values. The prime factors of these nonprime values are $2, 3, 5, 13, 37, 43$, none of which occur in the topograph. Rather miraculously, these prime values are realized instead by another form $2x^2 - 5y^2$ having the same discriminant as $x^2 - 10y^2$. Here is the topograph of this companion form $2x^2 - 5y^2$:

$Q_2(x, y) = 2x^2 - 5y^2$



Again the negative values are just the negatives of the positive values. The prime values this form takes on are 2 and 5, which are the prime divisors of the discriminant 40, along with primes congruent to ± 3 and ± 13 modulo 40, namely $3, 13, 37, 43, 53, 67, 83$.

Apart from the primes 2 and 5 that divide the discriminant 40, the possible values of primes modulo 40 are $\pm 1, \pm 3, \pm 7, \pm 9, \pm 11, \pm 13, \pm 17, \pm 19$ since even numbers and multiples of 5 are excluded. There are 16 different congruence classes here, and exactly half of them, 8, are realized by one or the other of the two forms $x^2 - 10y^2$ and $2x^2 - 5y^2$, with 4 classes realized by each form. The other 8 congruence classes are not realized by any form of discriminant 40 since every form of discriminant 40 is equivalent to one of the two forms $x^2 - 10y^2$ or $2x^2 - 5y^2$, as is easily checked by the methods from the previous chapter.

This turns out to be a general phenomenon valid for all elliptic and hyperbolic forms: If one excludes the primes that divide the discriminant, then the prime values of quadratic forms of that discriminant are exactly the primes in half of the possible congruence classes modulo the discriminant. This will be proved in Theorem 6.7 later in the chapter.

After further examination of the topographs of the two forms $Q_1 = x^2 - 10y^2$ and $Q_2 = 2x^2 - 5y^2$ it seems that the following statements should be true:

Conjecture. *The numbers represented primitively by either Q_1 or Q_2 are the products $(-1)^a 2^b 5^c p_1 p_2 \cdots p_k$ where $a, b, c \le 1$ and each p_i is a prime congruent to $\pm 1, \pm 3, \pm 9$, or ± 13 mod 40. Furthermore, one can determine which form will represent such a product by the rule that if the number of terms in the product that are represented by Q_2 (namely 2, 5, and $p_i \equiv \pm 3$ or ± 13 mod 40) is even, then the number is represented by Q_1 and if it is odd then the number is represented by Q_2.*

For example, the topograph of Q_1 contains the even powers of 3 while the topograph of Q_2 contains the odd powers. Another consequence is that the even values in one topograph are just the doubles of the odd values in the other topograph.

This characterization of numbers represented primitively by these two forms also implies that no number is represented by both Q_1 and Q_2, except 0 of course. However, for some discriminants it is possible for two non-equivalent forms of that discriminant to represent the same nonzero number, as we will see.

The preceding Conjecture will be proved piece by piece as we gradually develop the necessary general theory. We will focus first on determining which primes are represented byQ_1 and which by Q_2, where Proposition 6.10 will provide the final answer. For nonprimes the first sentence of the Conjecture will follow from Theorem 6.13, while the second sentence will use results from Chapter 7.

There is another way of formulating the second half of the Conjecture that is quite enlightening and turns out generalize to all discriminants. For the sake of simplicity let us just talk about representing numbers without distinguishing between primitive and nonprimitive representations. Then the second half of the Conjecture can be reformulated as the following three statements:

(1) The product of two numbers represented by Q_1 is again represented by Q_1.

(2) The product of two numbers represented by Q_2 is represented by Q_1.

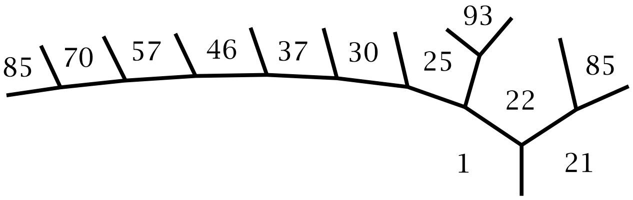
(3) The product of a number represented by Q_1 with a number represented by Q_2 is represented by Q_2.

An abbreviated way of writing these statements is by the formulas $Q_1Q_1 = Q_1$, $Q_2Q_2 = Q_1$, and $Q_1Q_2 = Q_2$. One can see that these are formally the same as the rules for addition of integers mod 2: $0+0=0$, $1+1=0$, and $0+1=1$. The two formulas $Q_1Q_1 = Q_1$ and $Q_1Q_2 = Q_2$ say that Q_1 serves as an identity element “1”

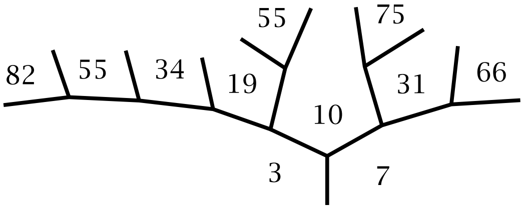
for this multiplication operation, and then the formula $Q_2Q_2 = Q_1$ can be interpreted as saying that Q_2 is equal to its own inverse, so $Q_2 = Q_2^{-1}$.

Let us look at another example where the representation problem has an answer that is qualitatively similar to the preceding example but just a little more complicated, the case of discriminant -84. Here there are twice as many equivalence classes of forms, four instead of two, with topographs shown below.

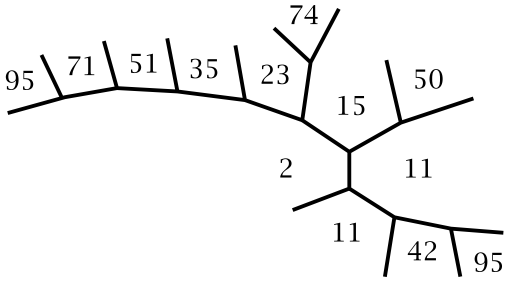
$Q_1(x,y) = x^2+21y^2$



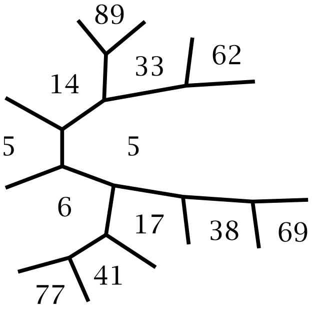
$Q_2(x,y) = 3x^2+7y^2$



$Q_3(x,y) = 2x^2+2xy+11y^2$



$Q_4(x,y) = 5x^2+4xy+5y^2$



The primes dividing the discriminant -84 are 2, 3, and 7, and these primes are each represented by one of the forms. For the remaining primes, we will show later in the chapter that the primes represented by each form are as follows:

- For Q_1 the primes $p \equiv 1, 25, 37 \bmod 84$.
- For Q_2 the primes $p \equiv 19, 31, 55 \bmod 84$.
- For Q_3 the primes $p \equiv 11, 23, 71 \bmod 84$.
- For Q_4 the primes $p \equiv 5, 17, 41 \bmod 84$.

This agrees with what is shown in the four topographs above, and one could expand the topographs to get further evidence that these are the right answers.

One can work out hypothetical rules for multiplying the forms by considering how products of two primes are represented. For example, 3 is represented by Q_2 and 11 is represented by Q_3, while their product $3 \cdot 11 = 33$ is represented by Q_4, so we might guess that $Q_2Q_3 = Q_4$. Some other products that give the same conclusion are $3 \cdot 2 = 6$, $3 \cdot 23 = 69$, $7 \cdot 2 = 14$, $7 \cdot 11 = 77$, $31 \cdot 2 = 62$, etc. In the same way one can determine tentative rules for all the products Q_iQ_j. One finds:

- The principal form Q_1 acts as the identity, so $Q_1Q_i = Q_i$ for each i.
- $Q_iQ_i = Q_1$ for each i so each Q_i equals its own inverse.
- The product of any two out of Q_2, Q_3, Q_4 is equal to the third.

These multiplication rules are formally identical to how one would add pairs (m,n) of integers mod 2 by adding their two coordinates separately. The form Q_1 corresponds to the pair $(0,0)$ and the first of the three rules above becomes the formula $(0,0) + (m,n) = (m,n)$. The forms Q_2, Q_3, and Q_4 correspond to $(1,0)$, $(0,1)$, and $(1,1)$ in any order, and then the second rule above becomes $(m,n)+(m,n) = (0,0)$ which is valid for addition mod 2, while the third rule becomes the fact that the sum of any two of $(1,0)$, $(0,1)$, and $(1,1)$ is equal to the third if we do addition mod 2.

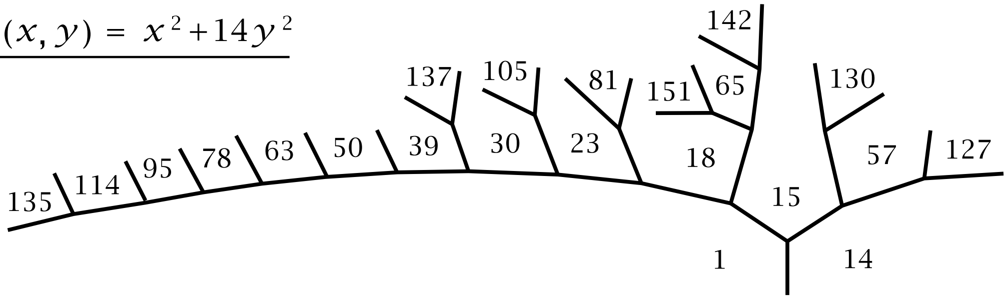
The multiplication rules determine which form represents a given number n by replacing each prime in the prime factorization of n by the form Q_i that represents it, then multiplying out the resulting product using the three multiplication rules. For example, for $n = 70 = 2 \cdot 5 \cdot 7$ we get the product $Q_3Q_4Q_2$ which equals Q_1 and so 70 is represented by Q_1, as the topograph shows. For $n = 66 = 2 \cdot 3 \cdot 11$ we get $Q_3Q_2Q_3 = Q_2$ and 66 is represented by Q_2. In general, for a number $n = 2^a3^b7^cp_1 \cdots p_k$ where each p_i is a prime other than $2,3,7$ that is represented by one of the forms Q_i, we can determine which form represents n by the following steps. First compute the number q_i of prime factors of n represented by Q_i. Next compute the sum $q_1(0,0) + q_2(1,0) + q_3(0,1) + q_4(1,1) = (q_2 + q_4, q_3 + q_4)$ where $(0,0),(1,0),(0,1),(1,1)$ correspond to Q_1,Q_2,Q_3,Q_4 respectively. The resulting sum (m,n) then tells which form represents n.

This description does not require restricting only to primitive representations, but if we do impose this restriction all that changes is that each of the exponents a,b,c must be either 0 or 1. For example the numbers 2^2, 3^2, and 7^2 are not represented primitively by any of the four forms since they do not appear in the topographs, but they are each represented by Q_1 nonprimitively since they are squares times 1 which is represented by Q_1. Similar, $2^3 \cdot 5$ is not represented primitively by any of the forms but it is represented nonprimitively by Q_2 since it is a square times $2 \cdot 5$ which is represented primitively by Q_2.

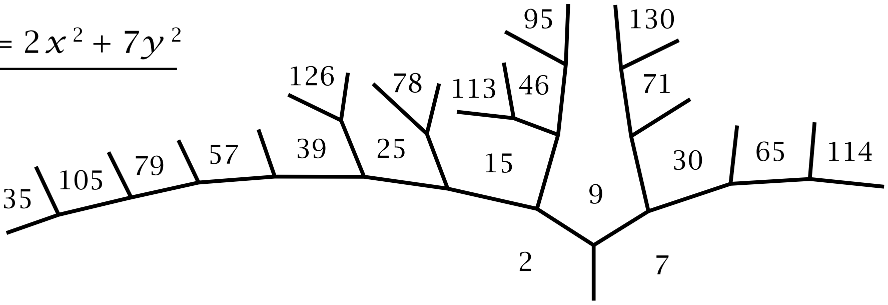
An interesting feature of all the forms at the first or second level of complexity that we have examined so far is that their topographs have mirror symmetry. This is actually a general phenomenon: Whenever all the forms of a given discriminant have mirror symmetry, then the question of which numbers are represented primitively by each of these forms has an answer just in terms of the prime factorizations of the numbers, with congruences modulo the discriminant determining which primes are represented by each form and with certain multiplication rules for the forms then determining which form represents a given nonprime.

Now we move on to the third level of complexity. In the preceding examples it was possible to determine which numbers are represented by a given form by looking at primes and which congruence classes they fall into modulo the discriminant. A consequence of the way the answer was formulated was that no number (except 0) could be represented by two inequivalent forms of the same discriminant. Both of these nice properties fail to hold in general, however. An example is provided by forms of discriminant -56. Two nonequivalent forms of this discriminant are $Q_1 = x^2 + 14y^2$ and $Q_2 = 2x^2 + 7y^2$, whose topographs are shown below. The primes 23 and 79 are congruent modulo 56, and yet 23 is represented by Q_1 since $Q_1(3,1) = 23$, while 79 is represented by Q_2 since $Q_2(6,1) = 79$. Also, some non-primes are represented by both Q_1 and Q_2. For example, $Q_1(1,1) = 15$ and $Q_2(2,1) = 15$.

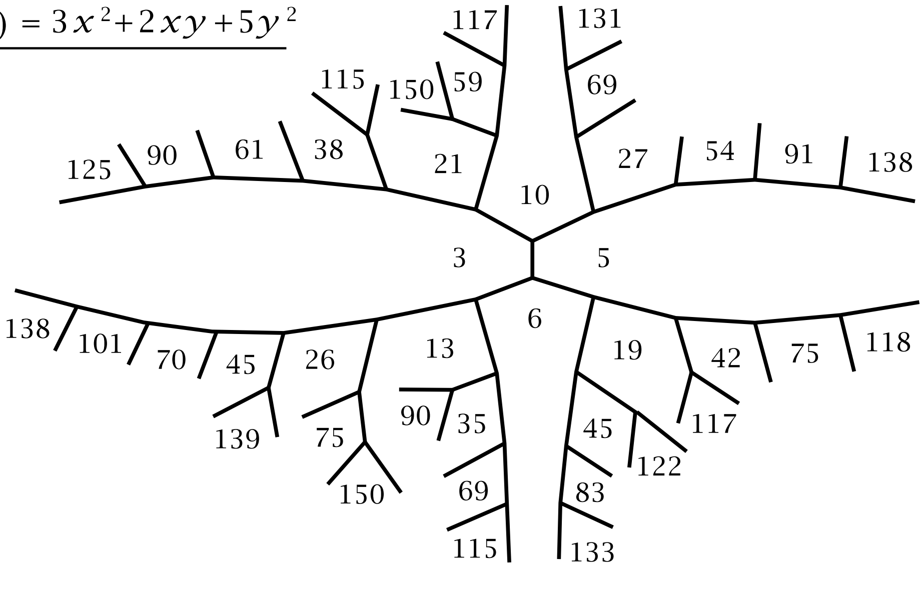
$Q_1(x,y) = x^2+14y^2$



$Q_2(x,y) = 2x^2+7y^2$



$Q_3(x,y) = 3x^2+2xy+5y^2$



The number of equivalence classes of forms of discriminant -56 is actually 3, and a third form with this discriminant, not equivalent to either Q_1 or Q_2, is also shown in the figure, the form $Q_3 = 3x^2 + 2xy + 5y^2$. Note that the topograph of Q_3 does not have mirror symmetry, so Q_3 counts twice when determining the class number for discriminant 56, which is therefore 4 rather than 3.

Apart from the primes 2 and 7 that divide the discriminant -56, all other primes belong to the following 24 congruence classes modulo 56, corresponding to odd numbers less than 56 not divisible by 7:

$$\underline{1}\ \overline{3}\ \overline{5}\ \underline{9}\ 11\ \overline{13}\ \underline{15}\ 17\ \overline{19}\ \underline{23}\ \underline{25}\ \overline{27}\ 29\ 31\ 33\ 37\ \underline{39}\ 41\ 43\ \overline{45}\ 47\ 51\ 53\ 55$$

The six congruence classes whose prime elements are represented by Q_1 or Q_2 are indicated by underlines, and the six congruence classes whose prime elements are represented by Q_3 are indicated by overlines. Primes not represented by any of the three forms are in the remaining 12 congruence classes.

The new thing that happens in this example is that one cannot tell whether a prime is represented by Q_1 or Q_2 just by considering congruence classes mod the discriminant. We saw this for the pair of primes 23 and 79, and another such pair visible in the topographs is 71 and 127. By extending the topographs we could find many more such pairs. One might try using congruences modulo some other number besides 56, but it is known that this does not help.

Congruences mod 56 suffice to tell which primes are represented by Q_3, but there is a different sort of novel behavior involving Q_3 when we look at representing products of primes. To illustrate this, observe that the primes 3 and 5 are represented by Q_3 but their product 15 is represented by both Q_1 and Q_2. This means there is some ambiguity about whether the product Q_3Q_3 should be Q_1 or Q_2. The same thing happens in fact for any pair of numbers represented by Q_3, although in some cases this involves representations that are not primitive. For example, 5 and 10 are represented by Q_3 and their product 50 is represented by Q_1 primitively and by Q_2 nonprimitively since Q_2 represents 2 and hence also $2 \cdot 5^2$.

For other products Q_iQ_j there seems to be no ambiguity. The principal form Q_1 acts as the identity for multiplication, while $Q_2Q_2 = Q_1$ and $Q_2Q_3 = Q_3$, although this last formula is somewhat odd since it seems to imply that Q_3 does not have a multiplicative inverse since if it did, we could multiply by this inverse to get that $Q_2 = Q_1$, the identity for multiplication.

It turns out that there is a way out of these difficulties, discovered by Gauss. The troublesome form Q_3 is different from the other forms in this example and in the preceding examples in that it does not have mirror symmetry. Thus the equivalence class of Q_3 splits into two proper equivalence classes, with Q_3 having a mirror image form $Q_4 = 3x^2 - 2xy + 5y^2$ obtained from Q_3 by changing the sign of either x or y and hence changing the coefficient of xy to its negative. Using Q_4 we can then resolve the ambiguous product Q_3Q_3 by setting $Q_3Q_3 = Q_2 = Q_4Q_4$ and $Q_3Q_4 = Q_1$

so that Q_4 is the inverse of Q_3. This means that each Q_i has its inverse given by the mirror image topograph since Q_1 and Q_2 have mirror symmetry and equal their own inverses. The rigorous justification for the formulas $Q_3Q_3 = Q_2 = Q_4Q_4$ and $Q_3Q_4 = Q_1$ will come in Chapter 7, but for the moment one can check that they are at least consistent with the topographs.

Since $Q_3^2 = Q_2$ we have $Q_3^4 = Q_2^2 = Q_1$. This implies that $Q_3^3 = Q_4$, the inverse of Q_3. Thus all four proper equivalence classes of forms are powers of the single form $Q = Q_3$ since $Q^2 = Q_2$, $Q^3 = Q_4$, and $Q^4 = Q_1$. Products of these powers Q^i are computed by adding exponents mod 4 since Q^4 is the identity. Thus multiplication of the four forms is formally identical with addition of integers mod 4. The earlier doubtful formula $Q_2Q_3 = Q_3$ is resolved to $Q_2Q_3 = Q_4$ and $Q_2Q_4 = Q_3$.

The appearance of the same number in two different topographs is easy to explain now that we have two forms Q_3 and Q_4 representing exactly the same numbers. For example, to find all appearances of the number $15 = 3 \cdot 5$ in the topographs we observe that its prime factors 3 and 5 appear in the topographs of both Q_3 and Q_4 so 15 will appear in the topographs of $Q_3Q_3 = Q_2$, $Q_3Q_4 = Q_1$, and $Q_4Q_4 = Q_2$, (although this last formula gives nothing new). The general procedure for finding which forms represent a given number $n = 2^a 7^b p_1 \cdots p_k$ for primes p_i different from 2 or 7 is to replace each prime factor by the power or powers of $Q = Q_3$ that represent it, then multiply the resulting expressions out by adding the exponents. For prime factors represented by Q_3 we have the choice of replacing these primes by eitherQ^1 or Q^3, so for the final product we will either get both Q^0 and Q^2 or both Q^1 and Q^3. Since Q^1 and Q^3 are equivalent forms, this means that only Q_1 and Q_2 can represent the same number.

The prescription we have just described can produce both primitive and nonprimitive representations of n. To get just primitive representations the exponents a and b must be at most 1, and in addition, whenever a prime p_i represented by Q_3 appears more than once in the prime factorization of n, we should replace each of its appearances in the factorization by the same one of Q_3 and Q_4. This last condition will be justified in Chapter 7. For example, the primitive representations of $18 = 2 \cdot 3^2$ arise just from the products $Q_2Q_3^2 = Q_1$ and $Q_2Q_4^2 = Q_1$ and not from $Q_2Q_3Q_4 = Q_2$ since this last product corresponds to a nonprimitive representation of 18 by Q_2.

We will show in Chapter 7 that the set $CG(\Delta)$ of proper equivalence classes of primitive forms of discriminant Δ always has a multiplication operation compatible with multiplying values of forms of that discriminant in the way illustrated by the preceding examples. This multiplication operation on $CG(\Delta)$ gives it the structure of a group, that is, a set with an associative multiplication operation for which there is an element of the set that functions as an identity for the multiplication, and such that each element of the set has a multiplicative inverse whose product with the given element is the identity element. The set $CG(\Delta)$ with this multiplication is called the *class group* for discriminant Δ, the word “class” referring to proper equivalence classes of forms.

The class group has the additional property that the multiplication is commutative. This makes its algebraic structure much simpler than the typical noncommutative group. An example of a noncommutative group that we have seen is the group $LF(\mathbb{Z})$ of linear fractional transformations, where the multiplication comes from multiplication of 2×2 matrices, or equivalently, composition of the transformations.

For a given discriminant, if the numbers represented by two forms cannot be distinguished by congruences mod the discriminant, then these two forms are said to belong to the same *genus*. Thus in the preceding example of discriminant -56 the two forms Q_1 and Q_2 are of the same genus while Q_3 is of a different genus from Q_1 and Q_2. Equivalent forms always belong to the same genus, of course. The first two of the three levels of complexity we have described correspond to the discriminants where there is only one equivalence class in each genus. For discriminant -56 there are two different genera (“genera” is the plural of “genus”), but in more complicated examples there can be large numbers of genera and large numbers of equivalence classes within a genus.

For negative discriminants there are 101 known discriminants for which each genus of primitive forms contains only one proper equivalence class, and hence congruences are sufficient to determine exactly which numbers a given form represents. Most likely this is a complete list, but this has not yet been proven. By contrast, the number of positive discriminants with this desirable property is likely to be infinite since the number of discriminants with class number one is already conjectured to be infinite.

We just saw an example where two non-equivalent forms of the same discriminant can both represent the same number. However, this does not happen for representations of 1 or primes:

Proposition 6.1. *Let Q_1 and Q_2 be two forms having the same discriminant. Then if Q_1 and Q_2 both represent the same prime p, or if they both represent 1, then Q_1 and Q_2 are equivalent.*

It follows that the same is true for $-p$ and -1 just by replacing Q_1 and Q_2 with $-Q_1$ and $-Q_2$, which does not change the discriminant.

Proof: Suppose that Q is a form representing a number p that is either 1 or a prime, hence the representation of p is primitive. The topograph of Q then has a region labeled p, and we have seen that the h-labels on the edges adjacent to this p-region form an arithmetic progression with increment $2p$ when these edges are all oriented in the same direction. We have the discriminant formula $\Delta = h^2 - 4pq$ where h is the label on one of these edges and q is the value of Q for the region on the other side of this edge. Since p is nonzero the equation $\Delta = h^2 - 4pq$ determines q in terms of Δ and h. This implies that Δ and the arithmetic progression determine the form Q up to equivalence since the progression determines p, and any h-value in the progression then determines the q-value corresponding to this h-value, so Q is equivalent to $px^2 + hxy + qy^2$.

In the case that $p = 1$ the increment in the arithmetic progressions is $2p = 2$ so the two possible progressions of h-values adjacent to the p-region are the even numbers and the odd numbers. We know that h has the same parity as Δ, so Δ determines which of the two progressions we have. As we saw in the preceding paragraph, this implies that the form is determined by Δ, up to equivalence.

Now we consider the case that p is prime. Let Q_1 and Q_2 be two forms of the same discriminant Δ both representing p. For Q_1 choose an edge in its topograph adjacent to the p-region, with h-label h_1 and q-label q_1. For the form Q_2 we similarly choose an edge with associated labels h_2 and q_2. Both h_1 and h_2 have the same parity as Δ. We have $\Delta = h_1^2 - 4pq_1 = h_2^2 - 4pq_2$ and hence $h_1^2 \equiv h_2^2 \bmod 4p$. This implies $h_1^2 \equiv h_2^2 \bmod p$, so p divides $h_1^2 - h_2^2 = (h_1 + h_2)(h_1 - h_2)$. Since p is prime, it must divide one of the two factors and hence we must have $h_1 \equiv \pm h_2 \bmod p$. By changing the orientations of the edges in the topograph for Q_1 or Q_2 if necessary, we can assume that $h_1 \equiv h_2 \bmod p$.

If p is odd we can improve this congruence to $h_1 \equiv h_2 \bmod 2p$ since we know that $h_1 - h_2$ is divisible by both p and 2 (since h_1 and h_2 have the same parity), hence $h_1 - h_2$ is divisible by $2p$. The congruence $h_1 \equiv h_2 \bmod 2p$ implies that the arithmetic progression of h-values adjacent to the p-region for Q_1 is the same as for Q_2 since $2p$ is the increment for both progressions. By what we showed earlier, this implies that Q_1 and Q_2 are equivalent.

When $p = 2$ this argument needs to be modified slightly. We still have $h_1^2 \equiv h_2^2 \bmod 4p$ so when $p = 2$ this becomes $h_1^2 \equiv h_2^2 \bmod 8$. Since $2p = 4$ the four possible arithmetic progressions of h-values are $h \equiv 0, 1, 2,$ or $3 \bmod 4$. We can interchange the possibilities 1 and 3 just by reorienting the edges, leaving only the possibilities $h \equiv 0, 1,$ or $2 \bmod 4$. Since h_1 and h_2 have the same parity, namely the parity of Δ, this takes care of the case that h_1 and h_2 are both odd. The remaining two cases $h \equiv 0, 2 \bmod 4$ are distinguished from each other by the congruence $h_1^2 \equiv h_2^2 \bmod 8$ since $(4k)^2 \equiv 0 \bmod 8$ and $(4k+2)^2 \equiv 4 \bmod 8$. □

The same argument shows another interesting fact:

Proposition 6.2. *If the topograph of a form Q has two regions labeled p where p is either 1 or a prime, then there is a symmetry of the topograph that takes one region to the other. Similarly, if there is one region labeled p and another labeled $-p$ then there is a skew symmetry taking one region to the other.*

Proof: Suppose first that there are two regions having the same label p. As we saw in the proof of the preceding Proposition, each of these regions is adjacent to an edge with the same label h and hence the labels q across these edges are also the same. This means there is a symmetry taking one region labeled p to the other. The other case is that one region is labeled p and the other $-p$. This means that Q and $-Q$ each have a region labeled p so there is an equivalence from Q to $-Q$ taking the p region for Q to the p region for $-Q$. This equivalence can be regarded as a skew symmetry of Q taking the p region to the $-p$ region. □

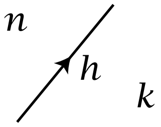
A Criterion for Representability

Ideally, we would like to determine which numbers are primitively represented by a given form, but this is quite difficult in general and there seems to be little hope that a complete answer can be found for all forms. A more approachable question that we will be able to answer is the following:

Problem. *For a given discriminant Δ, determine all the numbers that are represented primitively by at least one form of discriminant Δ.*

If it happens that all forms of discriminant Δ are equivalent, one then knows which numbers are represented primitively by the individual forms. However, this situation is rare, especially for elliptic forms where there are only the nine cases $\Delta = -3, -4, -7, -8, -11, -19, -43, -67, -163$. For hyperbolic forms there are many more, but they are still only a small proportion of all positive discriminants.

To begin we will reformulate the problem of primitive representability in a fixed discriminant as a congruence condition. Suppose a number n is represented primitively by some form $Q(x,y)$ of discriminant Δ, so n appears in the topograph of Q. If we look at an edge of the topograph bordering a region labeled n then we obtain an equation $\Delta = h^2 - 4nk$ where h is the label on the edge and k is the label on the region on the opposite side of this edge. The key observation is then that the equation $\Delta = h^2 - 4nk$ says precisely that Δ is congruent to h^2 modulo $4n$. Notice that if n is negative, "modulo $4n$" means the same thing as "modulo $4|n|$" since being divisible by a number d is equivalent to being divisible by $-d$ when we are considering both positive and negative numbers.



This in fact gives an exact criterion for primitive representability in a given discriminant:

Proposition 6.3. *Let two numbers n and Δ be given. Then the following two statements are equivalent*: (1) *There exists a form of discriminant Δ that represents n primitively.* (2) *Δ is congruent to a square modulo $4n$.*

Proof: As we saw above, if we have a form of discriminant Δ representing n primitively then by looking at the topograph we get an equation $\Delta = h^2 - 4nk$ for some integers h and k, and this equation says that Δ is the square of h modulo $4n$. Conversely, suppose that Δ is the square of some integer h modulo $4n$. This means that $h^2 - \Delta$ is an integer times $4n$, or in other words $h^2 - \Delta = 4nk$ for some k. This equation can also be written as $\Delta = h^2 - 4nk$. The three numbers n, h, and k can be used to construct a form whose topograph contains an edge with these three labels, for example $nx^2 + hxy + ky^2$ which has these three labels at the $1/0, 0/1$ edge. The discriminant of this form has the desired value $\Delta = h^2 - 4nk$, and the form represents n primitively since n appears as the label on a region in the topograph. □

Before proceeding further let us make a simple observation. If a form Q represents ± 1 or $\pm p$ for some prime p, then this must be a primitive representation since if it were nonprimitive then both variables x and y in this representation would be divisible by the same number $d > 1$ and hence $Q(x, y)$ would be divisible by d^2, which rules out ± 1 and $\pm p$ for primes p. Thus when we discuss representing ± 1 or $\pm p$ there will be no need to mention primitivity of the representation.

Also, for the problem of determining which numbers are represented primitively in a given discriminant it suffices to consider only representations of positive numbers since changing a form to its negative does not change the discriminant.

Let us see what the preceding proposition implies for small values of n. For $n = 1$ it says that there is a form of discriminant Δ representing 1 if and only if Δ is a square modulo 4. The squares modulo 4 are 0 and 1, and we already know that discriminants of forms are always congruent to 0 or 1 modulo 4. So we conclude that for every possible value of the discriminant there exists a form that represents 1. This isn't really new information, however, since the principal form $x^2 + dy^2$ or $x^2 + xy + dy^2$ represents 1 and there is a principal form for each discriminant.

In the next case $n = 2$ we will get some new information. The possible values of the discriminant modulo 8 are $0, 1, 4, 5$, and the squares modulo 8 are $0, 1, 4$ since $0^2 = 0$, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 \equiv 1$, and $(\pm 4)^2 \equiv 0$. Thus 2 is not represented by any form of discriminant congruent to 5 modulo 8, but for all other values of the discriminant there is a form representing 2. Explicit forms doing this are:

$$\begin{aligned} \Delta = 8k: &\quad 2x^2 - ky^2 \\ \Delta = 8k + 1: &\quad 2x^2 + xy - ky^2 \\ \Delta = 8k + 4: &\quad 2x^2 + 2xy - ky^2 \end{aligned}$$

Moving on to the next case $n = 3$, the discriminants modulo 12 are $0, 1, 4, 5, 8, 9$ and the squares modulo 12 are $0, 1, 4, 9$ since $0^2 = 0$, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 = 9$, $(\pm 4)^2 \equiv 4$, $(\pm 5)^2 \equiv 1$, and $(\pm 6)^2 \equiv 0$. The excluded discriminants are thus those congruent to 5 or 8 mod 12.

We could continue in this direction, exploring which discriminants have forms that represent a given number, but this is not really the question we want to answer, which is to start with a given discriminant, or even a given form, and decide which numbers it represents. The sort of answer we are looking for, based on the various examples we looked at earlier, is also a different sort of congruence condition, with congruence modulo the discriminant rather than congruence modulo $4n$. So there is more work to be done before we would have the sort of answer we want. Nevertheless, the representability criterion in the preceding proposition is the starting point.

An interesting consequence of the preceding proposition is the following:

Corollary 6.4. *If a number n is represented primitively in discriminant Δ then so is every divisor of n.*

Proof: This is based on a simple observation that we will use repeatedly:

If a congruence $a \equiv b$ holds mod n then it holds mod d for each divisor d of n.

This is true because if n divides $a - b$ then so does d for each divisor d of n.

Thus if $\Delta \equiv h^2$ mod $4n$, for some number h, then $\Delta \equiv h^2$ mod $4d$ whenever d divides n since $4d$ then divides $4n$. □

Representing Primes

The preceding corollary suggests a strategy for finding which numbers are represented primitively in a given discriminant Δ. First figure out which primes are represented (recall that representations of primes are automatically primitive), and then figure out which products of these primes are primitively represented. By the corollary these two steps will yield all numbers primitively represented in discriminant Δ.

Before pursuing this strategy let us first pause to derive a useful fact.

Lemma 6.5. *When n is odd, the condition that a discriminant Δ is congruent to a square mod $4n$ is equivalent to Δ being a square mod n.*

Proof: If $\Delta \equiv h^2$ mod $4n$ then certainly $\Delta \equiv h^2$ mod n, whether n is odd or even. For the less obvious converse, suppose that $\Delta \equiv h^2$ mod n. We can assume that h has the same parity as Δ since if it doesn't, we simply replace h by $h + n$ which has the opposite parity from h since n is odd, and then note that $(h+n)^2 \equiv h^2$ mod n. Since we always have $\Delta \equiv 0$ or 1 mod 4, we must have $\Delta = 4k$ or $\Delta = 4k + 1$, and since h has the same parity as Δ we have $h^2 = 4l$ or $h^2 = 4l + 1$ in these two cases. In either case $\Delta - h^2 = 4(k - l)$ so $\Delta - h^2$ is divisible by 4. It is also divisible by n by the assumption that $\Delta \equiv h^2$ mod n. Since n is odd, this implies that $\Delta - h^2$ is divisible by $4n$, so $\Delta \equiv h^2$ mod $4n$, which finishes the proof of the converse. □

Now we apply the preceding results to the first step of our program, which is to determine the primes that are represented in a given discriminant. One special case is easy:

Proposition 6.6. *For each prime p that divides the discriminant Δ there exists a form of discriminant Δ that represents p.*

Proof: First we deal with the special case $p = 2$. If 2 divides Δ then Δ is even so it is not 5 mod 8, hence from our earlier remarks we know there is a form of discriminant Δ representing 2.

In the remaining cases p is an odd prime dividing Δ and we wish to show that $\Delta \equiv h^2$ mod $4p$ for some number h. By the preceding lemma it suffices to find h satisfying $\Delta \equiv h^2$ mod p. But if p divides Δ then $\Delta \equiv 0$ mod p and we can simply take $h = 0$. □

At this point it will be convenient to introduce some shorthand notation. For p an odd prime and a an integer not divisible by p, define the *Legendre symbol* $\left(\frac{a}{p}\right)$ by

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } a \text{ is a square mod } p \\ -1 & \text{if } a \text{ is not a square mod } p \end{cases}$$

Using this notation we can say:

An odd prime p that does not divide Δ is representable by some form of discriminant Δ if and only if $\left(\frac{\Delta}{p}\right) = 1$.

It will therefore be useful to know how to compute $\left(\frac{a}{p}\right)$. The following four basic properties of the Legendre symbol will make this a feasible task:

(1) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(2) $\left(\frac{-1}{p}\right) = +1$ if $p \equiv 1$ mod 4 and $\left(\frac{-1}{p}\right) = -1$ if $p \equiv 3$ mod 4.

(3) $\left(\frac{2}{p}\right) = +1$ if $p \equiv \pm 1$ mod 8 and $\left(\frac{2}{p}\right) = -1$ if $p \equiv \pm 3$ mod 8.

(4) If p and q are distinct odd primes then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ unless p and q are both congruent to 3 mod 4, in which case $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Property (1), applied repeatedly, reduces the calculation of $\left(\frac{a}{p}\right)$ to the calculation of $\left(\frac{q}{p}\right)$ for the various prime factors q of a. Note that $\left(\frac{q^2}{p}\right) = +1$ so we can immediately reduce to the case that a is a product of distinct primes. Property (2) will be useful in dealing with negative discriminants, and property (3) will be used for certain even discriminants. Property (4), which is by far the most subtle of the four properties, is called *Quadratic Reciprocity*. Its proof is considerably more difficult than for the other three properties and will be given later in this chapter. Proofs of the first three properties will be obtained along the way.

For a quick illustration of the usefulness of these properties let us see how they can be used to compute the values of Legendre symbols. Suppose for example that one wanted to know whether 78 was a square mod 89. The naive approach would be to list the squares of all the numbers $\pm 1, \cdots, \pm 44$ and see whether any of these was congruent to 78 mod 89, but this would be rather tedious. Since 89 is prime we can instead evaluate $\left(\frac{78}{89}\right)$ using the basic properties of Legendre symbols. First we factor 78 to get $\left(\frac{78}{89}\right) = \left(\frac{2}{89}\right)\left(\frac{3}{89}\right)\left(\frac{13}{89}\right)$. By property (3) we have $\left(\frac{2}{89}\right) = +1$ since $89 \equiv 1 \bmod 8$. Next we apply reciprocity to get $\left(\frac{3}{89}\right) = \left(\frac{89}{3}\right)$ and $\left(\frac{13}{89}\right) = \left(\frac{89}{13}\right)$ since $89 \equiv 1 \bmod 4$. Next use the fact that $\left(\frac{a}{p}\right)$ depends only on the value of a mod p to reduce $\left(\frac{89}{3}\right)$ to $\left(\frac{2}{3}\right)$ and $\left(\frac{89}{13}\right)$ to $\left(\frac{11}{13}\right)$. Using property (3) again we have $\left(\frac{2}{3}\right) = -1$ (confirming the obvious fact that 2 is not a square mod 3). For $\left(\frac{11}{13}\right)$ reciprocity says this equals $\left(\frac{13}{11}\right)$. This reduces to $\left(\frac{2}{11}\right) = -1$. Summarizing, we have $\left(\frac{78}{89}\right) = \left(\frac{2}{89}\right)\left(\frac{3}{89}\right)\left(\frac{13}{89}\right) = (+1)(-1)(-1) = +1$ so 78 is a square mod 89, although this method does not actually produce a number x such that $x^2 \equiv 78 \bmod 89$.

Later in the chapter we will also see how to determine whether a number is a square mod a nonprime, showing how this reduces to the prime case.

Returning now to quadratic forms, let us see what the basic properties of Legendre symbols tell us about which primes are represented by the forms discussed at the beginning of the chapter. In the first four cases the class number is 1 so we will be determining which primes are represented by the given form.

Example: $x^2 + y^2$ with $\Delta = -4$. This form obviously represents 2, and it represents an odd prime p exactly when $\left(\frac{-4}{p}\right) = +1$. Using the first of the four properties we have $\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right)$, and the second property says this is $+1$ exactly for primes $p = 4k + 1$. Thus we see the primes represented by $x^2 + y^2$ are 2 and the primes $p = 4k + 1$.

Example: $x^2 + 2y^2$ with $\Delta = -8$. The only prime dividing Δ is 2, and it is representable. For odd primes p we have $\left(\frac{-8}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)^3 = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$. In the four cases $p \equiv 1, 3, 5, 7 \bmod 8$ this is, respectively, $(+1)(+1)$, $(-1)(-1)$, $(+1)(-1)$, and $(-1)(+1)$. We conclude that the primes representable by the form $x^2 + 2y^2$ are 2 and primes congruent to 1 or 3 mod 8.

Example: $x^2 - 2y^2$ with $\Delta = 8$. We have $\left(\frac{8}{p}\right) = \left(\frac{2}{p}\right)^3 = \left(\frac{2}{p}\right)$ so from property (3) we conclude that the primes represented by $x^2 - 2y^2$ are 2 and $p \equiv \pm 1 \bmod 8$.

Example: $x^2 + xy + y^2$ with $\Delta = -3$. The only prime dividing the discriminant is 3 and it is represented. The prime 2 is not represented since $\Delta \equiv 5 \bmod 8$. For primes $p > 3$ we can evaluate $\left(\frac{-3}{p}\right)$ using quadratic reciprocity, which says that $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ if $p = 4k + 1$ and $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$ if $p = 4k + 3$. Thus when $p = 4k + 1$ we have $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ and when $p = 4k + 3$ we have $\left(\frac{-3}{p}\right) = (-1)(-\left(\frac{p}{3}\right))$ so we get $\left(\frac{p}{3}\right)$ in both cases. Since $\left(\frac{p}{3}\right)$ only depends on p mod 3, we get $\left(\frac{p}{3}\right) = +1$ if $p \equiv 1 \bmod 3$ and $\left(\frac{p}{3}\right) = -1$ if $p \equiv 2 \bmod 3$. (Since $p \neq 3$ we do not need to consider the possibility $p \equiv 0 \bmod 3$.) The conclusion of all this is that the primes represented by $x^2 + xy + y^2$ are 3 and the primes $p \equiv 1 \bmod 3$.

Example: $\Delta = 40$. Here all forms are equivalent to either $x^2 - 10y^2$ or $2x^2 - 5y^2$. The primes dividing 40 are 2 and 5 so these are both represented by one form or the other, and in fact by $2x^2 - 5y^2$ as the topographs showed. For other primes p we have $\left(\frac{40}{p}\right) = \left(\frac{2}{p}\right)^3\left(\frac{5}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{p}{5}\right)$. The factor $\left(\frac{2}{p}\right)$ depends only on p mod 8 and $\left(\frac{p}{5}\right)$ depends only on p mod 5, so their product depends only on p mod 40. The following table lists all the possibilities for congruence classes mod 40 not divisible by 2 or 5:

	1	3	7	9	11	13	17	19	21	23	27	29	31	33	37	39
$\left(\frac{p}{5}\right)$	+1	−1	−1	+1	+1	−1	−1	+1	+1	−1	−1	+1	+1	−1	−1	+1
$\left(\frac{2}{p}\right)$	+1	−1	+1	+1	−1	−1	+1	−1	−1	+1	−1	−1	+1	+1	−1	+1

The product $\left(\frac{2}{p}\right)\left(\frac{p}{5}\right)$ is $+1$ in exactly the eight cases $p \equiv 1, 3, 9, 13, 27, 31, 37, 39$ mod 40. This agrees with our earlier observations based on the topographs. We conclude that these are the eight congruence classes containing primes (other than 2 and 5) represented by one of the two forms $x^2 - 10y^2$ and $2x^2 - 5y^2$. However, we have yet to verify our earlier guesses as to which of the two forms represents which of these eight congruence classes. The results in the next section will allow us to do this.

Our next goal will be to prove the following general statement that confirms something that we have observed in many examples so far:

Theorem 6.7. *For a non-square determinant Δ the odd primes not dividing Δ that are represented in discriminant Δ are the odd primes in exactly half of the congruence classes mod Δ of numbers coprime to Δ.*

The proof will rely on the following general fact commonly referred to as the *Chinese Remainder Theorem* since it was used in ancient Chinese manuscripts to solve mathematical puzzles of a certain type:

Proposition 6.8. *A collection of congruence conditions*

$$\begin{aligned} x &\equiv a_1 \ \ \textit{mod}\ m_1 \\ x &\equiv a_2 \ \ \textit{mod}\ m_2 \\ &\cdots \\ x &\equiv a_k \ \ \textit{mod}\ m_k \end{aligned}$$

always has a simultaneous solution provided that no two m_i's have a common divisor greater than 1. Moreover such a solution is unique modulo the product $m_1 \cdots m_k$.

The condition that the various moduli m_i are coprime is definitely a necessary hypothesis. For example, there is no common solution to the two congruences $x \equiv 5$ mod 6 and $x \equiv 7$ mod 15 since the first congruence implies $x \equiv 2$ mod 3 while the second congruence implies $x \equiv 1$ mod 3.

Proof: Let us first prove the existence of a common solution x when there are just two congruences $x \equiv a_1$ mod m_1 and $x \equiv a_2$ mod m_2. In this case the desired number x

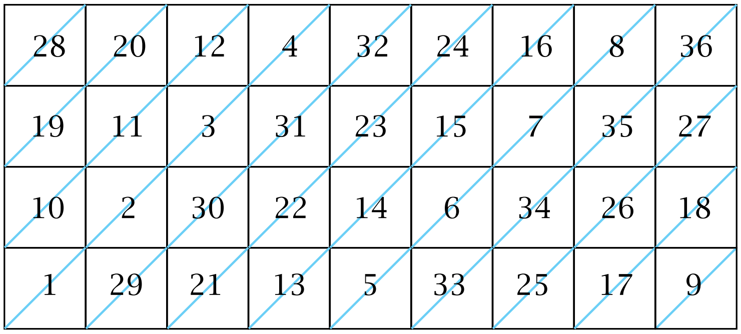
will have the form $x = a_1 + x_1m_1 = a_2 + x_2m_2$ for some pair of yet-to-be-determined numbers x_1 and x_2. We can rewrite the equation $a_1+x_1m_1 = a_2+x_2m_2$ as $a_2-a_1 = m_1x_1 - m_2x_2$. From our study of linear Diophantine equations in Chapter 2 we know that this equation has a solution (x_1, x_2) with integers x_1 and x_2 whenever m_1 and m_2 are coprime. This gives a simultaneous solution for the original two congruences $x \equiv a_1 \bmod m_1$ and $x \equiv a_2 \bmod m_2$, namely $x = a_1 + x_1m_1 = a_2 + x_2m_2$.

For more than two congruences we may suppose by induction that we have a number $x = a$ satisfying all but the last congruence $x \equiv a_k \bmod m_k$. From the preceding paragraph we know that a number x exists satisfying the two congruences $x \equiv a \bmod m_1 \cdots m_{k-1}$ and $x \equiv a_k \bmod m_k$. This gives the desired solution to all k congruences since $a \equiv a_i \bmod m_i$ for each $i < k$ by the inductive hypothesis.

Now we show that a simultaneous solution x of the given set of congruences is unique modulo $m_1 \cdots m_k$. Let y be another solution. Then the difference $x - y$ is congruent to 0 mod each of the numbers $m_1, \cdots, m_k$, which means that it is divisible by each m_i and hence by their product since they have no common factors. Thus $x \equiv y \bmod m_1 \cdots m_k$. □

There is another way to prove the existence of solutions in the Chinese Remainder Theorem by slightly more abstract reasoning. For this let us use the notation $[a]_m$ to denote the congruence class of an integer a mod m. Consider the function f defined by $f([a]_{m_1 \cdots m_k}) = ([a]_{m_1}, \cdots, [a]_{m_k})$. The domain of f is the set of congruence classes mod $m_1 \cdots m_k$ and the range of f is the set of k-tuples consisting of congruence classes mod m_1 up through m_k. Both the domain and range of f are finite sets with $m_1 \cdots m_k$ elements. It is a simple set theoretic fact that a function from one finite set S to another finite set T having the same number of elements as S is one-to-one if and if it is onto (where "one-to-one" means that no two elements of S are sent by the function to the same element of T, and "onto" means that every element of T occurs as the image of at least one element of S). In the last paragraph of the proof above we showed that the function f is one-to-one. Hence f is also onto, which is the assertion that the given set of k congruence conditions has a simultaneous solution.

It may be helpful to have a geometric picture to illuminate the Chinese Remainder Theorem. Consider the case of two simultaneous congruences $x \equiv a \bmod m$ and $x \equiv b \bmod n$. We can then label the mn unit squares in an $m \times n$ rectangle by the numbers 1 through mn, starting in the lower left corner and continuing upward to the right at a 45 degree angle as shown in the following figure for the case of a 4×9 rectangle:



28	20	12	4	32	24	16	8	36
19	11	3	31	23	15	7	35	27
10	2	30	22	14	6	34	26	18
1	29	21	13	5	33	25	17	9

Whenever we run over the top edge we jump back to the bottom in order to continue, and when we reach the right edge we jump back to the left edge. This amounts to taking congruence classes mod m horizontally and mod n vertically. What the Chinese Remainder Theorem says in this case is that each unit square in the rectangle is labeled exactly once by a number $1, \cdots, 36$. Here we are using the fact that 4 and 9 are coprime. (Without the coprimeness some grid points would have no labels while others would have multiple labels.) As the figure illustrates, specifying a congruence class mod 36 is equivalent to specifying a pair of congruence classes mod 4 and mod 9 via the projections onto the two axes.

For the case of three simultaneous congruences there is an analogous picture with a three-dimensional rectangular box partitioned into unit cubes. More generally, for k congruences one would be dealing with a k-dimensional box.

To illustrate one way in which the Chinese Remainder Theorem can be used let us show by an example how a Diophantine equation can have a solution mod n for each positive integer n and yet not have an actual integer solution. The example is the equation $2x^2 + 7y^2 = 1$. This obviously has no integer solutions, although it does have rational solutions such as $(x, y) = (1/3, 1/3)$ and $(3/5, 1/5)$. (These could be found by looking for integer solutions of $2x^2 + 7y^2 = z^2$, or in other words, squares z^2 in the topograph of $2x^2 + 7y^2$.) The rational solution $(1/3, 1/3)$ will give an integer solution mod n provided that 3 has a multiplicative inverse "$1/3$" mod n, which happens whenever 3 does not divide n. For example for $n = 22$ a multiplicative inverse for 3 is 15 since $3 \cdot 15 \equiv 1$ mod 22, and this leads to the solution $2 \cdot 15^2 + 7 \cdot 15^2 = 2025 \equiv 1$ mod 22. Thus we see that $2x^2 + 7y^2 = 1$ has a solution mod n whenever 3 does not divide n. Using the other rational solution $(3/5, 1/5)$ in a similar fashion we can solve $2x^2 + 7y^2 = 1$ mod n whenever 5 does not divide n by finding a multiplicative inverse for 5 mod n. Now if we factor an arbitrary n as $n_1 n_2$ where n_1 and n_2 are coprime and 3 does not divide n_1 and 5 does not divide n_2, then solutions (x_1, y_1) mod n_1 and (x_2, y_2) mod n_2 can be combined by applying the Chinese Remainder Theorem twice to give a pair (x, y) with $(x, y) \equiv (x_1, y_1)$ mod n_1 and $(x, y) \equiv (x_2, y_2)$ mod n_2, so we have $2x^2 + 7y^2 \equiv 1$

mod n_1 and mod n_2, hence also mod n.

Let us consider now a special case of the Chinese Remainder Theorem where we start with a number n factored into primes as $n = p_1^{r_1} \cdots p_k^{r_k}$ for distinct primes $p_1, \cdots, p_k$. We can then consider a set of k congruences $x \equiv a_i$ mod m_i where now $m_i = p_i^{r_i}$. Let us now impose the added condition that each a_i is not divisible by the corresponding prime p_i. A simultaneous solution $x = a$ for all k congruences must then be coprime to n since $a \equiv a_i$ mod $p_i^{r_i}$ implies $a \equiv a_i$ mod p_i and we assume a_i is nonzero mod p_i so a is also nonzero mod p_i. Since this holds for each i, this says that a is coprime to n. Conversely, if a is coprime to n and satisfies a set of congruences $a \equiv a_i$ mod $p_i^{r_i}$ and hence $a \equiv a_i$ mod p_i, then a_i must be nonzero mod p_i since a is. Thus congruence classes mod n of numbers a coprime to n are equivalent to congruence classes mod $p_i^{r_i}$ of numbers a_i coprime to p_i, one for each i.

In the geometric picture for the case $k = 2$ with a rectangular array of unit squares, when we require a_1 to be coprime to p_1 we are omitting the numbers in certain vertical columns of squares, the columns whose horizontal coordinate is a multiple of p_1. Similarly, when we require a_2 to be coprime to p_2 we omit the numbers in the horizontal rows whose vertical coordinate is a multiple of p_2. The numbers in the boxes that are not omitted are then the numbers coprime to $n = p_1^{r_1} p_2^{r_2}$. Here is the picture for the case $n = 2^2 \cdot 3^2$ that we showed earlier:

28	20	12	4	32	24	16	8	36
19	11	3	31	23	15	7	35	27
10	2	30	22	14	6	34	26	18
1	29	21	13	5	33	25	17	9

For $k = 3$ we would be omitting the cubes in certain slices parallel to the three coordinate planes, and similarly for $k > 3$.

The function which assigns to each positive integer n the number of congruence classes mod n of numbers coprime to n is called the *Euler phi function* $\varphi(n)$. The arguments above involving the Chinese Remainder Theorem show that $\varphi(n) = \varphi(p_1^{r_1}) \cdots \varphi(p_k^{r_k})$ when $n = p_1^{r_1} \cdots p_k^{r_k}$ for distinct primes p_i. For a prime p we have $\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$ since we are counting how many numbers remain from $1, 2, \cdots, p^r$ when we delete $p, 2p, \cdots, (p^{r-1})p = p^r$. Thus there is an explicit formula for $\varphi(n)$ in terms of the prime factorization of n.

To prove the earlier theorem about primes represented in a given discriminant we will need also the following fact:

Lemma 6.9. *For a power q^r of an odd prime q exactly half of the congruence classes mod q^r of numbers a not divisible by q satisfy $\left(\frac{a}{q}\right) = +1$.*

Proof: First we do the case $r = 1$. The $q-1$ nonzero congruence classes mod q are exactly $\pm1, \pm2, \cdots, \pm(q-1)/2$. The squares $(\pm1)^2$, $(\pm2)^2, \cdots, (\pm(q-1)/2)^2$ are all distinct since if $a^2 \equiv b^2$ mod q then q divides $a^2 - b^2 = (a-b)(a+b)$, so since q is prime it must divide either $a-b$ or $a+b$ which means that either $a \equiv b$ or $a \equiv -b$ mod q.

When $r > 1$ the congruence classes mod q^r we are counting are obtained from the numbers a in the interval $[1, q-1]$ with $\left(\frac{a}{q}\right) = +1$ by translating these numbers into the intervals $[q+1, 2q-1]$, then $[2q+1, 3q-1]$, and so on. Thus we again obtain half of the congruence classes mod q^r of numbers not divisible by q. □

Proof of Theorem 6.7: Let us write $\Delta = \varepsilon\, 2^s p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ where $\varepsilon = \pm1$, $s \ge 0$, and each p_i is an odd prime. (We allow the possibility $k = 0$ so that $\Delta = \varepsilon 2^s$.) The criterion for an odd prime p to be representable in discriminant Δ is that $\left(\frac{\Delta}{p}\right) = +1$. We have $\left(\frac{\Delta}{p}\right) = \left(\frac{\varepsilon}{p}\right)\left(\frac{2}{p}\right)^s\left(\frac{p_1}{p}\right)^{r_1}\cdots\left(\frac{p_k}{p}\right)^{r_k}$. Quadratic reciprocity implies that $\left(\frac{p_1}{p}\right)^{r_1}\cdots\left(\frac{p_k}{p}\right)^{r_k} = \left(\frac{\omega}{p}\right)\left(\frac{p}{p_1}\right)^{r_1}\cdots\left(\frac{p}{p_k}\right)^{r_k}$ where ω is $+1$ or -1 according to whether there are an even or an odd number of primes $p_i \equiv 3$ mod 4 with odd exponent r_i. Thus we have $\left(\frac{\Delta}{p}\right) = \left(\frac{\varepsilon}{p}\right)\left(\frac{\omega}{p}\right)\left(\frac{2}{p}\right)^s\left(\frac{p}{p_1}\right)^{r_1}\cdots\left(\frac{p}{p_k}\right)^{r_k}$.

By the Chinese Remainder Theorem the congruence class of a number n mod Δ is uniquely determined by its congruence classes mod 2^s and mod $q_i^{r_i}$ for each i, and these congruence classes can be varied independently. We are interested in numbers n coprime to Δ, and we call such numbers n *admissible*. If we choose for each i a number a_i not divisible by q_i (we call such an a_i *admissible* as well) and we also choose an odd number a if $s > 0$, then there exists a number n with $n \equiv a_i$ mod $q_i^{r_i}$ for each i and also $n \equiv a$ mod 2^s when $s > 0$. Such an n is admissible since $n \equiv a_i$ mod $q_i^{r_i}$ implies $n \equiv a_i$ mod q_i.

Now we break the proof up into several cases. The first case is that $s = 0$, so Δ is odd and hence $\Delta \equiv 1$ mod 4. This implies that $\varepsilon = \omega$ so the formula for $\left(\frac{\Delta}{p}\right)$ simplifies to $\left(\frac{p}{p_1}\right)^{r_1}\cdots\left(\frac{p}{p_k}\right)^{r_k}$. There must be at least one odd r_i since if $\varepsilon = +1$ we are assuming Δ is not a square, while if $\varepsilon = -1$ we have $\omega = -1$ which implies the existence of at least one odd r_i.

For all the other indices $j \ne i$ let us fix a choice of admissible a_j mod $p_j^{r_j}$. Restricting p to be congruent to a_j mod $p_j^{r_j}$ determines the value of all the terms in the product $\left(\frac{\varepsilon}{p}\right)\left(\frac{\omega}{p}\right)\left(\frac{2}{p}\right)^s\left(\frac{p}{p_1}\right)^{r_1}\cdots\left(\frac{p}{p_k}\right)^{r_k}$ except the one term $\left(\frac{p}{q_i}\right)^{r_i}$. By the lemma, this term will have the value $+1$ for p in half of the admissible choices of congruence classes for a_i mod $q_i^{r_i}$ and -1 for the other half. This means that the product $\left(\frac{p}{q_1}\right)^{r_1}\cdots\left(\frac{p}{q_l}\right)^{r_l}$ has the value $+1$ for half the admissible choices for a_i and -1 for the other half, where we are still keeping the other a_j's fixed. Since this "half and half" property holds for each fixed choice of the other a_j's, it therefore also holds when all the admissible choices for a_j's are taken together. Thus we have $\left(\frac{\Delta}{p}\right) = +1$ for exactly half of the admissible congruence classes of numbers p mod Δ. This proves the theorem when $s = 0$.

From now on we can assume $s > 0$ so Δ is even and hence $s \geq 2$ since $\Delta \equiv 0$ mod 4.

If some r_i is odd we proceed much as in the first case that $s = 0$. We fix admissible numbers a_j mod $p_j^{r_j}$ for $j \neq i$ and we also fix an odd number a mod 2^s. We again restrict p to be congruent to a_j mod $p_j^{r_j}$ and we also require p to be congruent to a mod 2^s. The latter condition determines $\left(\frac{\varepsilon}{p}\right)$ and $\left(\frac{\omega}{p}\right)$ since $s \geq 2$. It also determines $\left(\frac{2}{p}\right)^s$ since this is $+1$ when $s = 2$ and when $s \geq 3$ we know that $\left(\frac{2}{p}\right)$ depends only on p mod 8. Now all terms in $\left(\frac{\varepsilon}{p}\right)\left(\frac{\omega}{p}\right)\left(\frac{2}{p}\right)^s\left(\frac{p}{p_1}\right)^{r_1}\cdots\left(\frac{p}{p_k}\right)^{r_k}$ are determined except for the one term $\left(\frac{p}{q_i}\right)^{r_i}$, so the earlier "half and half" argument works to finish this case.

The next case is that all the r_i's are even and s is odd, hence $s \geq 3$. The formula for $\left(\frac{\Delta}{p}\right)$ then reduces to just $\left(\frac{\varepsilon}{p}\right)\left(\frac{2}{p}\right)$. The value of this product depends only on p mod 8. In both the cases $\varepsilon = +1$ and $\varepsilon = -1$ the value of $\left(\frac{\varepsilon}{p}\right)\left(\frac{2}{p}\right)$ is $+1$ for two of the four odd numbers mod 8 and -1 for the other two odd numbers. By an argument like one earlier in the proof, this implies that $\left(\frac{\varepsilon}{p}\right)\left(\frac{2}{p}\right)$ is $+1$ for p congruent to half the odd numbers mod 2^s and -1 for the other half. Then by the same reasoning $\left(\frac{\Delta}{p}\right)$ is $+1$ for p in half the admissible congruence classes mod Δ and $= 1$ in the other half.

The last remaining case is that all r_i's are even and s is also even. Then $\left(\frac{\Delta}{p}\right) = \left(\frac{\varepsilon}{p}\right)$ and we must have $\varepsilon = -1$ since Δ is not a square. In this case $\left(\frac{\Delta}{p}\right)$ is again $+1$ for p in half the admissible congruence classes and -1 in the other half. □

Genus and Characters

Recall the term "genus" that was introduced earlier: If two forms of the same discriminant cannot be distinguished by looking only at their values modulo the discriminant, then one says the two forms have the same genus, or belong to the same genus. Our aim now is to pin down more precisely what this means.

In an earlier example illustrating the use of Legendre symbols we saw that primes represented by either of the two forms $x^2 - 10y^2$ and $2x^2 - 5y^2$ of discriminant 40, other than the prime divisors 2 and 5 of 40, belong to eight of the sixteen congruence classes mod 40 not containing numbers divisible by 2 or 5. In four of these eight cases the product $\left(\frac{p}{5}\right)\left(\frac{2}{p}\right)$ was $(+1)(+1)$, namely the cases $p \equiv \pm 1, \pm 9$, and in the other four cases it was $(-1)(-1)$, namely $p \equiv \pm 3, \pm 13$. From the topographs it appears that the primes $p \equiv \pm 1, \pm 9$ are represented by $x^2 - 10y^2$ while $p \equiv \pm 3, \pm 13$

are represented by $2x^2 - 5y^2$. The following proposition will tell us this is indeed true, and could be predicted even before looking at the topographs:

Proposition 6.10. *Let Q be a form of discriminant Δ and let p be an odd prime dividing Δ. Then the Legendre symbol $\left(\frac{n}{p}\right)$ has the same value for all numbers n in the topograph of Q that are not divisible by p.*

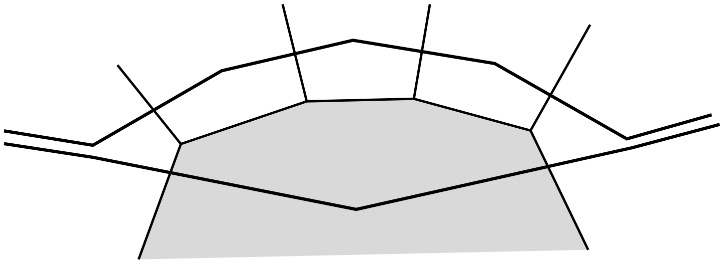
Before proving the proposition let us see how it applies in the case $\Delta = 40$ with $p = 5$. According to the proposition, the value of $\left(\frac{n}{5}\right)$ must be constant in the topograph of each of the forms $x^2 - 10y^2$ and $2x^2 - 5y^2$, leaving aside values of the forms that are divisible by 5. To determine the value of $\left(\frac{n}{5}\right)$ for each form it therefore suffices to compute it for a single number n in the topograph not divisible by 5. The simplest thing is just to compute it for $(x, y) = (1, 0)$ or $(0, 1)$. Choosing $(1, 0)$, for $x^2 - 10y^2$ we have $\left(\frac{1}{5}\right) = +1$ and for $2x^2 - 5y^2$ we have $\left(\frac{2}{5}\right) = -1$. The proposition then implies that all values n in the topograph of $x^2 - 10y^2$ not divisible by 5 have $\left(\frac{n}{5}\right) = +1$, hence $n \equiv \pm 1 \bmod 5$, while for $2x^2 - 5y^2$ we have $\left(\frac{n}{5}\right) = -1$, hence $n \equiv \pm 2 \bmod 5$. This implies that when we compute the product $\left(\frac{p}{5}\right)\left(\frac{2}{p}\right)$ for primes $p \neq 2, 5$ represented by $x^2 - 10y^2$ we must get $(+1)(+1)$ while for $2x^2 - 5y^2$ we must get $(-1)(-1)$ since in both cases the product $\left(\frac{p}{5}\right)\left(\frac{2}{p}\right)$ must equal $+1$. Thus we are able to tell exactly which primes each of these two forms represents.

Proof of the Proposition: For an edge in the topograph labeled h with adjacent regions labeled n and k we have $\Delta = h^2 - 4nk$. If p is a prime dividing Δ this implies that $4nk \equiv h^2 \bmod p$. Thus if neither n nor k is divisible by p and p is odd we have $\left(\frac{4nk}{p}\right) = +1$. Since $\left(\frac{4nk}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{n}{p}\right)\left(\frac{k}{p}\right)$ and $\left(\frac{4}{p}\right) = +1$ this implies $\left(\frac{n}{p}\right) = \left(\frac{k}{p}\right)$. In other words, the symbol $\left(\frac{n}{p}\right)$ takes the same value on any two adjacent regions of the topograph of Q labeled by numbers not divisible by p. To finish the proof we will use the following fact:

Lemma 6.11. *Given a form Q and a prime p dividing the discriminant of Q, then any two regions in the topograph of Q where the value of Q is not divisible by p can be connected by a path passing only through such regions.*

Assuming this, the proposition easily follows since we have seen that the value of $\left(\frac{n}{p}\right)$ is the same for any two adjacent regions with label not divisible by p. □

Proof of the Lemma: Let us call regions in the topograph of Q whose label is not divisible by p *good* regions, and the other regions *bad* regions. We can assume that at least one region is good, otherwise there is nothing to prove. What we will show is that no two bad regions can be adjacent. Thus a path in the topograph from one good region to another cannot pass through two consecutive bad regions, and if it does pass through a bad region then a detour around this region allows this bad region to be avoided, creating a new path passing through one fewer bad region as in the following figure:



By repeating this detouring process as often as necessary we eventually obtain a path avoiding bad regions entirely, still starting and ending at the same two given good regions.

To see that no two adjacent regions are bad, suppose this is false, so there are two adjacent regions whose Q values n and k are both divisible by p. If the edge separating these two regions is labeled h then we have an equation $\Delta = h^2 - 4nk$, and since we assume p divides Δ this implies that p divides h as well as n and k. Thus the form $nx^2 + hxy + ky^2$ is equal to p times another form. This implies that all regions in the topograph are bad. However we assumed this was not the case, so we conclude that there are no adjacent bad regions. □

A useful observation is that the value of $\left(\frac{n}{p}\right)$ for numbers n in the topograph of a form $ax^2 + bxy + cy^2$ with discriminant divisible by p can always be determined just by looking at the coefficients. This is because the coefficients a and c appear in adjacent regions of the topograph, so if both these coefficients were divisible by p, this would imply that b was also divisible by p (since p divides $b^2 - 4ac$) so the whole form would be divisible by p. Excluding this uninteresting possibility, we see that at least one of a and c is not divisible by p and we can use this to compute $\left(\frac{n}{p}\right)$.

Let us look at another example, the discriminant $\Delta = -84 = -2^2 \cdot 3 \cdot 7$ with three different prime factors. For this discriminant there are four different equivalence classes of forms: $Q_1 = x^2 + 21y^2$, $Q_2 = 3x^2 + 7y^2$, $Q_3 = 2x^2 + 2xy + 11y^2$, and $Q_4 = 5x^2 + 4xy + 5y^2$. The topographs of these forms were shown earlier in the chapter. To see which odd primes are represented in discriminant -84 we compute:

$$\left(\frac{-84}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{4}{p}\right)\left(\frac{7}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{7}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)\left(\frac{p}{7}\right)$$

As in the example of $\Delta = 40$ we can make a table of the values of these Legendre symbols for the 24 numbers mod 84 that are not divisible by the prime divisors $2, 3, 7$ of 84. Using the fact that the squares mod 3 are $(\pm 1)^2 = 1$ and the squares mod 7 are $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, and $(\pm 3)^2 \equiv 2$, we obtain the table below:

	1	5	11	13	17	19	23	25	29	31	37	41
$\left(\frac{-1}{p}\right)$	$+1$	$+1$	-1	$+1$	$+1$	-1	-1	$+1$	$+1$	-1	$+1$	$+1$
$\left(\frac{p}{3}\right)$	$+1$	-1	-1	$+1$	-1	$+1$	-1	$+1$	-1	$+1$	$+1$	-1
$\left(\frac{p}{7}\right)$	$+1$	-1	$+1$	-1	-1	-1	$+1$	$+1$	$+1$	-1	$+1$	-1
	Q_1	Q_4	Q_3		Q_4	Q_2	Q_3	Q_1		Q_2	Q_1	Q_4

	43	47	53	55	59	61	65	67	71	73	79	83
$\left(\frac{-1}{p}\right)$	-1	-1	$+1$	-1	-1	$+1$	$+1$	-1	-1	$+1$	-1	-1
$\left(\frac{p}{3}\right)$	$+1$	-1	-1	$+1$	-1	$+1$	-1	$+1$	-1	$+1$	$+1$	-1
$\left(\frac{p}{7}\right)$	$+1$	-1	$+1$	-1	-1	-1	$+1$	$+1$	$+1$	-1	$+1$	-1
				Q_2					Q_3			

The twelve cases when the product $\left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)\left(\frac{p}{7}\right)$ is $+1$ give the congruence classes of primes not dividing Δ that are represented by one of the four forms, and we can determine which form it is by looking at the values of $\left(\frac{p}{3}\right)$ and $\left(\frac{p}{7}\right)$ for each of the four forms. As noted earlier, these values can be computed directly from the coefficients of x^2 and y^2 that are not divisible by 3 for $\left(\frac{p}{3}\right)$ or by 7 for $\left(\frac{p}{7}\right)$. For example, for $Q_2 = 3x^2+7y^2$ the coefficient of y^2 tells us that $\left(\frac{p}{3}\right) = \left(\frac{7}{3}\right) = +1$ and the coefficient of x^2 tells us that $\left(\frac{p}{7}\right) = \left(\frac{3}{7}\right) = -1$. Thus we have $(\left(\frac{p}{3}\right), \left(\frac{p}{7}\right)) = (+1,-1)$ for Q_2, and in a similar way we find that $(\left(\frac{p}{3}\right), \left(\frac{p}{7}\right))$ is $(+1,+1)$ for $Q_1 = x^2 + 21y^2$, $(-1,+1)$ for $Q_3 = 2x^2 + 2xy + 11y^2$, and $(-1,-1)$ for $Q_4 = 5x^2 + 4xy + 5y^2$.

The table above is called the *character table* for the discriminant $\Delta = -84$. Each row can be regarded as a function assigning a number ± 1 to each congruence class of numbers n having no common divisors with Δ. Such a function is called a *character* for the given discriminant. For each odd prime p dividing Δ there is a character given by the Legendre symbol $\left(\frac{n}{p}\right)$. There is sometimes also a character associated to the prime 2 in a somewhat less transparent way. In the example $\Delta = -84$ this is the character defined by the first row of the table, which assigns the values $+1$ to numbers $n = 4k+1$ and -1 to numbers $n = 4k+3$. We will denote this character by χ_4 to indicate that its values $\chi_4(n) = \pm 1$ depend only on the value of n mod 4. Thus $\chi_4(p) = \left(\frac{-1}{p}\right)$ when p is an odd prime, but $\chi_4(n)$ is defined for all odd numbers n, not just primes. One can check that an explicit formula for χ_4 is $\chi_4(n) = (-1)^{(n-1)/2}$ although we will not be needing this formula.

In the example with $\Delta = 40$ the character corresponding to the prime 2 is given by the second row in the character table, the row labeled $\left(\frac{2}{p}\right)$. This character associates the value $+1$ to an odd number $n \equiv \pm 1$ mod 8 and the value -1 when $n \equiv \pm 3$ mod 8. We will denote it by χ_8 since its values $\chi_8(n) = \pm 1$ depend only on n mod 8. We have $\chi_8(p) = \left(\frac{2}{p}\right)$ for all odd primes p, but $\chi_8(n)$ is defined for all odd numbers n. There is again an explicit formula $\chi_8(n) = (-1)^{(n^2-1)/8}$ that we will not use.

By analogy we can also introduce the notation χ_p for the earlier character defined by $\chi_p(n) = \left(\frac{n}{p}\right)$ for p an odd prime not dividing n.

Another case we looked at was $\Delta = -56$ where there were three inequivalent forms $Q_1 = x^2 + 14y^2$, $Q_2 = 2x^2 + 7y^2$, and $Q_3 = 3x^2 + 2xy + 5y^2$. Here we have $\left(\frac{-56}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{7}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{p}{7}\right)$. The two characters are thus χ_8 (with $\chi_8(p) = \left(\frac{2}{p}\right)$) and χ_7 (with $\chi_7(p) = \left(\frac{p}{7}\right)$). The character table is:

	1	3	5	9	11	13	15	17	19	23	25	27
χ_8	$+1$	-1	-1	$+1$	-1	-1	$+1$	$+1$	-1	$+1$	$+1$	-1
χ_7	$+1$	-1	-1	$+1$	$+1$	-1	$+1$	-1	-1	$+1$	$+1$	-1
	$\binom{Q_1}{Q_2}$	Q_3	Q_3	$\binom{Q_1}{Q_2}$		Q_3	$\binom{Q_1}{Q_2}$		Q_3	$\binom{Q_1}{Q_2}$	$\binom{Q_1}{Q_2}$	Q_3

	29	31	33	37	39	41	43	45	47	51	53	55
χ_8	-1	$+1$	$+1$	-1	$+1$	$+1$	-1	-1	$+1$	-1	-1	$+1$
χ_7	$+1$	-1	-1	$+1$	$+1$	-1	$+1$	-1	-1	$+1$	$+1$	-1
					$\binom{Q_1}{Q_2}$			Q_3				

From the character table we see that $\left(\frac{2}{p}\right)\left(\frac{p}{7}\right)$ is $(+1)(+1)$ for $p \equiv 1, 9, 15, 23, 25, 39$ mod 56 and $(-1)(-1)$ for $p \equiv 3, 5, 13, 19, 27, 45$ mod 56. Thus primes in these twelve congruence classes are represented in discriminant -56, as are 2 and 7, the prime divisors of 56. Moreover, from the values of $\left(\frac{p}{7}\right)$ we deduce that primes $p \equiv 1, 9, 15, 23, 25, 39$ mod 56 are represented by Q_1 or Q_2 while primes $p \equiv 3, 5, 13, 19, 27, 45$ mod 56 are represented by Q_3. The forms Q_1 and Q_2 are not distinguished by characters, and so they belong to the same genus.

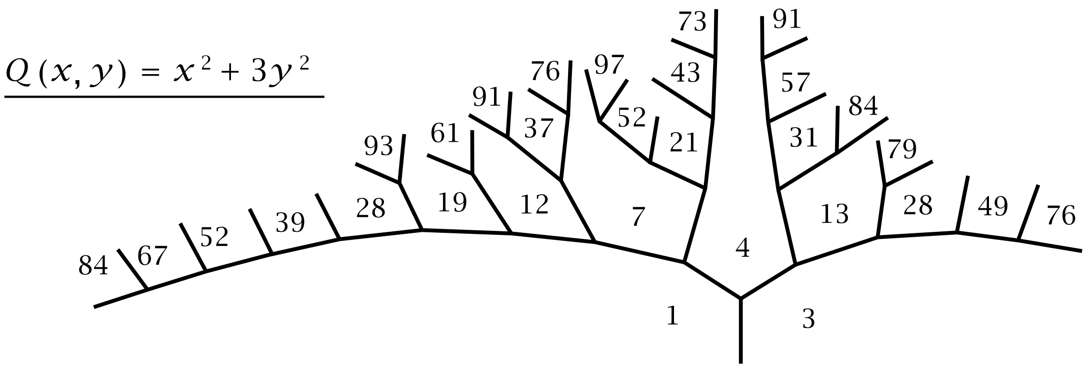
Let us consider now how characters can be associated to the prime 2 in general. Since characters arise from primes that divide the discriminant, this means we are interested in even discriminants. These are always multiples of 4, so we can write the discriminant as $\Delta = 4\delta$. The criterion for a number n to be represented primitively in discriminant Δ is that Δ is a square mod $4n$, so $\Delta = 4\delta = h^2 - 4nk$ for some integers h and k. This equation forces h to be even, say $h = 2l$, so the condition becomes $4\delta = 4l^2 - 4nk$ or just $\delta = l^2 - nk$, that is, δ is a square mod n. By analogy with the construction of characters for odd primes, we wish to see what the equation $\delta = l^2 - nk$ says about values n and k in adjacent regions of a topograph where neither n nor k is divisible by the prime in question. For the prime 2 this means we assume n and k are odd.

There will turn out to be six different cases. The first two are when δ is odd, which means that Δ is divisible by 4 but not 8. In these two cases we consider congruences mod 4, the highest power of 2 dividing Δ. Since δ is odd and both n and k are odd, the congruence $\delta \equiv l^2 - nk$ mod 4 implies that l must be even, so $l^2 \equiv 0$ mod 4 and the congruence can be written as $nk \equiv -\delta$ mod 4.

Case 1: $\delta = 4m - 1$. The congruence condition is then $nk \equiv 1$ mod 4. This says that $n \equiv k$ mod 4, otherwise we would have $nk \equiv -1$ since the only possibilities for n and k mod 4 are 1 and -1. Thus the previous lemma implies that the character χ_4 assigning $+1$ to integers $4s + 1$ and -1 to integers $4s - 1$ has the same value for all odd numbers in the topograph of a form of discriminant $\Delta = 4(4m - 1)$.

An example for this case is the discriminant $\Delta = -84$ considered earlier, where the first row of the character table gave the values for χ_4.

Case 2: $\delta = 4m + 1$. The difference from the previous case is that the congruence condition is now $nk \equiv -1 \bmod 4$ and hence $n \equiv -k \bmod 4$. This means the mod 4 value of odd numbers in the topograph is not constant, and so we do not get a character for the prime 2. As an example, consider $\Delta = -12$. Here there is one primitive form $x^2 + 3y^2$ and one non-primitive form $2x^2 + 2xy + 2y^2$.



As one can see, there are odd numbers in the topograph of $x^2 + 3y^2$ congruent to both 1 and 3 mod 4. We might try to fix this problem by considering odd numbers mod 8 instead of mod 4 but this does not help since the topograph contains numbers congruent to each of $1, 3, 5, 7$ mod 8. Trying congruences modulo higher powers of 2 does not help either.

The absence of a character for the prime 2 when $\delta = 4m + 1$ could perhaps be predicted from the calculation of $\left(\frac{\delta}{p}\right)$. Since δ is odd we have $\delta = p_1 \cdots p_r$ for odd primes p_i and $\left(\frac{\delta}{p}\right) = \left(\frac{p_1}{p}\right) \cdots \left(\frac{p_r}{p}\right)$. This equals $\left(\frac{p}{p_1}\right) \cdots \left(\frac{p}{p_r}\right)$ since the number of p_i's congruent to 3 mod 4 is even when $\delta = 4m + 1$. Thus the value of $\left(\frac{\delta}{p}\right)$ depends only on the characters associated to the odd prime factors of Δ.

There remain the cases that δ is even. The next two cases are when Δ is divisible by 8 but not by 16. After that is the case that Δ is divisible by 16 but not by 32, and finally the case that Δ is divisible by 32. In all these cases we will consider congruences mod 8, so the equation $\delta = l^2 - nk$ becomes $\delta \equiv l^2 - nk \bmod 8$. Since δ is now even while n and k are still odd, this congruence implies l is odd, and so $l^2 \equiv 1 \bmod 8$ and the congruence can be written as $nk \equiv 1 - \delta \bmod 8$. Since $k^2 \equiv 1$ mod 8 when k is odd, we can multiply both sides of the congruence $nk \equiv 1 - \delta$ by k to obtain the equivalent congruence $n \equiv (1 - \delta)k \bmod 8$.

Case 3: $\delta \equiv 2 \bmod 8$. The congruence is then $n \equiv -k \bmod 8$. It follows that in the topograph of a form of discriminant $\Delta = 4(8m + 2)$ either the odd numbers must all be congruent to ± 1 mod 8 or they must all be congruent to ± 3 mod 8. Thus the character χ_8 which takes the value $+1$ on numbers $8s \pm 1$ and -1 on numbers $8s \pm 3$ has a constant value, either $+1$ or -1, for all odd numbers in the topograph.

An example for this case is $\Delta = 40$. Here the two rows of the character table computed earlier gave the values for χ_5 and χ_8.

Case 4: $\delta \equiv 6 \bmod 8$. Now the congruence $n \equiv (1-\delta)k \bmod 8$ becomes $n \equiv -5k$ or $n \equiv 3k \bmod 8$. This implies that all odd numbers in the topograph of a form of discriminant $\Delta = 4(8m+6)$ must be congruent to 1 or $3 \bmod 8$, or they must all be congruent to 5 or $7 \bmod 8$. The character associated to the prime 2 in this case has the value $+1$ on numbers $8s+1$ and $8s+3$, and the value -1 on numbers $8s+5$ and $8s+7$. We have not encountered this character previously, so let us give it the new name χ_8'. However, it is not entirely new since it is actually just the product $\chi_4\chi_8$ as one can easily check by evaluating this product on $1, 3, 5$, and 7.

A simple example is $\Delta = -8$ with class number 1. Here we have $\left(\frac{\delta}{p}\right) = \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$ which equals $+1$ for $p \equiv 1, 3 \bmod 8$ and -1 for $p \equiv 5, 7 \bmod 8$ so this is just the character χ_8'.

Another example is $\Delta = 24$ where there are the two forms $Q_1 = x^2 - 6y^2$ and $Q_2 = 6x^2 - y^2$. We have $\left(\frac{\delta}{p}\right) = \left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)$. The character table is

	1	5	7	11	13	17	19	23
χ_8'	$+1$	-1	-1	$+1$	-1	$+1$	$+1$	-1
χ_3	$+1$	-1	$+1$	-1	$+1$	-1	$+1$	-1

Thus Q_1 represents primes $p \equiv 1, 19 \bmod 24$ and Q_2 represents primes $p \equiv 5, 23 \bmod 24$.

Case 5: $\delta \equiv 4 \bmod 8$. Now we have the congruence $n \equiv -3k \bmod 8$. Thus in the topograph of a form of discriminant $\Delta = 4(8m+4)$ all odd numbers must be congruent to 1 or $5 \bmod 8$, or they must all be congruent to 3 or $7 \bmod 8$. More simply, one can say that all odd numbers in the topograph must be congruent to $1 \bmod 4$ or they must all be congruent to $3 \bmod 4$. Thus we obtain the character χ_4 again.

An example is $\Delta = -48$ where we have the two forms $Q_1 = x^2 + 12y^2$ and $Q_2 = 3x^2 + 4y^2$ as well as the non-primitive form $Q_3 = 2x^2 + 6y^2$. We have $\left(\frac{\delta}{p}\right) = \left(\frac{-12}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$. This is the character χ_3. We also have the character χ_4 that we just described. The character table is

	1	5	7	11	13	17	19	23	25	29	31	35	37	41	43	47
χ_4	$+1$	$+1$	-1	-1	$+1$	$+1$	-1	-1	$+1$	$+1$	-1	-1	$+1$	$+1$	-1	-1
χ_3	$+1$	-1	$+1$	-1	$+1$	-1	$+1$	-1	$+1$	-1	$+1$	-1	$+1$	-1	$+1$	-1
	Q_1		Q_2		Q_1		Q_2		Q_1		Q_2		Q_1		Q_2	

In contrast with earlier examples, the representability of a prime $p > 3$ in discriminant -48 is determined by one character, χ_3, and the other character χ_4 serves only to decide which of the forms Q_1 and Q_2 achieves the representation. Note that χ_4 says nothing about the non-primitive form Q_3 whose values are all even. On the other hand, from χ_3 we can deduce that all values of Q_3 not divisible by 3 must be congruent to $2 \bmod 3$.

Case 6: $\delta \equiv 0 \bmod 8$, so Δ is a multiple of 32. In this case the congruence $n \equiv (1-\delta)k \bmod 8$ becomes simply $n \equiv k \bmod 8$. Thus all odd numbers in the topograph of a form of discriminant $\Delta = 32m$ must lie in the same congruence class mod 8. The two characters χ_4 and χ_8 can now both occur independently, as shown in the following chart listing their values on the four classes $1, 3, 5, 7$ mod 8:

	1	3	5	7
χ_4	$+1$	-1	$+1$	-1
χ_8	$+1$	-1	-1	$+1$

As an example consider the discriminant $\Delta = -32$. Here there are two primitive forms $Q_1 = x^2 + 8y^2$ and $Q_2 = 3x^2 + 2xy + 3y^2$ along with one non-primitive form $Q_3 = 2x^2 + 4y^2$. We have $\left(\frac{\delta}{p}\right) = \left(\frac{-8}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$ with the two factors being the two independent characters for the prime 2. The full character table is then just a four-fold repetition of the previous shorter table:

	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
χ_4	$+1$	-1	$+1$	-1	$+1$	-1	$+1$	-1	$+1$	-1	$+1$	-1	$+1$	-1	$+1$	-1
χ_8	$+1$	-1	-1	$+1$	$+1$	-1	-1	$+1$	$+1$	-1	-1	$+1$	$+1$	-1	-1	$+1$
	Q_1	Q_2			Q_1	Q_2			Q_1	Q_2			Q_1	Q_2		

This finishes the analysis of the six cases for characters associated to the prime 2. It might be worth noting that if one restricts attention to fundamental discriminants then only the cases 1, 3, and 4 can arise since in the other three cases there always exist non-primitive forms of the given discriminant.

We have now defined a set of characters for each discriminant Δ, with one character for each odd prime dividing Δ and either zero, one, or two characters for the prime 2 when Δ is even. This collection of characters assigns a symbol $(\pm 1, \pm 1, \cdots, \pm 1)$ to each number n coprime to Δ, with one coordinate $\chi_i(n) = \pm 1$ for each character χ_i.

Proposition 6.12. *For each discriminant Δ the number of congruence classes mod Δ having a given symbol $(\pm 1, \pm 1, \cdots, \pm 1)$ is the same for each symbol.*

Proof: By the Chinese Remainder Theorem we can regard congruence classes mod Δ as collections of congruence classes mod a power of a prime for each prime-power factor of Δ. Thus it suffices to consider each prime divisor of Δ separately. Suppose we change the sign of one coordinate $\chi_i(n) = \pm 1$ of the symbol and keep the sign for the other characters the same. In the case that $\chi_i = \chi_p$ for an odd prime p dividing Δ with exponent r we have $\chi_p(n) = \left(\frac{n}{p}\right)$ and we know that there are the same number of congruence classes mod p^r with $\left(\frac{n}{p}\right) = +1$ as with $\left(\frac{n}{p}\right) = -1$. This also holds for the characters χ_4, χ_8, and χ_8'. Thus changing coordinates of a symbol $(\pm 1, \pm 1, \cdots, \pm 1)$ one at a time never changes the number of congruence classes with that symbol. □

Since characters have constant values on all numbers in a topograph coprime to the discriminant, we can associate a well-defined symbol $(\pm 1, \pm 1, \cdots, \pm 1)$ to each equivalence class of forms of a given discriminant.

With this terminology we can define a *genus* to be the collection of all forms in a given discriminant having the same associated symbol. A priori the number of genera in discriminant Δ is therefore 2^κ where κ is the number of characters in discriminant Δ. However, not all symbols are actually realizable by forms and the number of non-empty genera is only half as big:

Theorem. *The number of genera of primitive forms of discriminant Δ is $2^{\kappa-1}$ where κ is the number of characters in discriminant Δ.*

To prove this requires going considerably deeper into the theory than we have done so far, so we will not attempt it here.

We have used characters to help determine the representability of primes not dividing the discriminant. For the finitely many primes that do divide the discriminant, the forms that represent them can be determined just by examining the various topographs. However, characters can also be used to do this, at least in some cases. Let us illustrate this by looking again at discriminant -84 where there are three characters χ_4, χ_3, and χ_7, associated to the three prime divisors 2, 3, and 7 of 84. For determining which form represents 2 we can use the characters χ_3 and χ_7. We have $\chi_3(2) = \left(\frac{2}{3}\right) = -1$ and $\chi_7(2) = \left(\frac{2}{7}\right) = +1$. From the earlier character table we see that of the four forms Q_1, Q_2, Q_3, Q_4 only Q_3 has this pair of values, so we conclude that Q_3 must be the form that represents 2, and indeed this is what the topographs show. In a similar way, to check which form represents 3 we use the values $\chi_4(3) = -1$ and $\chi_7(3) = -1$, and the character table then says that Q_2 must be the form representing 3. For representing 7 we have $\chi_4(7) = -1$ and $\chi_3(7) = +1$ so it must again be Q_2 that represents 7.

Representing Non-primes

We have been focusing on determining which primes are represented in a given discriminant, and now we turn to the corresponding problem for non-primes. Our general criterion is that a number n is represented primitively by at least one form of discriminant Δ if and only if Δ is a square mod $4n$. As we noted before, this implies that if n is primitively represented in discriminant Δ, then so is every divisor of n, and in particular every prime divisor. The question we address now is to what extent the converse holds, that is, if the prime divisors of n are primitively represented, then is n also primitively represented?

The main result in this subsection will be an answer to this question:

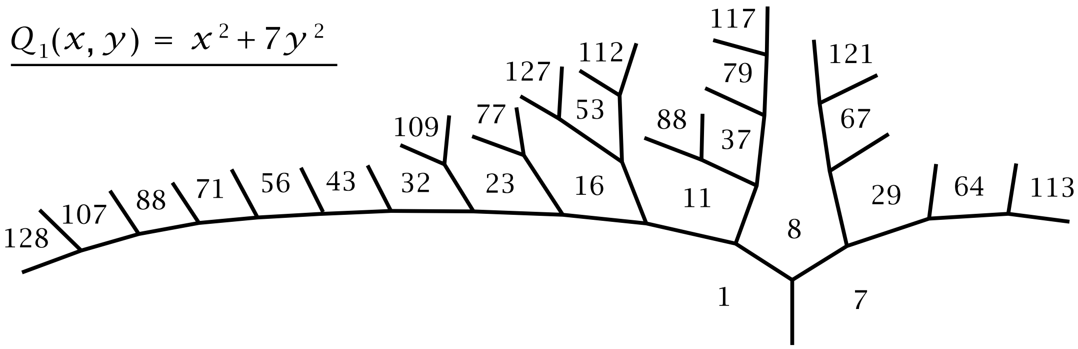
Theorem 6.13. *A number $n > 1$ is primitively represented by at least one form of discriminant Δ exactly when n factors as a product $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ of powers* *of distinct primes p_i each of which is represented by some form of discriminant Δ, where the exponents e_i of the primes p_i not dividing Δ are unrestricted, while for primes p_i dividing Δ we have $e_i \leq 1$ in the cases that Δ is a fundamental discriminant. If Δ is not a fundamental discriminant the condition on the exponents e_i of primes p_i dividing Δ is more complicated: First write $\Delta = p_i^s q$ with p_i^s the highest power of p_i dividing Δ. Then if p_i is odd the condition on e_i is that either (a) $e_i \leq s$ or (b) $e_i \geq s+1$ and s is even and $\left(\frac{q}{p_i}\right) = +1$. If $p_i = 2$ then the condition on e_i is that either (a) $e_i \leq s-2$ or (b) s is even and one of the following three possibilities holds: (1) $e_i = s-1$, (2) $e_i = s$ and $q = 4l+1$, or (3) $e_i \geq s+1$ and $q = 8l+1$.*

This finishes the story for the representation problem in the cases of fundamental discriminants for which all forms are equivalent, such as those at the first level of complexity that we considered at the beginning of the chapter.

Before proving the theorem let us look at some examples to illustrate the more complicated case of nonfundamental discriminants.

Example: $\Delta = -12$. The two forms here are $Q_1 = x^2+3y^2$ and the nonprimitive form $Q_2 = 2x^2+2xy+2y^2$. The primes represented in discriminant -12 are 2, 3, and primes p with $\left(\frac{-12}{p}\right) = \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = +1$, so these are the primes $p \equiv 1$ mod 3. The theorem says that the numbers represented primitively in discriminant -12 are the numbers $n = 2^a 3^b p_1 \cdots p_k$ with $a \leq 2$, $b \leq 1$, and each p_i a prime congruent to 1 mod 3. (When we apply the theorem for $p_i = 2$ we have $s = 2$ and $q = -3$, and for $p_i = 3$ we have $s = 1$.) We can in fact determine which of Q_1 and Q_2 is giving these representations. The form Q_2 is twice x^2+xy+y^2 and we have already determined which numbers the latter form represents primitively, namely the products $3^b p_1 \cdots p_k$ with $b \leq 1$ and each prime $p_i \equiv 1$ mod 3. Thus, of the numbers represented primitively by Q_1 or Q_2, the numbers represented primitively by Q_2 are those with $a = 1$. None of these numbers with $a = 1$ are represented by Q_1 since x^2+3y^2 is never 2 mod 4, as x^2 and y^2 must be 0 or 1 mod 4.

Example: $\Delta = -28$. Here the only two forms up to equivalence are $Q_1 = x^2+7y^2$ and $Q_2 = 2x^2+2xy+4y^2$ which is not primitive. The primes represented in discriminant -28 are 2, 7, and odd primes p with $\left(\frac{-28}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right) = +1$ so $p \equiv 1,2,4$ mod 7. According to the theorem the numbers represented primitively by Q_1 or Q_2 are the numbers $n = 2^a 7^b p_1 \cdots p_k$ with $b \leq 1$ and odd primes $p_i \equiv 1,2,4$ mod 7. There is no restriction on a since when we apply the theorem with $p_i = 2$ we have $s = 2$ and $q = -7 = 8l+1$. We can say exactly which numbers are primitively represented by Q_2 since it is twice the form $x^2+xy+2y^2$ of discriminant -7, which is a fundamental discriminant of class number 1 so the theorem tells us which numbers this form represents primitively, namely the numbers $7^b p_1 \cdots p_k$ with $b \leq 1$ and primes $p_i \equiv 1,2,4$ mod 7, including now the possibility $p_i = 2$. Thus Q_2 represents primitively exactly the numbers $2^a 7^b p_1 \cdots p_k$ with $a \geq 1$, $b \leq 1$ and odd primes $p_i \equiv 1, 2, 4 \bmod 7$. Hence Q_1 must represent primitively at least the numbers $2^a 7^b p_1 \cdots p_k$ with $a = 0$, $b \leq 1$, and odd primes $p_i \equiv 1, 2, 4 \bmod 7$. These numbers are all odd since $a = 0$, but Q_1 also represents some even numbers since $x^2 + 7y^2$ is even whenever both x and y are odd.



From the topograph we might conjecture that Q_1 represents primitively exactly the numbers $2^a 7^b p_1 \cdots p_k$ with $a = 0$ or $a \geq 3$, and with $b \leq 1$ and the same odd primes $p_i \equiv 1, 2, 4 \bmod 7$ as before. It is not difficult to exclude $a = 1$ and $a = 2$ by considering the values of $x^2 + 7y^2 \bmod 4$ and mod 8. In the next chapter we will show that all the conjectured numbers with $a \geq 3$ are in fact primitively represented by Q_1.

Now we turn to proving the theorem, using the familiar criterion that a number n is primitively represented by at least one form of discriminant Δ if and only if Δ is a square mod $4n$. As a first step we have:

Lemma 6.14. *If a number x is a square mod m_1 and is also a square mod m_2 where m_1 and m_2 are coprime, then x is a square mod $m_1 m_2$.*

For example, the number 2 is a square mod 7 (since $3^2 \equiv 2 \bmod 7$) and also mod 17 (since $6^2 \equiv 2 \bmod 17$) so 2 must also be a square mod $7 \cdot 17 = 119$. And in fact $2 \equiv 11^2 \bmod 119$.

Proof: This will follow from the Chinese Remainder Theorem. Suppose that a number x is a square mod m_1 and is also a square mod m_2 where m_1 and m_2 are coprime. This means there are numbers a_1 and a_2 such that $x \equiv a_1^2 \bmod m_1$ and $x \equiv a_2^2 \bmod m_2$. By the Chinese Remainder Theorem there exists a number a that is congruent to a_1 mod m_1 and to a_2 mod m_2. Then $x \equiv a_1^2 \equiv a^2 \bmod m_1$ and $x \equiv a_2^2 \equiv a^2 \bmod m_2$. This implies $x \equiv a^2 \bmod m_1 m_2$ since the difference $x - a^2$ is divisible by both m_1 and m_2 and hence by their product $m_1 m_2$ since we assume m_1 and m_2 are coprime. This shows that x is a square mod $m_1 m_2$. □

As a simple application of the preceding lemma we can deduce that if a discriminant Δ is a square modulo an odd number n then it is a square mod $4n$ since discriminants are always squares mod 4, being either 0 or 1 mod 4. Earlier we proved this fact using a special argument, but now we see that it follows from a more general principle.

The preceding lemma reduces the problem of primitive representation in a fixed discriminant to the case of representing prime powers. It remains to reduce further from prime powers to just primes themselves. For most primes this will be possible using the following result:

Lemma 6.15. *If a number x is a square mod p for an odd prime p not dividing x, then x is also a square mod p^r for each $r > 1$. The corresponding statement for the prime $p = 2$ is that if an odd number x is a square mod 8 then x is also a square mod 2^r for each $r > 3$.*

For example, 2 is a square mod 7 since $2 \equiv 3^2$ mod 7, so 2 is also a square mod 7^2, namely $2 \equiv 10^2$ mod 49. It is also a square mod $7^3 = 343$ since $2 \equiv 108^2$ mod 343. Likewise it must be a square mod 7^4, mod 7^5, etc. The proof of the lemma will give a method for refining the initial congruence $2 \equiv 3^2$ mod 7 to each subsequent congruence $2 \equiv 10^2$ mod 49, $2 \equiv 108^2$ mod 343, etc.

For the prime $p = 2$ we have to begin with squares mod 8 since 3 is a square mod 2 but not mod 4, while 5 is a square mod 4 but not mod 8.

Proof of the Lemma: We will show that if x is a square mod p^r then it is also a square mod p^{r+1}, assuming $r \geq 1$ in the case that p is odd and $r \geq 3$ in the case $p = 2$. By induction this will prove the lemma.

We begin by assuming that x is a square mod p^r, so there is a number y such that $x \equiv y^2$ mod p^r or in other words p^r divides $x - y^2$, say $x - y^2 = p^r l$ for some integer l. We seek a number z such that $x \equiv z^2$ mod p^{r+1}, so it is reasonable to look for a z with $z \equiv y$ mod p^r, or in other words $z = y + kp^r$ for some k. Thus we want to choose k so that $x \equiv (y + kp^r)^2$ mod p^{r+1}. This means we want p^{r+1} to divide the number

$$\begin{aligned} x - (y + kp^r)^2 &= x - (y^2 + 2kp^r y + k^2 p^{2r}) \\ &= (x - y^2) - 2kp^r y - k^2 p^{2r} \\ &= p^r l - 2kp^r y - k^2 p^{2r} \\ &= p^r(l - 2ky - k^2 p^r) \end{aligned}$$

For this to be divisible by p^{r+1} means that p should divide $l - 2ky - k^2 p^r$. Since we assume $r \geq 1$ this is equivalent to p dividing $l - 2ky$, or in other words, $l - 2ky = pq$ for some integer q. Rewriting this as $l = 2yk + pq$ we see that this linear Diophantine equation with unknowns k and q always has a solution when p is odd since $2y$ and p are coprime if p is odd, in view of the fact that p does not divide y since $x \equiv y^2$ mod p^r and we assume x is not divisible by p. This finishes the induction step in the case that p is odd.

When $p = 2$ this argument breaks down at the last step since the equation $l = 2yk + pq$ becomes $l = 2yk + 2q$ and this will not have a solution when l is odd. To modify the proof so that it works for $p = 2$ we would like to get rid of the factor 2 in the equation $l = 2yk + pq$ which arose when we squared $y + kp^r$. To do this, suppose that instead of trying $z = y + k \cdot 2^r$ we try $z = y + k \cdot 2^{r-1}$. Then we would want 2^{r+1} to divide

$$\begin{aligned} x - (y + k \cdot 2^{r-1})^2 &= (x - y^2) - k \cdot 2^r y - k^2 2^{2r-2} \\ &= 2^r l - k \cdot 2^r y - k^2 2^{2r-2} \\ &= 2^r (l - ky - k^2 2^{r-2}) \end{aligned}$$

Assuming $r \geq 3$, this means 2 should divide $l - ky$, or in other words $l = yk + 2q$ for some integer q. The number y is odd since $y^2 \equiv x \bmod 2^r$ and x is odd by assumption. This implies the equation $l = yk + 2q$ has a solution (k, q). □

Corollary 6.16. *If a prime p not dividing the discriminant Δ is represented by at least one form of discriminant Δ then every power of p is represented primitively in discriminant Δ.*

Proof: First assume that p is odd. Since we assume p is represented in discriminant Δ we know that Δ is a square mod p. The preceding lemma then says that Δ is a square mod each power of p, so all powers of p are also represented in discriminant Δ. For $p = 2$ the argument is almost the same. In this case the representability of 2 implies that Δ is a square mod $4p = 8$ so the lemma implies that Δ is also a square mod all higher powers of 2, so all powers of 2 are represented in discriminant Δ. □

Now let p be a prime that does divide the discriminant Δ. In this case we know there is a form of discriminant Δ representing p (primitively), and it remains to determine whether powers of p are also represented primitively.

Lemma 6.17. *For a given prime p suppose that a number x divisible by p factors as $p^s q$ where p does not divide q, so p^s is the largest power of p dividing x. Then:*
(a) x is a square mod p^r for each $r \leq s$.
(b) If $r > s$ and s is odd then x is not a square mod p^r.
(c) If $r > s$ and s is even then x is a square mod p^r if and only if q is a square mod p^{r-s}.

Proof: Part (a) is easy since x is 0 mod p^s hence also mod p^r if $r \leq s$, and 0 is always a square mod anything.

For (b) we assume $r > s$ and s is odd. Suppose $p^s q$ is a square mod p^r, so $p^s q = y^2 + lp^r$ for some integers y and l. Then p^s divides $y^2 + lp^r$ and it divides lp^r (since $r > s$) so p^s divides y^2. Since s is assumed to be odd and the exponent of p in y^2 must be even, this implies p^{s+1} divides y^2. It also divides lp^r since $s + 1 \leq r$, so from the equation $p^s q = y^2 + lp^r$ we conclude that p divides q, contrary to definition of q. This contradiction shows that $p^s q$ is not a square mod p^r when $r > s$ and s is odd, so statement (b) is proved.

For (c) we assume $r > s$ and s is even. As in part (b), if $p^s q$ is a square mod p^r we again have an equation $p^s q = y^2 + lp^r$ and this implies that p^s divides y^2. Since s is now even, this means $y^2 = p^s z^2$ for some number z. Canceling p^s from $p^s q = y^2 + lp^r$ yields an equation $q = z^2 + lp^{r-s}$, which says that q is a square mod p^{r-s}. Conversely, if q is a square mod p^{r-s} we have an equation $q = z^2 + lp^{r-s}$ and hence $p^s q = p^s z^2 + lp^r$. Since s is even, this says that $p^s q$ is a square mod p^r. □

Corollary 6.18. *Let p be a prime dividing the discriminant Δ, and let us write $\Delta = p^s q$ with p^s the highest power of p dividing Δ. If p is odd then p^r is primitively represented in discriminant Δ if and only if either (a) $r \le s$ or (b) s is even and $\left(\frac{q}{p}\right) = +1$. If $p = 2$ then 2^r is primitively represented in discriminant Δ if and only if either (a) $r \le s - 2$ or (b) s is even and one of the following three possibilities holds: $r = s - 1$; $r = s$ and $q = 4k + 1$; or $r \ge s + 1$ and $q = 8k + 1$.*

Proof: When p is odd this follows immediately from the lemma by taking $x = \Delta$, using the fact that q is a square mod powers of p exactly when it is a square mod p.

When $p = 2$ we need to determine when Δ is a square mod $4 \cdot 2^r = 2^{r+2}$. By the lemma this happens only when $r \le s - 2$ or when s is even and q (which is odd) is a square mod 2^{r+2-s}. When $r + 2 - s = 1$, so $r = s - 1$, every q is a square mod $2^{r+2-s} = 2$. When $r + 2 - s = 2$, so $r = s$, q is a square mod $2^{r+2-s} = 4$ only when $q = 4k + 1$. And when $r + 2 - s \ge 3$, so $r \ge s + 1$, q is a square mod 2^{r+2-s} only when $q = 8k + 1$. □

Corollary 6.19. *If Δ is a fundamental discriminant and p is a prime dividing Δ, then no power p^r with $r > 1$ is primitively represented in discriminant Δ.*

Proof: First suppose p is odd. Then $p^2 \equiv 1$ mod 4 so if p^2 divided a discriminant Δ, the quotient Δ/p^2 would be congruent to Δ mod 4 so it would also be a discriminant. Thus a fundamental discriminant Δ can have no odd square factors, so in the preceding corollary we must have $s = 1$ when p is odd, which implies $r \le 1$ as well. In the case $p = 2$ we must have $s \le 3$ if Δ is a fundamental discriminant since otherwise $\Delta/4$ would also be a discriminant. We cannot have $s = 1$ since this would mean $\Delta \equiv 2$ mod 4. If $s = 2$ then in case (b) of the preceding corollary the possibilities $q = 4k + 1$ and $q = 8k + 1$ occur only when $\Delta/4$ is a discriminant, so this is ruled out as well. The only possibility remaining is $r = 1$. □

Putting together the preceding lemmas and corollaries, we have now proved the theorem.

Proof of Quadratic Reciprocity

First let us show that quadratic reciprocity can be expressed more concisely as a single formula

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{[\frac{p-1}{2}][\frac{q-1}{2}]} \qquad (*)$$

Here p and q are distinct odd primes. Since they are odd, the fractions $\frac{p-1}{2}$ and $\frac{q-1}{2}$ are integers. The only way the exponent $[\frac{p-1}{2}][\frac{q-1}{2}]$ can be odd is for both factors to be odd, so $\frac{p-1}{2} = 2k+1$ and $\frac{q-1}{2} = 2l+1$. These equations can be rewritten as $p = 4k+3$ and $q = 4l+3$. Thus the only time that the right side of the formula $(*)$ can be -1 is when p and q are both congruent to 3 mod 4, and quadratic reciprocity is the assertion that the left side of $(*)$ has exactly this property.

There will be three main steps in the proof of quadratic reciprocity. The first is to derive an explicit algebraic formula for $\left(\frac{a}{p}\right)$ due originally to Euler. The second step is to use this formula to give a somewhat more geometric interpretation of $\left(\frac{a}{p}\right)$ in terms of the number of dots in a certain triangular pattern. Then the third step is the actual proof of quadratic reciprocity using symmetry properties of the patterns of dots. This proof is due to Eisenstein, first published in 1844, simplifying an earlier proof by Gauss who was the first to give a full proof of quadratic reciprocity.

Step 1. In what follows we will always use p to denote an odd prime, and the symbol a will always denote an arbitrary nonzero integer not divisible by p. When we write a congruence such as $a \equiv b$ this will always mean congruence mod p, even if we do not explicitly say mod p.

Euler's formula is:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$$

For example, for $p = 11$ Euler's formula says $\left(\frac{2}{11}\right) = 2^5 = 32 \equiv -1 \bmod 11$ and $\left(\frac{3}{11}\right) = 3^5 = 243 \equiv +1 \bmod 11$. These are the correct values since the squares mod 11 are $(\pm1)^2 = 1$, $(\pm2)^2 = 4$, $(\pm3)^2 = 9$, $(\pm4)^2 \equiv 5$, and $(\pm5)^2 \equiv 3$.

Note that Euler's formula determines the value of $\left(\frac{a}{p}\right)$ uniquely since $+1$ and -1 are not congruent mod p since $p > 2$. It is not immediately obvious that the number $a^{\frac{p-1}{2}}$ should always be congruent to either $+1$ or -1 mod p, but when we prove Euler's formula we will see that this has to be true.

As a special case, taking $a = -1$ in Euler's formula gives the calculation

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{if } p = 4k+1 \\ -1 & \text{if } p = 4k+3 \end{cases}$$

Before proving Euler's formula we will need to derive a few preliminary general facts about congruences modulo a prime p. The first fact is that each of the numbers $a = 1, 2, \cdots, p-1$ has a multiplicative inverse mod p. To see why this is true, notice that each such a is coprime to p, so we know from Chapter 2 that the equation

$ax + py = 1$ has an integer solution (x, y). This equation can be rewritten as the congruence $ax \equiv 1 \bmod p$, which says that x is an inverse for $a \bmod p$. Note that any two choices for x here are congruent mod p since if $ax \equiv 1$ and $ax' \equiv 1$ then multiplying both sides of $ax' \equiv 1$ by x gives $xax' \equiv x$, and $xa \equiv 1$ so we conclude that $x \equiv x'$.

Which numbers equal their own inverse mod p? If $a \cdot a \equiv 1$, then we can rewrite this as $a^2 - 1 \equiv 0$, or in other words $(a+1)(a-1) \equiv 0$. This is certainly a valid congruence if $a \equiv \pm 1$, so suppose that $a \not\equiv \pm 1$. The factor $a+1$ is then not congruent to 0 mod p so it has a multiplicative inverse mod p, and if we multiply the congruence $(a+1)(a-1) \equiv 0$ by this inverse, we get $a - 1 \equiv 0$ so $a \equiv 1$, contradicting the assumption that $a \not\equiv \pm 1$. This argument shows that the only numbers among $1, 2, \cdots, p-1$ that are congruent to their inverses mod p are 1 and $p-1$.

An application of this fact is a result known as *Wilson's Theorem*:

$(p-1)! \equiv -1$ modulo p whenever p is prime.

To see why this is true, observe that in the product $(p-1)! = (1)(2)\cdots(p-1)$ each factor other than 1 and $p-1$ can be paired up with its multiplicative inverse mod p and these two terms multiply together to give 1 mod p, so the whole product is congruent to just $(1)(p-1)$ mod p. Since $p - 1 \equiv -1$ mod p this gives Wilson's Theorem.

Now let us prove the following congruence known as *Fermat's Little Theorem*:

$$a^{p-1} \equiv 1 \quad \text{mod } p \;\text{ whenever } p \text{ is an odd prime not dividing } a.$$

To see this, note first that the numbers $a, 2a, 3a, \cdots, (p-1)a$ are all distinct mod p since we know that a has a multiplicative inverse mod p, so in a congruence $ma \equiv na$ we can multiply both sides by the inverse of a to deduce that $m \equiv n$. Let us call this property that $ma \equiv na$ implies $m \equiv n$ the *cancellation property* for congruences mod p.

Thus the set $\{a, 2a, 3a, \cdots, (p-1)a\}$ is the same mod p as $\{1, 2, 3, \cdots, p-1\}$ since both sets have $p-1$ elements and neither set contains numbers that are 0 mod p. If we take the product of all the numbers in each of these two sets we obtain the congruence

$$(a)(2a)(3a)\cdots(p-1)a \equiv (1)(2)(3)\cdots(p-1) \quad \text{mod } p$$

We can cancel the factors $2, 3, \cdots, p-1$ from both sides by repeated applications of the cancellation property. The result is the congruence $a^{p-1} \equiv 1$ claimed by Fermat's Little Theorem.

Now we can prove Euler's formula for $\left(\frac{a}{p}\right)$. The first case is that $\left(\frac{a}{p}\right) = 1$, so a is a square mod p and $a \equiv x^2$ for some $x \not\equiv 0$. In this case we have $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1$ by Fermat's Little Theorem. So in this case Euler's formula $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$ is valid, both sides being $+1$.

The other case is that $\left(\frac{a}{p}\right) = -1$ so a is not a square mod p. Observe first that the congruence $xy \equiv a$ has a solution y mod p for each $x \not\equiv 0$ since x has an inverse x^{-1} mod p so we can take $y = x^{-1}a$. Moreover the solution y is unique mod p since $xy_1 \equiv xy_2$ implies $y_1 \equiv y_2$ by the cancellation property. Since we are in the case that a is not a square mod p the solution y of $xy \equiv a$ satisfies $y \not\equiv x$. Thus the numbers $1, 2, 3, \cdots, p-1$ are divided up into $\frac{p-1}{2}$ pairs $\{x_1, y_1\}$, $\{x_2, y_2\}$, $\cdots$, $\{x_{\frac{p-1}{2}}, y_{\frac{p-1}{2}}\}$ with $x_i y_i \equiv a$ for each i. Multiplying all these $\frac{p-1}{2}$ pairs together, we get

$$a^{\frac{p-1}{2}} \equiv x_1 y_1 x_2 y_2 \cdots x_{\frac{p-1}{2}} y_{\frac{p-1}{2}}$$

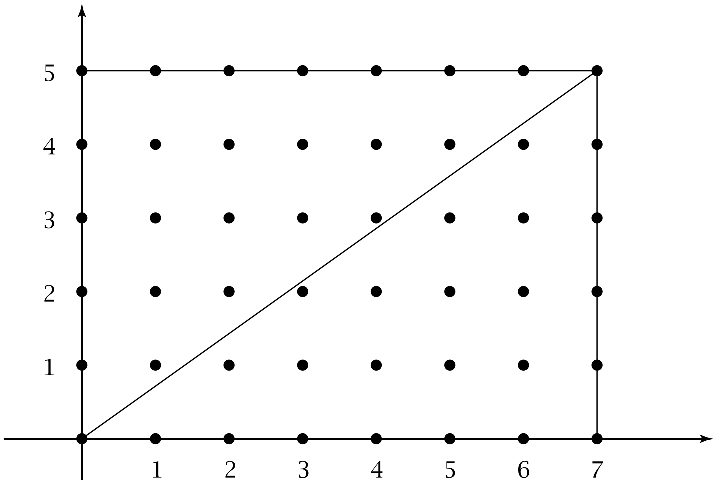
The product on the right is just a rearrangement of $(1)(2)(3)\cdots(p-1)$, and Wilson's Theorem says that this product is congruent to -1 mod p. Thus we see that Euler's formula $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$ holds also when $\left(\frac{a}{p}\right) = -1$, completing the proof in both cases.

A consequence of Euler's formula is the multiplicative property of Legendre symbols that we stated and used earlier in the chapter:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

This holds since $(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}}$.

Step 2. Here our aim is to express the Legendre symbol $\left(\frac{a}{p}\right)$ in more geometric terms. To begin, consider a rectangle in the first quadrant of the xy-plane that is p units wide and a units high, with one corner at the origin and the opposite corner at the point (p, a). For example for $p = 7$ and $a = 5$ we have the picture

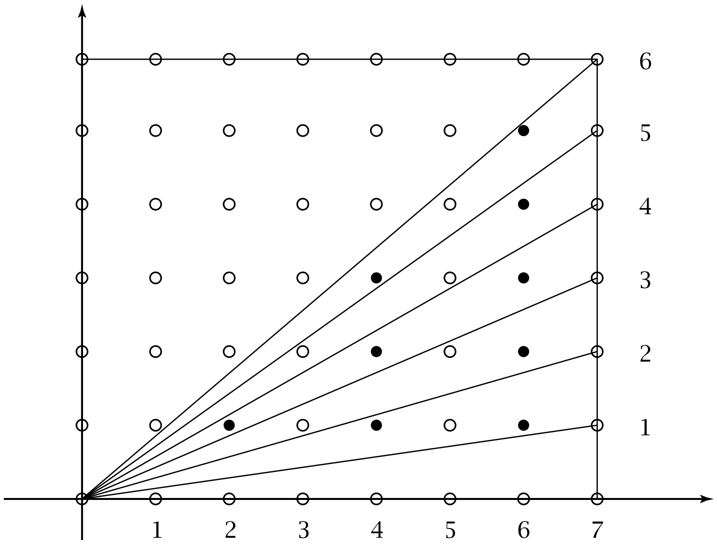


We will be interested in points that lie strictly in the interior of the rectangle and whose coordinates are integers. Points satisfying the latter condition are called *lattice points*. The number of lattice points in the interior is then $(p-1)(a-1)$ since their x-coordinates can range from 1 to $p-1$ and their y-coordinates from 1 to $a-1$, independently.

The diagonal of the rectangle from $(0,0)$ to (p, a) does not pass through any of these interior lattice points since we assume that the prime p does not divide a, so the fraction a/p, which is the slope of the diagonal, is in lowest terms. (If there were an interior lattice point on the diagonal, the slope of the diagonal would be a fraction with numerator and denominator smaller than a and p.) Since there are no interior lattice points on the diagonal, exactly half of the lattice points inside the rectangle lie on each side of the diagonal, so the number of lattice points below the diagonal is $\frac{1}{2}(p-1)(a-1)$. This is an integer since p is odd, which makes $p-1$ even.

A more refined question one can ask is how many lattice points below the diagonal have even x-coordinate and how many have odd x-coordinate. Here there is no guarantee that these two numbers must be equal, and indeed if they were equal then both numbers would have to be $\frac{1}{4}(p-1)(a-1)$ but this fraction need not be an integer, for example when $p=7$ and $a=4$.

We denote the number of lattice points that are below the diagonal and have even x-coordinate by the letter e. Here is a figure showing the values of e when $p=7$ and a ranges from 1 to 6:



a	e	$\left(\frac{a}{7}\right)$
6	9	−1
5	7	−1
4	6	+1
3	3	−1
2	2	+1
1	0	+1

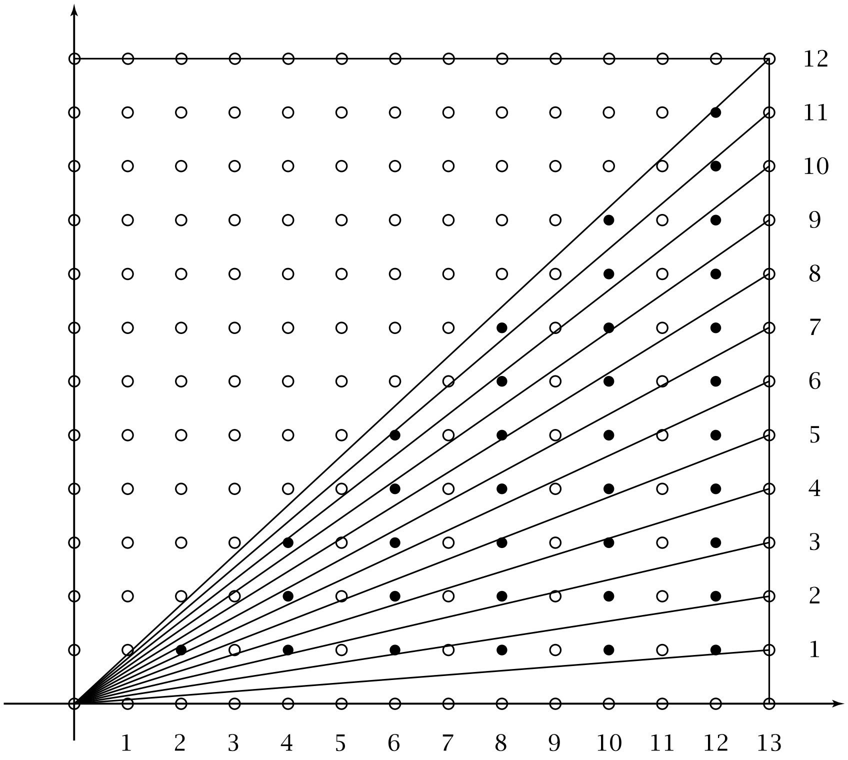
A slightly more complicated example when $p=13$ and a goes from 1 to 12 is shown at the top of the next page.

The way that e varies with a seems somewhat unpredictable. What we will show is that just knowing the parity of e is already enough to determine the value of the Legendre symbol via the formula

$$\left(\frac{a}{p}\right) = (-1)^e$$

To prove this we first derive a formula for e. The segment of the vertical line $x=u$ going from the x-axis up to the diagonal has length ua/p since the slope of the diagonal is a/p. If u is a positive integer the number of lattice points on this line segment is $\lfloor \frac{ua}{p} \rfloor$, the greatest integer $n \le \frac{ua}{p}$. Now if we add up these numbers of lattice points for u running through the set of even numbers $E=\{2,4,\cdots,p-1\}$ we get

$$e = \sum_E \left\lfloor \frac{ua}{p} \right\rfloor$$



a	e	$\left(\frac{a}{13}\right)$
12	36	+1
11	33	–1
10	30	+1
9	26	+1
8	23	–1
7	21	–1
6	15	–1
5	13	–1
4	10	+1
3	6	+1
2	3	–1
1	0	+1

The way to compute $\lfloor\frac{ua}{p}\rfloor$ is to apply the division algorithm for integers, dividing p into ua to obtain $\lfloor\frac{ua}{p}\rfloor$ as the quotient with a remainder that we denote $r(u)$. Thus we have the formula

$$ua = p\Big\lfloor\frac{ua}{p}\Big\rfloor + r(u) \tag{1}$$

This formula implies that the number $\lfloor\frac{ua}{p}\rfloor$ has the same parity as $r(u)$ since u is even and p is odd. This relation between parities implies that the number $(-1)^e$ that we are interested in can also be computed as

$$(-1)^e = (-1)^{\sum_E \lfloor \frac{ua}{p}\rfloor} = (-1)^{\sum_E r(u)} \tag{2}$$

With this last expression in mind we will focus our attention on the remainders $r(u)$.

The number $r(u)$ lies strictly between 0 and p and can be either even or odd, but in both cases we can say that $(-1)^{r(u)}r(u)$ is congruent to an even number in the interval $(0,p)$ since if $r(u)$ is odd, so is $(-1)^{r(u)}r(u)$ and then adding p to this gives an even number between 0 and p. Thus there is always an even number $s(u)$ between 1 and p that is congruent to $(-1)^{r(u)}r(u)$ mod p. Obviously $s(u)$ is unique since no two numbers in the interval $(0,p)$ are congruent mod p.

A key fact about these even numbers $s(u)$ is that they are all distinct as u varies over the set E. For suppose we have $s(u) = s(v)$ for another even number v in E. Thus $r(u) \equiv \pm r(v)$ mod p, which implies $au \equiv \pm av$ mod p in view of the equation (1) above. We can cancel the a from both sides of this congruence to get $u \equiv \pm v$. However we cannot have $u \equiv -v$ because the number between 0 and p that is congruent to $-v$ is $p - v$, so we would have $u = p - v$ which is impossible since u and

v are even while p is odd. Thus we must have $u \equiv +v$, hence $u = v$ since these are numbers strictly between 0 and p. This shows that the numbers $s(u)$ are all distinct.

Now consider the product of all the numbers $(-1)^{r(u)}r(u)$ as u ranges over the set E. Written out, this is

$$\Big[(-1)^{r(2)}r(2)\Big]\Big[(-1)^{r(4)}r(4)\Big]\cdots\Big[(-1)^{r(p-1)}r(p-1)\Big] \qquad (3)$$

By equation (1) we have $r(u) \equiv ua \bmod p$, so this product is congruent mod p to

$$\Big[(-1)^{r(2)}2a\Big]\Big[(-1)^{r(4)}4a\Big]\cdots\Big[(-1)^{r(p-1)}(p-1)a\Big]$$

On the other hand, by the definition of the numbers $s(u)$ the product (3) is congruent mod p to

$$[s(2)][s(4)]\cdots[s(p-1)]$$

There are $\frac{p-1}{2}$ factors here and they are all distinct even numbers in the interval $(0,p)$ as we showed in the previous paragraph, so they are just a rearrangement of the numbers $2,4,\cdots,p-1$. Thus we have the congruence

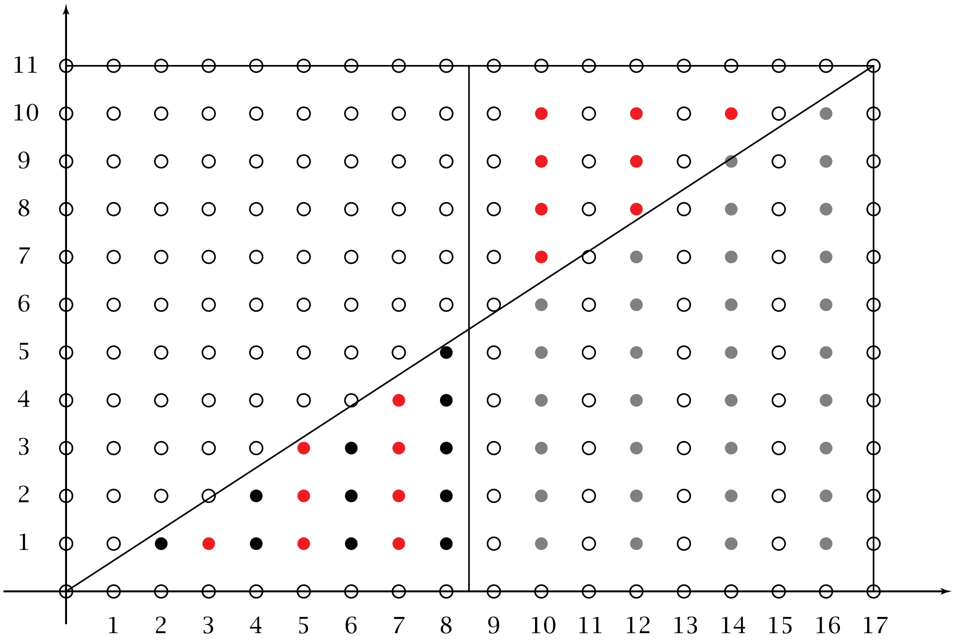
$$\Big[(-1)^{r(2)}2a\Big]\Big[(-1)^{r(4)}4a\Big]\cdots\Big[(-1)^{r(p-1)}(p-1)a\Big] \equiv (2)(4)\cdots(p-1) \mod p$$

We can cancel the factors $2,4,\cdots,p-1$ from both sides of this congruence to obtain

$$(-1)^{\sum_E r(u)}a^{\frac{p-1}{2}} \equiv 1 \mod p$$

Both the factors $(-1)^{\sum_E r(u)}$ and $a^{\frac{p-1}{2}}$ are ± 1 mod p and their product is 1 so they must be equal mod p (using the fact that 1 and -1 are not congruent modulo an odd prime). By Euler's formula we have $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p$, so from the earlier formula (2) we conclude that $\left(\frac{a}{p}\right) = (-1)^e$. This finishes Step 2 in the proof of quadratic reciprocity.

Step 3. Now we specialize the value of a to be an odd prime q distinct from p. As in Step 2 we consider a $p \times q$ rectangle.



We know that $\left(\frac{q}{p}\right) = (-1)^e$ where e is the number of lattice points with even x-coordinate inside the rectangle and below the diagonal. Suppose that we divide the rectangle into two equal halves separated by the vertical line $x = \frac{p}{2}$. This line does not pass through any lattice points since p is odd. This vertical line cuts off two smaller triangles from the two large triangles above and below the diagonal of the rectangle. Call the lower small triangle L and the upper one U, and let l and u denote the number of lattice points with even x-coordinate in L and U respectively. We note that u has the same parity as the number of lattice points with even x-coordinate in the quadrilateral below U in the right half of the rectangle since each column of lattice points in the rectangle has $q-1$ points, an even number. Thus e has the same parity as $l+u$, hence $(-1)^e = (-1)^{l+u}$.

The next thing to notice is that rotating the triangle U by 180 degrees about the center of the rectangle carries it onto the triangle L. This rotation takes the lattice points in U with even x-coordinate onto the lattice points in L with odd x-coordinate. Thus we obtain the formula $\left(\frac{q}{p}\right) = (-1)^t$ where t is the total number of lattice points in the triangle L.

Reversing the roles of p and q, we can also say that $\left(\frac{p}{q}\right) = (-1)^{t'}$ where t' is the number of lattice points in the triangle L' above the diagonal and below the horizontal line $y = \frac{q}{2}$ bisecting the rectangle. Then $t + t'$ is the number of lattice points in the small rectangle formed by L and L' together. This number is just $[\frac{p-1}{2}][\frac{q-1}{2}]$. Thus we have

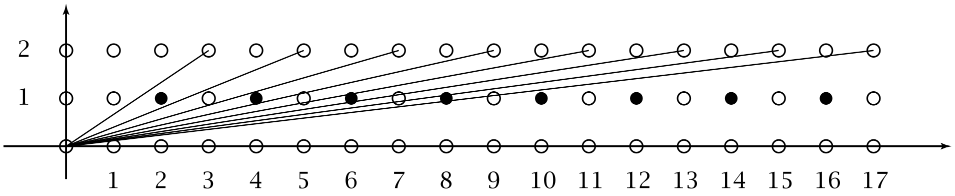
$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^t(-1)^{t'} = (-1)^{t+t'} = (-1)^{[\frac{p-1}{2}][\frac{q-1}{2}]}$$

which finally finishes the proof of quadratic reciprocity.

We can also use the geometric interpretation of $\left(\frac{a}{p}\right)$ to prove the formula for $\left(\frac{2}{p}\right)$ that was stated earlier in this chapter, namely

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & \text{if } p = 8k \pm 1 \\ -1 & \text{if } p = 8k \pm 3 \end{cases}$$

We have shown that $\left(\frac{2}{p}\right) = (-1)^e$ where e is the number of lattice points inside a $p \times 2$ rectangle lying below the diagonal and having even x coordinate, as indicated in the following figure which shows the diagonals for $p = 3, 5, 7, \cdots, 17$:



p	3	5	7	9	11	13	15	17
e	1	1	2	2	3	3	4	4

Another way to describe e is to say that it is equal to the number of even integers in the interval from $p/2$ to p. We do not need to assume that p is prime in order to count these points below the diagonals, just that p is odd. One can see what the pattern is just by looking at the figure: Each time p increases by 2 there is one more even number at the right end of the interval $(p/2, p)$, and there may or may not be one fewer even number at the left end of the interval, depending on whether p is increasing from $4k - 1$ to $4k + 1$ or from $4k + 1$ to $4k + 3$. It follows that the parity of e depends only on the value of p mod 8 as in the table for $p \leq 17$, so e is even for $p \equiv \pm 1$ mod 8 and e is odd for $p \equiv \pm 3$ mod 8.

Exercises

1. For the form $Q(x,y) = x^2 + xy - y^2$ do the following things:

(a) Draw enough of the topograph to show all the values less than 100 that occur in the topograph. This form is hyperbolic and it takes the same negative values as positive values, so you need not draw all the negative values.

(b) Make a list of the primes less than 100 that occur in the topograph, and a list of the primes less than 100 that do not occur.

(c) Characterize the primes in the two lists in part (b) in terms of congruence classes modulo $|\Delta|$ where Δ is the discriminant of Q.

(d) Characterize the nonprime values in the topograph in terms of their factorizations into primes in the lists in part (b).

(e) Summarize the previous parts by giving a simple criterion for which numbers are representable by the form Q, i.e., the numbers n such that $Q(x,y) = n$ has an integer solution (x,y), primitive or not. The criterion should say something like n is representable if and only if $n = m^2 p_1 \cdots p_k$ where each p_i is a prime such that ...

(e) Check that all forms having the same discriminant as Q are equivalent to Q.

2. Do the same things for the form $x^2 + xy + 2y^2$, except that this time you only need to consider values less than 50 instead of 100.

3. For discriminant $\Delta = -24$ do the following:

(a) Verify that the class number is 2 and find two quadratic forms Q_1 and Q_2 of discriminant -24 that are not equivalent.

(b) Draw topographs for Q_1 and Q_2 showing all values less than 100. (You don't have to repeat parts of the topographs that are symmetric.)

(c) Divide the primes less than 100 into three lists: those represented by Q_1, those represented by Q_2, and those represented by neither Q_1 nor Q_2. (No primes are represented by both Q_1 and Q_2.)

(d) Characterize the primes in the three lists in part (c) in terms of congruence classes modulo $|\Delta| = 24$.

(e) Characterize the nonprime values in the topograph of Q_1 in terms of their factorizations into primes in the lists in part (c), and then do the same thing for Q_2. Your answers should be in terms of whether there are an even or an odd number of prime factors from certain of the lists.

(f) Summarize the previous parts by giving a criterion for which numbers are representable by the form Q_1 and which are representable by Q_2.

4. This problem will show how things can be more complicated than in the previous problems.

(a) Show that the number of equivalence classes of forms of discriminant -23 is 2 while the number of proper equivalence classes is 3, and find reduced forms Q_1 and Q_2 of discriminant -23 that are not equivalent.

(b) Draw the topographs of Q_1 and Q_2 up to the value 70. (Again you don't have to repeat symmetric parts.)

(c) Find a number n that occurs in both topographs, and find the x and y values that give $Q_1(x_1, y_1) = n = Q_2(x_2, y_2)$. (This sort of thing never happens in the previous problems.)

(d) Find a prime p_1 in the topograph of Q_1 and a different prime p_2 in the topograph of Q_2 such that p_1 and p_2 are congruent modulo $|\Delta| = 23$. (This sort of thing also never happens in the previous problems.)

5. As a sort of converse to Wilson's theorem, show that if n is not a prime then $(n-1)!$ is not congruent to -1 mod n. More precisely, when $n > 4$ and n is not prime, show that n divides $(n-1)!$, so $(n-1)! \equiv 0$ mod n. What happens when $n = 4$?

6. Determine the values of Δ for which there exists a quadratic form of discriminant Δ that represents 5, and also determine the discriminants Δ for which there does not exist a form representing 5.

7. Verify that the statement of quadratic reciprocity is true for the following pairs of primes (p, q): $(3, 5)$, $(3, 7)$, $(3, 13)$, $(5, 13)$, $(7, 11)$, and $(13, 17)$.

8. (a) There is an example near the end of this chapter that works out which primes are represented by some form of discriminant 13, using quadratic reciprocity for the key step. Do the same thing for discriminant 17.

(b) Show that all forms of discriminant 17 are equivalent to the principal form $x^2 + xy - 4y^2$.

(c) Draw enough of the topograph of $x^2 + xy - 4y^2$ to show all values between -70 and 70, and verify that the primes that occur are precisely the ones predicted by your answer in part (a).

9. Using quadratic reciprocity as in part (a) of the previous problem, figure out which primes are represented by at least one form of discriminant Δ for the following values of Δ: -3, 8, -20, 21.

10. Consider a discriminant $\Delta = q^2$, $q > 0$, corresponding to 0-hyperbolic forms. Using the description of the topographs of such forms obtained in the previous chapter, show:

(a) Every number is represented primitively by at least one form of discriminant Δ, so in particular all primes are represented.

(b) The primes represented by a given form of discriminant Δ are exactly the primes in certain congruence classes mod q (and hence also mod Δ).

(c) For each of the values $q = 1, 2, 7$, and 15 determine the class number for discriminant $\Delta = q^2$ and find which primes are represented by the forms in each equivalence class.

11. Show that the calculation of the Legendre symbol $\left(\frac{-1}{p}\right)$ can also be obtained using the method in the proof of quadratic reciprocity involving counting certain lattice points in a $(p-1) \times p$ rectangle.

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*.

We will also have occasion to consider numbers $x + y\sqrt{D}$ where x and y are allowed to be rational numbers, not just integers. The set of all such numbers is

$$\mathbb{Q}(\sqrt{D}) = \{\, x + y\sqrt{D} \mid x, y \in \mathbb{Q} \,\}$$

Here round parentheses are used instead of square brackets as a way of emphasizing that $\mathbb{Q}(\sqrt{D})$ is a *field* while $\mathbb{Z}[\sqrt{D}]$ is only a *ring*. In other words, in $\mathbb{Q}(\sqrt{D})$ we can perform all four of the basic arithmetic operations of addition, subtraction, multiplication, and division, whereas in $\mathbb{Z}[\sqrt{D}]$ only the first three operations are possible in general. (Multiplicative inverses of nonzero elements of $\mathbb{Q}(\sqrt{D})$ are given by the formula $(x + y\sqrt{D})^{-1} = \frac{x - y\sqrt{D}}{x^2 - Dy^2}$.)

Prime Factorization

The ring $\mathbb{Z}[\sqrt{D}]$ is useful for factoring the form $x^2 - Dy^2$ as $(x+y\sqrt{D})(x-y\sqrt{D})$. For this form the discriminant $\Delta = 4D$ is 0 mod 4, and it would be nice to treat also the discriminants $\Delta = 4d+1 \equiv 1$ mod 4, when the principal form is $x^2 + xy - dy^2$. This can be factored as

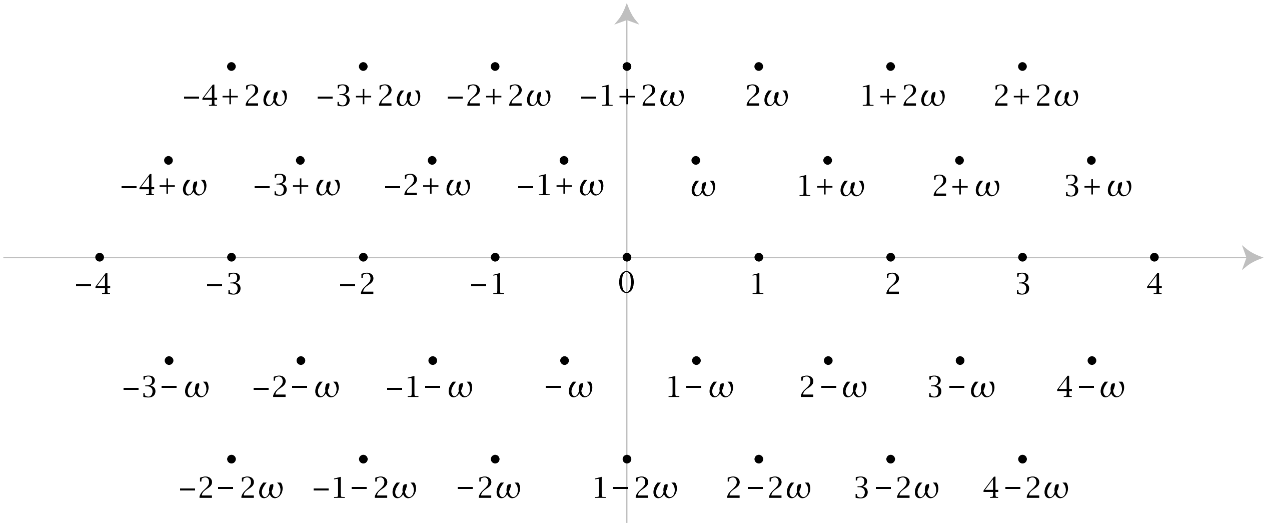
$$x^2 + xy - dy^2 = \Big(x + \frac{1+\sqrt{1+4d}}{2}y\Big)\Big(x + \frac{1-\sqrt{1+4d}}{2}y\Big)$$

To simplify the notation we let $\omega = (1+\sqrt{1+4d})/2$ and $\overline{\omega} = 1 - \sqrt{1+4d})/2$, the conjugate of ω, so the factorization becomes $x^2 + xy - dy^2 = (x+\omega y)(x+\overline{\omega}y)$. The quadratic equation satisfied by ω is $\omega^2 - \omega - d = 0$. Thus $\omega^2 = \omega + d$ and this allows the product of two numbers of the form $m + n\omega$ to be written in the same form. In other words, the set

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

is closed under multiplication and hence is a ring, just like $\mathbb{Z}[\sqrt{D}]$.

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:



The picture for larger negative values of d is similar but stretched in the vertical direction. In these cases the xy-plane is just the plane of complex numbers. When d is positive we can still draw the same figure but this is just a schematic representation of $\mathbb{Z}[\omega]$ since all the numbers in $\mathbb{Z}[\omega]$ are real numbers in this case.

Elements of $\mathbb{Z}[\omega]$ can always be written in the form $m + n\omega = (a + b\sqrt{1+4d})/2$ for suitable integers a and b. Here a and b must have the same parity since this is true for $\omega = (1+\sqrt{1+4d})/2$ and hence for any integer multiple $n\omega$, and then adding an arbitrary integer m to $n\omega$ preserves the equal parity condition since it adds an even integer to a. Conversely, if two integers a and b have the same parity then $(a + b\sqrt{1+4d})/2$ lies in $\mathbb{Z}[\omega]$ since by adding or subtracting a suitable even integer from a we can reduce to the case $a = b$ when one has a multiple of ω. Notice that having both a and b even is equivalent to $(a+b\sqrt{1+4d})/2$ lying in $\mathbb{Z}[\sqrt{1+4d}]$, so $\mathbb{Z}[\sqrt{1+4d}]$ is a subring of $\mathbb{Z}[\omega]$. In the figure above we can see that $\mathbb{Z}[\sqrt{1+4d}]$ consists of the even rows, the numbers $m+n\omega$ with n even.

To have a unified notation for both the cases $\mathbb{Z}[\sqrt{D}]$ and $\mathbb{Z}[\omega]$ let us define R_Δ to be $\mathbb{Z}[\sqrt{D}]$ when the discriminant Δ is $4D$ and $\mathbb{Z}[\omega]$ when Δ is $4d+1$. We will often write elements of R_Δ using lower case Greek letters, for example $\alpha = x + y\sqrt{D}$ or $\alpha = x + y\omega$.

The main theme of this chapter will be how elements of R_Δ factor into 'primes' within R_Δ. For example, 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 $p = (x+y\sqrt{D})(x-y\sqrt{D}) = \alpha\overline{\alpha}$ for $\alpha = x+y\sqrt{D}$. Of course, we should say precisely what we mean by a 'prime' in $\mathbb{Z}[\sqrt{D}]$ or $\mathbb{Z}[\omega]$. 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 R_Δ things can be a little more complicated because of the existence of *units* in R_Δ, the nonzero elements ε in R_Δ whose inverse ε^{-1} also lies in R_Δ. 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 Δ things are somewhat less tidy because there are always infinitely many units in R_Δ. For example, in $\mathbb{Z}[\sqrt{2}]$ 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 R_Δ we can factor any number α in R_Δ as $\alpha = (\alpha\varepsilon)(\varepsilon^{-1})$. If we allowed this as a genuine factorization there would be no primes in R_Δ, so it is best not to consider it as a genuine factorization. This leads us to the following definition: An element α of R_Δ is said to be *prime* in R_Δ if it is neither 0 nor a unit, and if whenever we have a factorization of α as $\alpha = \beta\gamma$ with both β and γ in R_Δ, then it must be the case that either β or γ is a unit in R_Δ. 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 R_Δ 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 R_Δ".

Having defined what we mean by primes in R_Δ it is then natural to ask whether every nonzero element of R_Δ that is not a unit can be factored as a product of primes, and if so, is this factorization in any way unique? As we will see, the existence of prime factorizations is fairly easy to prove, but the uniqueness question is much more difficult and subtle. To clarify what the uniqueness question means, notice first that if we have a unit ε in R_Δ we can always modify a factorization $\alpha = \beta\gamma$ to give another factorization $\alpha = (\varepsilon\beta)(\varepsilon^{-1}\gamma)$. 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 R_Δ being unique, we will always mean unique up to multiplying the factors by units.

A fruitful way to study factorizations in R_Δ is to relate them to factorizations in $\mathbb{Z}$ by means of the function $N : R_\Delta \to \mathbb{Z}$ defined by $N(\alpha) = \alpha\overline{\alpha}$. Thus in the two cases $\mathbb{R}_\Delta = \mathbb{Z}[\sqrt{D}]$ and $\mathbb{R}_\Delta = \mathbb{Z}[\omega]$ we have

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

The number $N(\alpha)$ is called the *norm* of α. Notice that when the discriminant is negative, so α is a complex number which can be written as $a + bi$ for real numbers a and b, the norm of α is just $\alpha\overline{\alpha} = (a + bi)(a - bi) = a^2 + b^2$, the square of the distance from α to the origin in the complex plane. When the discriminant is negative the norm can be negative so it does not have a nice geometric interpretation in terms of distance, but it will be quite useful in spite of this.

The reason the norm is useful for studying factorizations is that it satisfies the following multiplicative property:

Proposition 7.1. *$N(\alpha\beta) = N(\alpha)N(\beta)$ for all α and β in R_Δ.*

Proof: We will deduce multiplicativity of the norm from multiplicativity of the conjugation operation, the fact that $\overline{\alpha\beta} = \overline{\alpha}\,\overline{\beta}$. The argument will apply more generally to all elements of $\mathbb{Q}(\sqrt{D})$ for any integer D that is not a square. To verify that $\overline{\alpha\beta} = \overline{\alpha}\,\overline{\beta}$, write $\alpha = x + y\sqrt{D}$ and $\beta = z + w\sqrt{D}$, so that $\alpha\beta = (xz + ywD) + (xw + yz)\sqrt{D}$. Then

$$\overline{\alpha\beta} = (xz + ywD) - (xw + yz)\sqrt{D} = (x - y\sqrt{D})(z - w\sqrt{D}) = \overline{\alpha}\,\overline{\beta}$$

Now for the norm we have $N(\alpha\beta) = (\alpha\beta)(\overline{\alpha\beta}) = \alpha\beta\overline{\alpha}\,\overline{\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = N(\alpha)N(\beta)$ □

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

Proposition 7.2. *An element $\varepsilon \in R_\Delta$ 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 R_Δ. Then $N(\varepsilon)N(\varepsilon^{-1}) = N(\varepsilon\varepsilon^{-1}) = N(1) = 1$. Since both $N(\varepsilon)$ and $N(\varepsilon^{-1})$ are elements of $\mathbb{Z}$, this forces $N(\varepsilon)$ to be ± 1. For the converse, the inverse of an element ε in R_Δ is $\varepsilon^{-1} = \overline{\varepsilon}/N(\varepsilon)$ since multiplying this by ε gives 1. Hence if $N(\varepsilon) = \pm 1$ we have $\varepsilon^{-1} = \pm\overline{\varepsilon}$ which is an element of R_Δ if ε is, so ε is a unit. □

When Δ is negative there are very few units in R_Δ. In the case of $\mathbb{Z}[\sqrt{D}]$ 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. In the case of $\mathbb{Z}[\omega]$ one can see from the earlier figure of $\mathbb{Z}[\omega]$ when $d = -1$ that there are six lattice points of distance 1 from the origin, giving the six units ± 1, $\pm\omega$, and $\pm(\omega - 1)$. These are the powers ω^n for $n = 0, 1, 2, 3, 4, 5$ since $\omega^2 = \omega - 1$ and $\omega^3 = -1$, hence $\omega^6 = 1$. When $d < -1$ the only units in $\mathbb{Z}[\omega]$ are ± 1 since the lattice is stretched vertically so there are only two lattice points of distance 1 from the origin.

The situation for R_Δ with Δ positive is quite different. For $\mathbb{Z}[\sqrt{D}]$ we are looking for solutions of $x^2 - Dy^2 = \pm 1$ with $D > 0$, while for $\mathbb{Z}[\omega]$ the corresponding equation is $x^2 + xy - dy^2 = \pm 1$ with $d > 0$. We know from our study of topographs of hyperbolic forms that these equations have infinitely many integer solutions since the value 1 occurs along the periodic separator line in the topograph of the principal form when $(x, y) = (1, 0)$, so it appears infinitely often by periodicity. For some values of D or d the number -1 also appears along the separator line, and then it too appears infinitely often. Thus when $\Delta > 0$ the ring R_Δ has infinitely many units $\varepsilon = x + y\sqrt{D}$ or $x + y\omega$, with arbitrarily large values of x and y.

There is a nice interpretation of units in R_Δ as symmetries of the topograph of the principal form of discriminant Δ, as we shall now describe. A unit ε in R_Δ defines a transformation T_ε of R_Δ by the formula $T_\varepsilon(\alpha) = \varepsilon\alpha$. In the case of $\mathbb{Z}[\sqrt{D}]$, if $\varepsilon = p + q\sqrt{D}$ then

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

while for $\mathbb{Z}[\omega]$, if $\varepsilon = p + q\omega$ we have

$$\begin{aligned} T_\varepsilon(x + y\omega) = (p + q\omega)(x + y\omega) &= (px + qy\omega^2) + (qx + py)\omega) \\ &= (px + dqy) + (qx + (p + q)y)\omega \end{aligned}$$

since $\omega^2 = \omega + d$. In both cases we see that T_ε is a linear transformation of x and y, with matrix $\left(\begin{smallmatrix} p & Dq \\ q & p \end{smallmatrix}\right)$ in the first case and $\left(\begin{smallmatrix} p & dq \\ q & p+q \end{smallmatrix}\right)$ in the second case. The determinants in the two cases are $p^2 - Dq^2$ and $p^2 + pq - dq^2$ which equal $N(\varepsilon)$ and hence are ± 1 since ε is a unit. Thus T_ε defines a linear fractional transformation giving a symmetry of the Farey diagram. Since $N(\varepsilon\alpha) = N(\varepsilon)N(\alpha)$ we see that T_ε is an orientation-preserving symmetry of the topograph of the norm form when $N(\varepsilon) = +1$ and an orientation-reversing skew symmetry when $N(\varepsilon) = -1$. The symmetry corresponding to the 'universal' unit $\varepsilon = -1$ is just the identity since $\frac{-x}{-y} = \frac{x}{y}$.

When $\Delta < 0$ the only interesting cases are $\Delta = -3$, when T_ε for $\varepsilon = \omega$ is a 120 degree rotation of the topograph, and $\Delta = -4$ when T_ε for $\varepsilon = i$ rotates the topograph by 180 degrees.

When $\Delta > 0$ there is a *fundamental unit* ε corresponding to the ± 1 in the topograph of the norm form at the vertex p/q with smallest positive values of p and q. When $N(\varepsilon) = +1$ the transformation T_ε is then the translation giving the periodicity along the separating line since it is an orientation-preserving symmetry. In the opposite case $N(\varepsilon) = -1$ the transformation T_ε is an orientation-reversing skew symmetry so it must be a glide reflection along the separator line by half a period.

Proposition 7.3. *If $\Delta > 0$ then the units in R_Δ are the elements $\pm\varepsilon^n$ for $n \in \mathbb{Z}$, where ε is the fundamental unit.*

Proof: The units appear along the separator line at the regions x/y where the norm form takes the value ± 1. From our previous comments, these are the points $T_\varepsilon^n(1/0)$ as n varies over $\mathbb{Z}$. Since T_ε is multiplication by ε, the power T_ε^n is multiplication by ε^n. Thus the values ± 1 occur at the regions labeled x/y for $\varepsilon^n = x + y\sqrt{D}$ or $\varepsilon^n = x + y\omega$. The units are therefore the elements $\pm\varepsilon^n$ where the $\pm$ comes from the fact that the topograph does not distinguish between (x, y) and $(-x, -y)$. □

The conjugation operation in R_Δ sending α to $\overline{\alpha}$ also gives a symmetry of the topograph of the norm form since $N(\alpha) = N(\overline{\alpha})$. Conjugation in $\mathbb{Z}[\sqrt{D}]$ sends $x + y\sqrt{D}$ to $x - y\sqrt{D}$ so in the Farey diagram it is reflection across the edge joining $1/0$ and $0/1$. Conjugation in $\mathbb{Z}\omega$ sends $x + y\omega$ to $x + y\overline{\omega} = (x + y) - \omega$ since $\overline{\omega} = 1 - \omega$, so conjugation fixes the vertex $1/0$ and interchanges $0/1$ and $-1/1$ by reflecting across the line perpendicular to the edge from $0/1$ to $-1/1$.

Proposition 7.4. *All symmetries and skew symmetries of the topograph of the norm form are obtainable as combinations of conjugation and the transformations T_ε associated to units ε in R_Δ.*

Proof: It will suffice to reduce an arbitrary symmetry or skew symmetry T to the identity by composing with conjugation and transformations T_ε. If T is a skew symmetry we must have $\Delta > 0$ with -1 appearing along the separator line as well as $+1$. Composing T with a glide reflection T_ε then converts T into a symmetry, so we may assume T is a symmetry from now on. If T reverses orientation of the Farey diagram we may compose it with conjugation to reduce further to the case that T preserves orientation. When $\Delta < 0$ the only possibility for T is then the identity except when $\Delta = -4$ and $T = T_\varepsilon$ for $\varepsilon = i$, or when $\Delta = -3$ and $T = T_\varepsilon$ for $\varepsilon = \omega$ or ω^2. If

$\Delta > 0$ the only possibility for T is a translation along the separator line, which is T_ε for some unit ε. □

Now we begin to study primes and prime factorizations in R_Δ. First we have a useful fact:

Proposition 7.5. *If the norm $N(\alpha)$ of an element α in R_Δ is prime in $\mathbb{Z}$ then α is prime in R_Δ.*

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 is 5, which is prime in $\mathbb{Z}$.

Proof: Suppose an element α in R_Δ 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.

Now we can prove that prime factorizations always exist:

Proposition 7.6. *Every nonzero element of R_Δ that is not a unit can be factored as a product of primes in R_Δ.*

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 R_Δ, 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 $\mathbb{Z}[i]$. 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 of which are 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 $3 + i = (1 + i)(2 - i)$. This 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

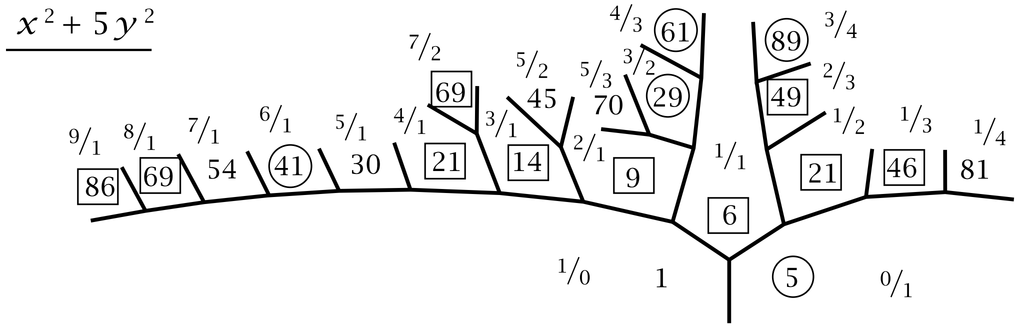
$$244 + 158i = (1 + i)(1 - i)(2 - i)^3(2 + 3i)^2$$

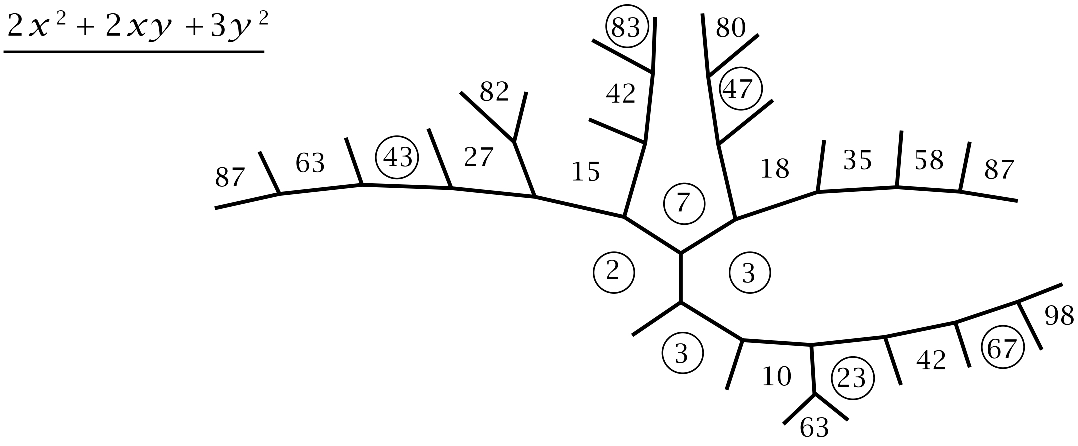
The method in this example for computing prime factorizations in $\mathbb{Z}[i]$ depended on unique factorization. When unique factorization fails, things are more complicated. One of the simplest instances of this is in $\mathbb{Z}[\sqrt{-5}]$ where we have the factorizations

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

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. Using the formula $N(x+y\sqrt{-5}) = x^2+5y^2$ we see that the norms of 2, 3, and $1\pm\sqrt{-5}$ are 4, 9, and 6, so if one of 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 in $\mathbb{Z}$. However, the equations $x^2+5y^2 = 2$ and $x^2+5y^2 = 3$ obviously 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.





The boxed nonprime values in the topograph of $x^2 + 5y^2$ give rise to nonunique prime factorizations like the two factorizations of 6 given above. For example $14 = (2)(7) = (3+\sqrt{-5})(3-\sqrt{-5})$. Some numbers occur in boxes twice, leading to three different prime factorizations. Thus 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 $69 = 3 \cdot 23 = (7+2\sqrt{-5})(7-2\sqrt{-5}) = (8+\sqrt{-5})(8-\sqrt{-5})$.

The question of how a prime p in $\mathbb{Z}$ factors in R_Δ can be rephrased in terms of the norm form $x^2 - Dy^2$ or $x^2 + xy - dy^2$, according to the following result:

Proposition 7.7. *Let p be a prime in $\mathbb{Z}$. Then:*
(a) If either p or $-p$ is represented by the norm form for R_Δ, so $N(\alpha) = \pm p$ for some α in R_Δ, then p factors in R_Δ as $p = \pm\alpha\overline{\alpha}$ and both these factors are prime in R_Δ.
(b) If neither p nor $-p$ is represented by the norm form then p remains prime in R_Δ.

In statement (a) note that when $\Delta < 0$ the norm only takes positive values, so if a positive prime p factors in R_Δ it must factor as $p = \alpha\overline{\alpha}$, never as $-\alpha\overline{\alpha}$. However for $\Delta > 0$ the opposite can be true. For example for $\mathbb{Z}[\sqrt{3}]$ the topograph of $x^2 - 3y^2$ (shown in Chapter 4) contains the value -2 but not 2, so the prime 2 factors as $-(1+\sqrt{3})(1-\sqrt{3})$ in $\mathbb{Z}[\sqrt{3}]$ but not as $\alpha\overline{\alpha}$.

Proof: For part (a), if $p = \pm N(\alpha)$, then p factors in R_Δ as $p = \pm\alpha\overline{\alpha} = \pm N(\alpha)$. 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 R_Δ then it factors in R_Δ 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 $N(\alpha) = N(\beta) = \pm p$. The equation $N(\alpha) = \pm p$ says that the norm form represents $\pm p$. Thus if the norm form represents neither p nor $-p$ then p must be prime in R_Δ. □

Proposition 7.8. *If R_Δ has unique factorization into primes then the only primes in R_Δ are the primes described in (a) or (b) of the preceding proposition (or units times these primes).*

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

We have seen that prime factorizations in R_Δ may not be unique (even up to units) but there is one special situation in which they are:

Proposition 7.9. *The factorization of a prime p in $\mathbb{Z}$ into primes in R_Δ is always unique up to units.*

Proof: If p is prime in R_Δ then uniqueness is automatic. If p is not prime in R_Δ then it has a prime factorization $p = \pm\alpha\overline{\alpha}$ and we want to show that any other prime factorization is the same as this one, up to units. Note that a prime factorization of p in R_Δ cannot have more than two factors since $N(p) = p^2$ is the product of two primes in $\mathbb{Z}$.

Suppose that we have a factorization $p = \beta\gamma$ with β and γ prime in R_Δ. Both β and γ have norm $\pm p$, so in the topograph of the norm form the number p or $-p$ appears in the regions corresponding to β and γ as well as α and $\overline{\alpha}$. By Proposition 6.2 there is a symmetry or skew symmetry of the topograph taking the α region to the β region. By Proposition 7.4 this symmetry or skew symmetry is realizable by a combination of conjugation and multiplication by units, hence β is a unit times α or $\overline{\alpha}$. Interchanging α and $\overline{\alpha}$ if necessary, we may assume that β is a unit times α. The equation $\pm\alpha\overline{\alpha} = \beta\gamma$ then implies that γ is a unit times $\overline{\alpha}$. Thus the two factorizations differ only by units. □

There are two qualitatively different ways in which a prime p can factor as the product of two primes in R_Δ. The distinction is illustrated by the factorizations $2 = (1+i)(1-i)$ and $5 = (2+i)(2-i)$ in $\mathbb{Z}[i]$. The two factors $1+i$ and $1-i$ differ only by multiplication by a unit since $-i(1+i) = 1-i$. However, $2+i$ and $2-i$ do not differ just by a unit since multiplying $2+i$ by the units i, -1, and $-i$ gives $-1+2i$, $-2-i$, and $1-2i$, none of which equals $2-i$. The terminology usually used for this distinction is to say that 2 is *ramified* in $\mathbb{Z}[i]$ while 5 is *not ramified* in $\mathbb{Z}[i]$.

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 of the rings R_Δ as well:

$(\ast)$ *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 factorizations of a number $n > 1$ into positive primes:

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

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. We are assuming all the p_i's and q_i's are positive, so the fact that the prime p_1 divides the prime q_1 implies that p_1 equals q_1. We can then 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 R_Δ we could make essentially the same argument to show that unique factorization holds in R_Δ. 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 R_Δ when R_Δ 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 $\mathbb{Z}[\sqrt{-5}]$.

Our task now is to prove the property $(*)$ without using unique factorization. As we saw in Chapter 2, an equation $ax+by=1$ always has integer solutions (x,y) whenever a and b are coprime integers. This fact can be used to show that property $(*)$ holds in $\mathbb{Z}$. To see how, 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 are coprime. 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.

The fact that equations $ax+by=1$ in $\mathbb{Z}$ are solvable whenever a and b are coprime can be deduced from the Euclidean algorithm, in the following way. What the Euclidean algorithm gives is a method for starting with two positive integers α_0 and α_1 and constructing a sequence of positive integers α_i and β_i satisfying the 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 $\alpha_{n+1}=\alpha_0x+\alpha_1y$ 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 are coprime 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.

Putting all the preceding arguments together, we see that the Euclidean algorithm in $\mathbb{Z}$ implies unique factorization in $\mathbb{Z}$.

A very similar argument works in R_Δ 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 R_Δ. The only difference in the more general case is that α_{n+1} might not be 1, but only a unit in R_Δ. 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 $\alpha_{n+1} = \alpha_0 x + \alpha_1 y$ could be modified by multiplying through by α_{n+1}^{-1} to get an equation $1 = \alpha_0 x + \alpha_1 y$ with a solution x, y in R_Δ. As we have seen, this would imply unique factorization in R_Δ.

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 $\alpha_0 = \beta_1\alpha_1 + \alpha_2$ with α_2 being 'smaller' than α_1. We measure 'smallness' of complex numbers by computing their distance to the origin in the complex plane. For a complex number $\alpha = x + yi$ this distance is $\sqrt{x^2 + y^2}$. Here x^2+y^2 is just the norm $N(\alpha)$ when x and y are integers, so we could measure the size of a Gaussian integer α by $\sqrt{N(\alpha)}$. However it is simpler just to use $N(\alpha)$ without the square root, so this is what we will do.

Thus our goal is to find an equation $\alpha_0 = \beta_1\alpha_1 + \alpha_2$ with $N(\alpha_2) < N(\alpha_1)$, starting from two given nonzero Gaussian integers α_0 and α_1. If we can always do this, then by repeating the process we can 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, hence this α_i will 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 α_2 to have a smaller norm than α_1. To get an idea how we can do this let us look instead 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

$$12 + 15i = (3+2i)(5+2i) + \alpha_2 = (11+16i) + \alpha_2$$

hence $\alpha_2 = 1-i$. 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 (so 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 $|x| \leq \frac{1}{2}$ and $|y| \leq \frac{1}{2}$, so

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

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.

Just as an exercise 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 $2 + 4i$. Let us stick with the choice $1 + 3i$ and use this to calculate the next α_i:

$$5 + 2i = (1 + 3i)(1 - i) + \alpha_3 = (4 + 2i) + \alpha_3$$

hence $\alpha_3 = 1$. The final step would be simply to write $1 - i = (1 - i)1 + 0$. Thus the full Euclidean algorithm gives the following equations:

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

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.

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.

Having shown that prime factorizations in $\mathbb{Z}[i]$ are unique, let us see what this implies about the representation problem for the form $x^2 + y^2$. Since $x^2 + y^2$ is the norm $N(x + yi)$, determining whether $x^2 + y^2 = n$ has an integer solution for a given n is equivalent to determining which integers n are norms of elements of $\mathbb{Z}[i]$. Since the norm is multiplicative and all elements of $\mathbb{Z}[i]$ factor into primes, we obtain all norms by taking all products of norms of primes in $\mathbb{Z}[i]$. Using the unique factorization property, we know that primes in $\mathbb{Z}[i]$ have norms that are either the ordinary primes 2 and $p = 4k+1$ or the squares p^2 of primes $p = 4k+3$. From this it follows that the numbers $n > 1$ represented by $x^2 + y^2$ are exactly the numbers whose prime factorization contains primes $p = 4k + 3$ only to even powers. This agrees with the answer we got in Chapter 6, but the only nontrivial result from that chapter we have used here is the fact that all primes $p = 4k + 1$ are represented by $x^2 + y^2$.

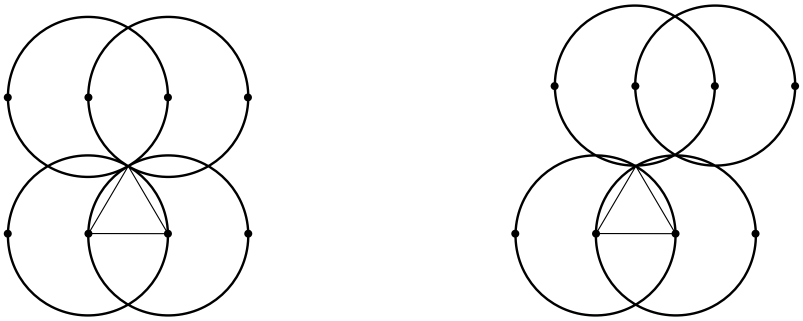
Going further, we can also answer the more subtle question of which numbers have primitive representations by $x^2 + y^2$. Thus we must weed out the nonprimitive representations $n = x^2 + y^2 = N(x + yi)$. These are the ones for which both x and y are divisible by some prime p in $\mathbb{Z}$, which is the same as saying that $x + yi$ is divisible by p in $\mathbb{Z}[i]$. In the prime factorization of $x + yi$ in $\mathbb{Z}[i]$ this is saying that we have either a prime factor $p = 4k + 3$ or we have both factors α and $\overline{\alpha}$ of a factorization of a prime $p = 2$ or $p = 4k + 1$.

To see what remains after these nonprimitive representations are excluded, consider the prime factorization $n = 2^a p_1^{k_1} \cdots p_m^{k_m}$ in $\mathbb{Z}$, where the p_i's are distinct odd primes. For a primitive representation $n = x^2 + y^2 = (x + yi)(x - yi)$ we cannot have any p_i be a prime $p = 4k+3$ since this would give p as a factor of $x+yi$ in the prime factorization of $(x + yi)(x - yi)$ in $\mathbb{Z}[i]$. Furthermore, we cannot have $a \ge 2$ since in $\mathbb{Z}[i]$ we have the prime factorization $2 = (1 + i)(1 - i)$ with $1 - i = i(1 + i)$ so the two prime factors of 2 in $\mathbb{Z}[i]$ are the same up to units, hence if 2^2 was a factor of $(x + yi)(x - yi)$ in $\mathbb{Z}[i]$ we would have $2 = \alpha\overline{\alpha}$ as a factor of $x + yi$, forcing the representation to be nonprimitive. Thus we have shown that for primitive representations we must have $a \le 1$ and $p_i \equiv 1 \bmod 4$ for each p_i.

Conversely, suppose each p_i has the form $4k + 1$ and hence factors as $\alpha_i\overline{\alpha}_i$ in $\mathbb{Z}[i]$. Then if we let $x+yi = (1+i)^a \alpha_1^{k_1} \cdots \alpha_m^{k_m}$ with $a \le 1$, we have a representation $x^2 + y^2 = N(x + yi) = 2^a p_1^{k_1} \cdots p_m^{k_m} = n$ and this is primitive since no $\overline{\alpha}_i$ is a unit times α_i, as one can see by writing α_i as $a + bi$ since we cannot have $a = \pm b$, else α_i would not be prime.

For negative discriminants it is not difficult to figure out exactly which of the rings R_Δ have a Euclidean algorithm. Recall that this means that for each pair of nonzero elements α_0 and α_1 in R_Δ there should exist elements β and α_2 such that $\alpha_0 = \beta\alpha_1 + \alpha_2$ and $N(\alpha_2) < N(\alpha_1)$. Since α_2 is determined by α_0, α_1, and β, this is equivalent to saying that there should exist an element β in R_Δ such that $N(\alpha_0 - \beta\alpha_1) < N(\alpha_1)$. The last inequality can be rewritten as $N(\frac{\alpha_0}{\alpha_1} - \beta) < 1$. Geometrically this is saying that every point $\frac{\alpha_0}{\alpha_1}$ in the plane should be within a distance less than 1 of a point in the lattice R_Δ. We can check this by seeing whether the interiors of all circles of radius 1 centered at points of R_Δ completely cover the plane.

For $\mathbb{Z}[\sqrt{D}]$ with $D < 0$ the critical case $D = -3$ is shown in the first figure below, where the triangle is an equilateral triangle of side length 1.



Here the four circles of radius 1 centered at 0, 1, $\sqrt{-3}$, and $1 + \sqrt{-3}$ intersect at the point $(1 + \sqrt{-3})/2$ so this point $\frac{\alpha_0}{\alpha_1}$ is not within a distance less than 1 of an element of $\mathbb{Z}[\sqrt{-3}]$ and therefore the Euclidean algorithm fails in $\mathbb{Z}[\sqrt{-3}]$. For $D < -3$ the lattice $\mathbb{Z}[\sqrt{D}]$ is stretched vertically so the Euclidean algorithm fails in these cases too. For $D = -2$ the lattice is compressed vertically so $\mathbb{Z}[\sqrt{-2}]$ does have a Euclidean algorithm.

The case of $\mathbb{Z}[\omega]$ for $\omega = (1 + \sqrt{1 + 4d})/2$ with $d < 0$ is illustrated in the right half of the figure above. Here the second row of disks are at height $\sqrt{|1 + 4d|}/2$ above the first row, so from the figure we see that the condition we need is that this height should be less than $1 + \frac{\sqrt{3}}{2}$. Thus we need $\sqrt{|1 + 4d|} < 2 + \sqrt{3}$. Squaring both sides gives $|1 + 4d| < 7 + 4\sqrt{3}$ which is satisfied only in the cases $d = -1, -2, -3$.

In summary, we have shown the following result:

Proposition 7.10. *The only negative discriminants* Δ *for which* R_Δ *has a Euclidean algorithm are* $\Delta = -3, -4, -7, -8, -11$.

Notice that these are the first five negative discriminants.

For even negative discriminants it is easy to prove that unique factorization fails in all cases when there is no Euclidean algorithm:

Proposition 7.11. *Unique factorization fails in* $\mathbb{Z}[\sqrt{D}]$ *whenever* $D < -2$*, and it also fails when* $D > 0$ *and* $D \equiv 1$ *modulo* 4.

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 $D-1$ in $\mathbb{Z}[\sqrt{D}]$ 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. □

This proposition says in particular that unique factorization fails in $\mathbb{Z}[\sqrt{-3}]$, $\mathbb{Z}[\sqrt{-7}]$, and $\mathbb{Z}[\sqrt{-11}]$, but when we enlarge these three rings to $\mathbb{Z}[\omega]$ for ω equal to $\frac{1+\sqrt{-3}}{2}$, $\frac{1+\sqrt{-7}}{2}$, and $\frac{1+\sqrt{-11}}{2}$ we do have unique factorization. A similar thing happens when we enlarge $\mathbb{Z}[\sqrt{-8}]$ to $\mathbb{Z}[\sqrt{-2}]$. In all these cases the enlargement replaces a nonfundamental discriminant by one which is fundamental.

One might wonder whether there are other ways to enlarge $\mathbb{Z}[\sqrt{D}]$ to make prime factorization unique when it is not unique in $\mathbb{Z}[\sqrt{D}]$ itself. Without changing things too drastically, suppose we just tried a different choice of ω besides $(1+\sqrt{1+4d})/2$. In order to do multiplication within the set $\mathbb{Z}[\omega]$ of numbers $x+y\omega$ with x and y integers one must be able to express ω^2 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 in the definition of ω will not work. If m is even, say $m=2k$, then ω becomes $k\pm\sqrt{k^2+n}$, with no denominators at all and we are back in the situation of $\mathbb{Z}[\sqrt{D}]$. If m is odd, say $m=2k+1$, then ω is $(2k+1\pm\sqrt{4k^2+4k+1+4n})/2$, which can be written as $k+(1\pm\sqrt{1+4d})/2$ so the ring $\mathbb{Z}[\omega]$ in this case would be the same as when we chose $\omega=(1+\sqrt{1+4d})/2$.

It is known that there are only nine negative discriminants for which R_Δ has unique factorization, 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 since the usual way one determines whether unique factorization holds is by proving that unique factorization holds precisely when all forms of the given discriminant are equivalent.

For positive discriminants the norm form is hyperbolic so it takes on both positive and negative values. The Euclidean algorithm is then 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 discriminants for which there is a Euclidean algorithm in R_Δ:

$$\Delta = 5, 8, 12, 13, 17, 21, 24, 28, 29, 33, 37, 41, 44, 57, 73, 76$$

The determination of this list is much more difficult than for negative discriminants since the norm no longer has the nice geometric meaning of the square of the distance to the origin in the plane.

There are many positive discriminants, probably infinitely many in fact, for which R_Δ has unique factorization even though there is no Euclidean algorithm. The discriminants less than 100 with this property are $53, 56, 61, 69, 77, 88, 89, 92, 93, 97$.

To conclude this section we will illustrate further the usefulness of unique prime factorization in R_Δ by an extended example in which we finish the determination of which numbers are represented primitively by the form $x^2 + 7y^2$. We studied this problem in an example in Chapter 6 and found that a necessary condition for a number n to be primitively represented by $x^2 + 7y^2$ was that n factors into primes as $n = 2^a 7^b p_1^{k_1} \cdots p_m^{k_m}$ where $a = 0$ or $a \geq 3$, $b \leq 1$, and the p_i's are distinct odd primes congruent to 1, 2, or 4 mod 7. Now we will show the converse, that each n having such a factorization is primitively represented by $x^2 + 7y^2$. This includes the curious fact that all powers of 2 starting with 8 have such a representation. For example $8 = 1^2 + 7\cdot 1^2$, $16 = 3^2 + 7\cdot 1^2$, $32 = 5^2 + 7\cdot 1^2$, $64 = 1^2 + 7\cdot 3^2$, $128 = 11^2 + 7\cdot 1^2$, $256 = 9^2 + 7\cdot 5^2$, $512 = 13^2 + 7\cdot 7^2$, $1024 = 31^2 + 7\cdot 3^2$, $2048 = 5^2 + 7\cdot 17^2$, $4096 = 57^2 + 7\cdot 11^2$, $8192 = 67^2 + 7\cdot 23^2$, $16384 = 47^2 + 7\cdot 45^2$, and $32768 = 181^2 + 7\cdot 1^2$. As we will see, these are the unique primitive solutions with positive x and y in each case. Without the primitivity requirement solutions are much easier to construct just by repeated doubling of the solutions for $n = 8$ and $n = 16$, so for example $32 = 2^2 + 7\cdot 2^2$, $64 = 6^2 + 7\cdot 2^2$, $128 = 4^2 + 7\cdot 4^2$, and so on.

The form $x^2 + 7y^2$ is the norm form in $\mathbb{Z}[\sqrt{-7}]$, but rather than using $\mathbb{Z}[\sqrt{-7}]$ which does not have the unique factorization property we will use the larger ring $\mathbb{Z}[\omega]$ for $\omega = (1+\sqrt{-7})/2$ which does have unique factorization. This implies in particular that all primes in $\mathbb{Z}[\omega]$ are obtained by factoring primes in $\mathbb{Z}$. Primes in $\mathbb{Z}$ that do not appear in the topograph of the norm form $x^2 + xy + 2y^2$ remain prime in $\mathbb{Z}[\omega]$ while primes that do appear factor as $p = \alpha\overline{\alpha}$. The methods of Chapter 6 show that the primes p that factor as $\alpha\overline{\alpha}$ are 7 (the only prime dividing the discriminant) which factors as $(\sqrt{-7})(-\sqrt{-7})$ and primes $p \equiv 1, 2, 4$ mod 7. This includes $p = 2$ which has the factorization $2 = \omega\overline{\omega}$. For odd primes the factorization actually takes place in $\mathbb{Z}[\sqrt{-7}]$ since otherwise we would have $p = \frac{a+b\sqrt{-7}}{2}\cdot\frac{a-b\sqrt{-7}}{2} = \frac{a^2+7b^2}{4}$ with a and b both odd, so a^2 and b^2 would be 1 mod 8 making $a^2 + 7b^2$ zero mod 8 which would mean p was even.

For factorizations $p = \alpha\overline{\alpha}$ we will need to know whether α and $\overline{\alpha}$ differ only by a unit. Since the only units in $\mathbb{Z}[\omega]$ are ± 1 this is easy to figure out. In the factorization of 7 as $(\sqrt{-7})(-\sqrt{-7})$ the two factors differ by a unit. In all other cases the two factors $\frac{a+b\sqrt{-7}}{2}$ and $\frac{a-b\sqrt{-7}}{2}$ do not differ just by a unit (that is, just by a sign) since both a and b must be nonzero.

With $n = 2^a 7^b p_1^{k_1} \cdots p_m^{k_m}$ as before, let p_i factor as $p_i = \alpha_i\overline{\alpha}_i$. In the cases $a \geq 3$ let x and y be defined by the equation

$$x + y\sqrt{-7} = 2\omega^{a-2}(\sqrt{-7})^b \alpha_1^{k_1} \cdots \alpha_m^{k_m}$$

The reason for including the factor 2 on the right side of the equation is to guarantee that x and y are integers since ω^{a-2}, as an element of $\mathbb{Z}[\omega]$, might have a denominator of 2. (We already noted that each α_i lies in $\mathbb{Z}[\sqrt{-7}]$.) When we take the norm of $x + y\sqrt{-7}$ we get

$$x^2 + 7y^2 = 4 \cdot 2^{a-2} 7^b p_1^{k_1} \cdots p_m^{k_m}$$

so we have a solution of $x^2 + 7y^2 = n$. All that remains to check is that this is a primitive solution when $a \geq 3$ and $b \leq 1$. This is where the unique factorization property in $\mathbb{Z}[\omega]$ will be used strongly.

Suppose that some prime p divides both x and y, hence p divides $x + y\sqrt{-7}$ in $\mathbb{Z}[\omega]$. There are several cases to consider:

- If p remains prime in $\mathbb{Z}[\omega]$ then it cannot divide $x + y\sqrt{-7}$ since it does not divide any of the prime factors of $x + y\sqrt{-7}$.
- If $p = p_i$ for some i then since $p = \alpha_i\overline{\alpha}_i$, for p to divide $x + y\sqrt{-7}$ implies that $\overline{\alpha}_i$ divides $x + y\sqrt{-7}$, which it doesn't since $\overline{\alpha}_i$ is not a unit times α_i.
- If $p = 7$ then it does not divide $x + y\sqrt{-7}$ since we assume $b \leq 1$.
- If $p = 2$ we can divide the formula for $x + y\sqrt{-7}$ by 2 to obtain a formula $w + z\sqrt{-7} = \omega^{a-2}(\sqrt{-7})^b \alpha_1^{k_1} \cdots \alpha_m^{k_m}$ with both w and z integers. Since we assume $a \geq 3$ this means $N(x + y\sqrt{-7})$ is divisible by 8 so $N(w + z\sqrt{-7}) = w^2 + 7z^2$ is divisible by 2. This implies that w and z have the same parity. If they are both even then $2 = \omega\overline{\omega}$ would divide the right side of the formula for $w + z\sqrt{-7}$, hence $\overline{\omega}$ would divide it, a contradiction. If w and z are both odd then $\frac{w+z\sqrt{-7}}{2}$ would be an element of $\mathbb{Z}[\omega]$ so 2 would again divide $w+z\sqrt{-7}$ leading to the same contradiction.

Thus we have found a primitive solution of $x^2 + 7y^2 = n$ in the cases $a \geq 3$. When $a = 0$ we can omit the term $2\omega^{a-2}$ from the formula for $x + y\sqrt{-7}$ and follow the same line of reasoning, with a few resulting simplifications in the argument. The only difference occurs at the very last step, where we check that 2 does not divide $x + y\sqrt{-7}$ by noting that neither ω nor $\overline{\omega}$ divides $(\sqrt{-7})^b \alpha_1^{k_1} \cdots \alpha_m^{k_m}$.

We stated earlier that the equation $x^2 + 7y^2 = 2^k$ has only one primitive solution with x and y positive. To see this, factor this equation as $(x + y\sqrt{-7})(x - y\sqrt{-7}) = \omega^k\overline{\omega}^k$. By unique factorization, $x + y\sqrt{-7}$ must equal $\pm\omega^l\overline{\omega}^m$ for some l and m

with $l+m=k$. Choosing $m=1$ gives the primitive solution $\pm 2\omega^{k-2}$ that we found above, and the conjugate of this solution with $l=1$ is another primitive solution. Choosing $l=0$ or $m=0$ gives a solution in $\mathbb{Z}[\omega]$ but not in $\mathbb{Z}[\sqrt{-7}]$, otherwise multiplying this solution by $2=\omega\overline{\omega}$ would give the nonprimitive solution $\pm 2\omega^k$ or $\pm 2\overline{\omega}^k$ of $x^2+7y^2=2^{k+2}$, contradicting our earlier proof that this solution is primitive. When $l>1$ and $m>1$ with $l\neq m$ we get nonprimitive solutions obtained from the known primitive solutions for a smaller value of k by multiplying by a power of 2. When $l=m$ we get the nonprimitive solution $x=2^l$, $y=0$. Thus we have shown that there are at most four primitive solutions. The signs of x and y can be changed arbitrarily, so if we take x and y to be positive the number of primitive solutions reduces to one.

A historical footnote: In the early 1900s the number theorist Ramanujan observed that the Diophantine equation $x^2+7=2^k$ has solutions for $k=3,4,5,7,15$ and he conjectured that there were no solutions for larger k. In terms of the preceding example this is saying that the only solutions of $x^2+7y^2=2^k$ with $y=1$ occur in these five cases. Ramanujan's conjecture was later proved in a paper by Skolem, Chowla, and Lewis published in 1959.

The Correspondence Between Forms and Ideals

So far in this chapter we have focused on principal forms, and now we begin to extend what we have done to arbitrary forms. For principal forms we began by factoring them as a product of two linear factors whose coefficients involved square roots, for example the factorization $x^2-Dy^2=(x+\sqrt{D}y)(x-\sqrt{D}y)$ in the case of discriminant $\Delta=4D$. For a general form $Q(x,y)=ax^2+bxy+cy^2$ of discriminant Δ the corresponding factorization is $a(x-\alpha y)(x-\overline{\alpha}y)$ where α is a root of the quadratic equation $ax^2+bx+c=0$. Thus we have

$$ax^2+bxy+cy^2=a\Big(x-\frac{-b+\sqrt{\Delta}}{2a}y\Big)\Big(x-\frac{-b-\sqrt{\Delta}}{2a}y\Big)$$

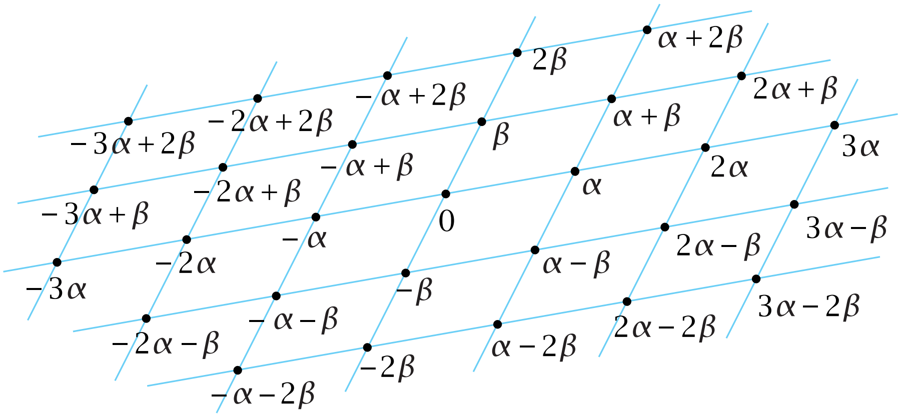
An equivalent equation that will be more convenient for our purposes is obtained by multiplying both sides by the coefficient a to obtain

$$a(ax^2+bxy+cy^2)=\Big(ax+\frac{b+\sqrt{\Delta}}{2}y\Big)\Big(ax+\frac{b-\sqrt{\Delta}}{2}y\Big)$$

Notice that now in each of the two linear factors on the right the coefficients of x and y lie in the ring R_Δ since b must have the same parity as Δ, so if $\Delta=4D$ we can eliminate the denominator 2 in the coefficient of y to obtain an element of $\mathbb{Z}[\sqrt{D}]$ while if $\Delta=4d+1$ the fraction lies in $\mathbb{Z}[\omega]$ since b is odd. Another thing to observe is that the right side of the equation is just the norm $N\big(ax+\frac{b+\sqrt{\Delta}}{2}y\big)$.

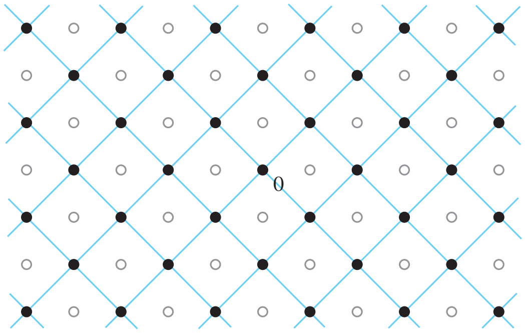
For a form $Q(x,y)=ax^2+bxy+cy^2$ the set of numbers $ax+\frac{b+\sqrt{\Delta}}{2}y$ as x and y range over all integers forms a lattice contained in the larger lattice R_Δ in the plane. Here we use the term *lattice* to refer to a set of numbers of the form $\alpha x+\beta y$

for fixed nonzero elements α and β of R_Δ, with x and y varying over $\mathbb{Z}$, and we assume that α and β do not lie on the same line through the origin. We denote this lattice by $L(\alpha, \beta)$ and call α and β a *basis* for this lattice.

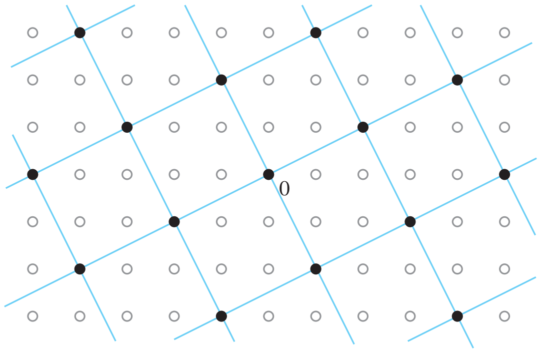


In particular we have the lattice $L_Q = L(a, (b+\sqrt{\Delta})/2)$ associated to the form Q. Let us look at some examples to see what L_Q can look like in the case $\Delta = -4$ so $R_\Delta = \mathbb{Z}[i]$, the Gaussian integers. In this case we have $ax + \frac{b+\sqrt{\Delta}}{2}y = ax + (b' + i)y$ where $b' = b/2$, an integer since b always has the same parity as Δ. For the principal form $x^2 + y^2$ we have $a = 1$ and $b' = 0$ so $L_Q = L(1, i) = \mathbb{Z}[i]$. Four more cases are shown in the figures below.

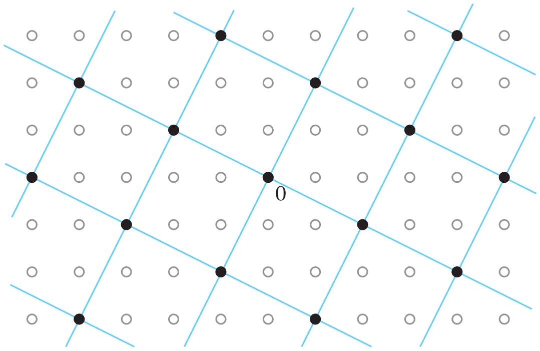
$2x^2 + 2xy + y^2 \longrightarrow L(2, 1+i)$



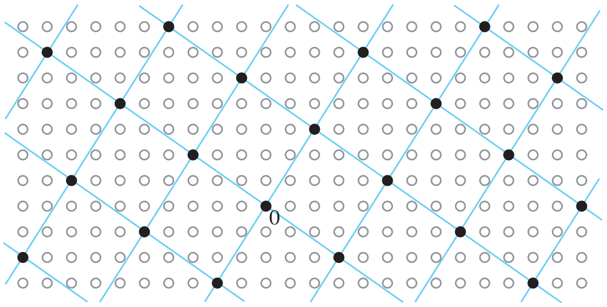
$5x^2 + 4xy + y^2 \longrightarrow L(5, 2+i)$



$5x^2 + 6xy + 2y^2 \longrightarrow L(5, 3+i)$



$13x^2 + 10xy + 2y^2 \longrightarrow L(13, 5+i)$



In each case the lattice forms a grid of squares, rotated and expanded from the square grid formed by $\mathbb{Z}[i]$ itself. Not all lattices in $\mathbb{Z}[i]$ form square grids since for example one could have a lattice of long thin rectangles such as $L(10, i)$.

A 90 degree rotation of the plane about the origin takes a square lattice to itself.

Conversely, a lattice that is taken to itself by a 90 degree rotation about the origin must be a square lattice. To see this, observe first that the 90 degree rotation takes the closest lattice point to the origin to another closest lattice point, with the sum of these two lattice points giving another lattice point that is the fourth vertex of a square of lattice points. There can be no lattice points in the interior of this square since such a point would be closer to a corner of the square than the length of the side of the square, which is impossible since the minimum distance between any two points in a lattice equals the minimum distance from the origin to a lattice point.

Since 90 degree rotation is the same as multiplication of complex numbers by i, we could also say that square lattices are those that are taken to themselves by multiplication by i. Once a lattice has this property it follows that multiplication by an arbitrary element of $\mathbb{Z}[i]$ takes the lattice into itself. Namely, if we know that $i\alpha$ is in a lattice L whenever α is in L, then for arbitrary integers m and n it follows that $m\alpha$ and $ni\alpha$ are in L and hence also $(m+ni)\alpha$ is in L.

There is a standard term for this concept. A lattice L in R_Δ is called an *ideal* if for each element α in L and each β in R_Δ the product $\beta\alpha$ is in L. In other words, L is taken to itself by multiplication by every element of R_Δ. The term 'ideal' may seem like an odd name, but it originally arose in a slightly different context where it seems more natural, as we will see later in the chapter. For now we can just imagine that ideals are the best kind of lattices, 'ideal lattices'.

The fact that all lattices L_Q in $\mathbb{Z}[i]$ are square lattices is a special case of the following general fact:

Proposition 7.12. *Every lattice L_Q associated to a quadratic form Q of discriminant Δ is an ideal in R_Δ.*

Proof: To cover all discriminants at once we can write R_Δ as $\mathbb{Z}[\tau]$ for $\tau = (e+\sqrt{\Delta})/2$ where e is 0 if $\Delta = 4D$ and 1 if $\Delta = 4d+1$. What we need to check in order to verify that the lattice $L_Q = L(a, (b+\sqrt{\Delta})/2)$ is an ideal is that both of the products $\tau \cdot a$ and $\tau \cdot (b+\sqrt{\Delta})/2$ are elements of L_Q. For the product $\tau \cdot a$ this means we want to solve the equation

$$\frac{e+\sqrt{\Delta}}{2}\cdot a = ax + \frac{b+\sqrt{\Delta}}{2}y$$

for integers x and y. Comparing the coefficients of $\sqrt{\Delta}$ on both sides of the equation, we get $y = a$, an integer. Substituting $y = a$ into the equation then gives $\frac{ea}{2} = ax + \frac{ba}{2}$ so $x = \frac{e-b}{2}$. This is an integer since both e and b have the same parity as Δ.

For the other product $\tau \cdot (b+\sqrt{\Delta})/2$ we have a similar equation

$$\frac{e+\sqrt{\Delta}}{2}\cdot\frac{b+\sqrt{\Delta}}{2} = ax + \frac{b+\sqrt{\Delta}}{2}y$$

which we can rewrite as

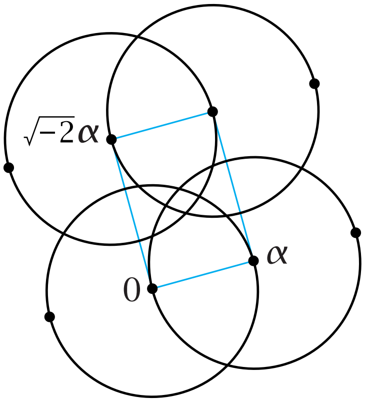
$$\frac{eb+\Delta+(e+b)\sqrt{\Delta}}{4} = ax + \frac{b+\sqrt{\Delta}}{2}y$$

From the coefficients of $\sqrt{\Delta}$ we get $y = (e+b)/2$ which is an integer since e and b have the same parity. Then the equation becomes

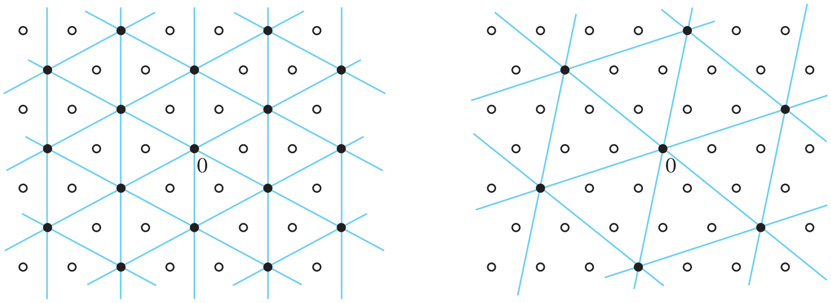
$$\frac{eb+\Delta}{4} = ax + \frac{eb+b^2}{4}$$

which simplifies to $ax = (\Delta - b^2)/4$. Since $\Delta = b^2 - 4ac$ we have the integer solution $x = c$. □

We saw in the case of $\mathbb{Z}[i]$ that all ideals are square lattices, so they are obtained from $\mathbb{Z}[i]$ by rotation about the origin and expansion. There are a few other negative discriminants where the same thing happens and all ideals differ only by rotation and rescaling, either expansion or contraction. One example is when $\Delta = -8$ so we have $R_\Delta = \mathbb{Z}[\sqrt{-2}]$ which forms a rectangular lattice with rectangles of side lengths 1 and $\sqrt{2}$. For an arbitrary ideal L in $\mathbb{Z}[\sqrt{-2}]$ let α be a nonzero point in L closest to the origin. Since L is an ideal, the product $\sqrt{-2}\,\alpha$ must also be in L. Since multiplication by $\sqrt{-2}$ rotates the plane by 90 degrees and expands it by a factor of $\sqrt{2}$, the set of all linear combinations $\alpha x + \sqrt{-2}\,\alpha y$ for integers x and y forms a rectangular sublattice L' of L obtained from $\mathbb{Z}[\sqrt{-2}]$ by rotation and expansion. Since we chose α as the closest point of L to the origin, say of distance A to the origin, there can be no points of L within a distance less than A of any point of L'. In other words, if one takes the union of the interiors of all disks of radius A centered at points of L', this union intersects L just in L'. However, this union is the whole plane since the ratio of the side lengths of the rectangles of L' is $\sqrt{2}$. Thus L equals the rectangular lattice L'.



This is essentially the same geometric argument we used to show that $\mathbb{Z}[\sqrt{-2}]$ has a Euclidean algorithm. There were five negative discriminants Δ for which R_Δ has a Euclidean algorithm, $\Delta = -3, -4, -7, -8, -11$. The argument in the preceding paragraph shows that in each of these cases all ideals in R_Δ are equivalent under rotation and rescaling. In the case $\Delta = -3$ the Eisenstein integers $\mathbb{Z}[\omega]$ form a grid of equilateral triangles so all ideals are also grids of equilateral triangles that are taken to themselves by multiplication by ω, rotating the plane by 60 degrees.

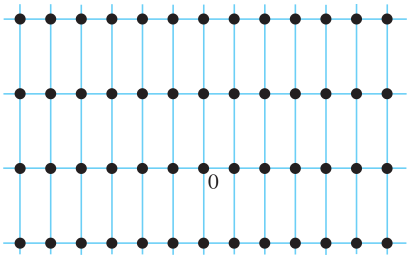


For $\Delta = -7$ and -11 the lattice $R_\Delta = \mathbb{Z}[\omega]$ for $\Delta = -3$ is stretched vertically to form a grid of isosceles triangles and all ideals are also grids of isosceles triangles, rotated and rescaled from the triangles in R_Δ.

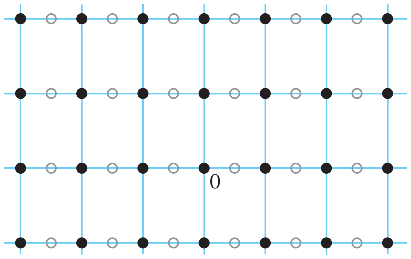
We have been using the fact that multiplication by a fixed nonzero complex number α always has the effect of rotating and rescaling the plane, keeping the origin fixed. Since multiplication by α sends 1 to α, the rescaling factor is the distance from α to the origin and the angle of rotation is the angle between the positive x axis and the ray from the origin to α. Since α can be any nonzero complex number, every rotation and rescaling is realizable as multiplication by a suitably chosen α.

Let us look at some examples of discriminants where not all forms are equivalent to see whether there is more variety in the shapes of the lattices L_Q, so they are not all obtained from R_Δ by rotation and rescaling. First consider the lattices L_Q in $\mathbb{Z}[\sqrt{-6}]$ for the two non-equivalent forms x^2+6y^2 and $2x^2+3y^2$ of discriminant -24. These are the lattices $L(1,\sqrt{-6}) = \mathbb{Z}[\sqrt{-6}]$ and $L(2,\sqrt{-6})$ shown below.

$x^2 + 6y^2 \longrightarrow L(1,\sqrt{-6})$



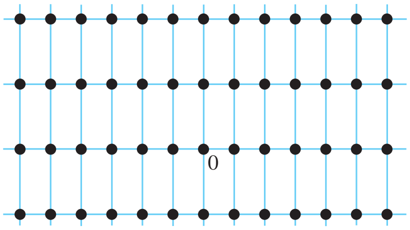
$2x^2 + 3y^2 \longrightarrow L(2,\sqrt{-6})$



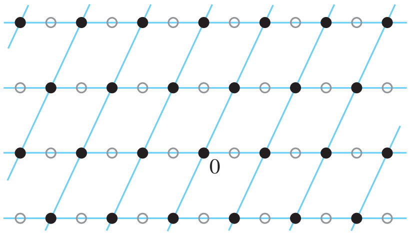
The two lattices do not appear to differ just by rotation and rescaling, and we can verify this by computing the ratio of the distances from the origin to the closest lattice point and to the next-closest lattice point on a different line through the origin. For the lattice $\mathbb{Z}[\sqrt{-6}]$ this ratio is $1/\sqrt{6}$ while for the other lattice it is $2/\sqrt{6}$. If the lattices differed only by rotation and rescaling the ratios would be the same.

As another example, consider the lattices L_Q in $\mathbb{Z}[\sqrt{-5}]$ for the non-equivalent forms $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$ of discriminant -20. The two lattices are $L(1,\sqrt{-5}) = \mathbb{Z}[\sqrt{-5}]$ and $L(2, 1+\sqrt{-5})$.

$x^2 + 5y^2 \longrightarrow L(1,\sqrt{-5})$

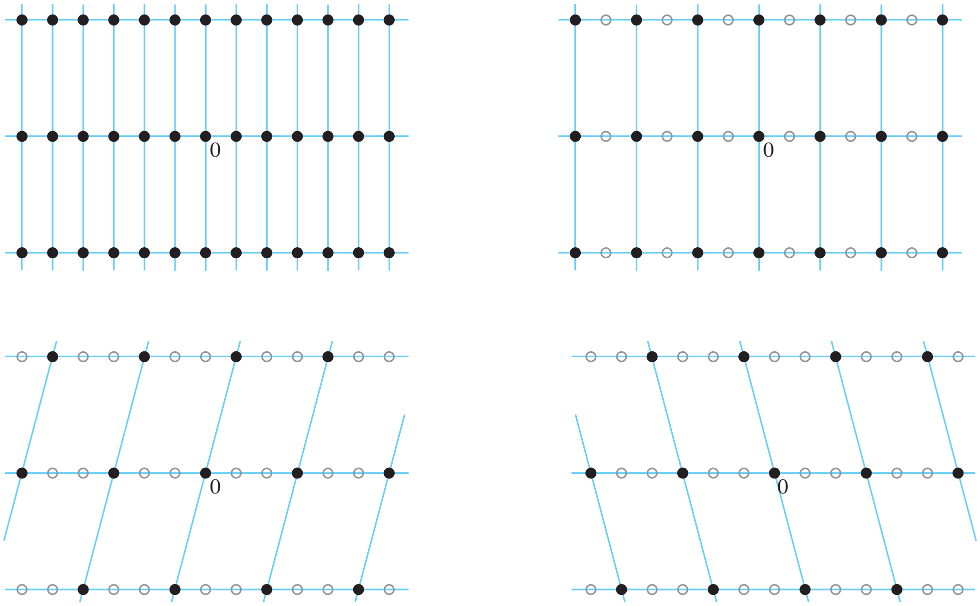


$2x^2 + 2xy + 3y^2 \longrightarrow L(2, 1+\sqrt{-5})$



Again we can check the lattices are not related just by rotation and rescaling by computing the same ratios of distances, which are $1/\sqrt{5}$ and $2/\sqrt{6}$ for the two lattices. It is also clear visually that the first lattice is rectangular while the second is not.

A slightly more complicated example is $\mathbb{Z}[\sqrt{-14}]$ with $\Delta = -56$ where there are four proper equivalence classes of forms given by x^2+14y^2, $2x^2+7y^2$, $3x^2+2xy+5y^2$, and $3x^2-2xy+5y^2$. The corresponding lattices are $L(1,\sqrt{-14})$, $L(2,\sqrt{-14})$, $L(3,1+\sqrt{-14})$, and $L(3,-1+\sqrt{-14})$ shown below.



Here the third and fourth forms are equivalent but not properly equivalent since their topographs have a source vertex surrounded by the three distinct numbers $3,5,6$. The topographs are mirror images obtained by changing the sign of x or y, so the corresponding lattices are also mirror images obtained by reflecting across the x or y axis. No two of the four lattices are equivalent under rotation and rescaling.

The examples we have seen so far may lead one to ask how exact a correspondence there is between proper equivalence classes of forms of a given discriminant Δ and the shapes of lattices that are ideals in R_Δ, where two lattices that differ only by rotation and rescaling are regarded as having the same shape. The main theorem will be that this is an exact one-to-one correspondence for negative discriminants, while for positive discriminants there is an analogous one-to-one correspondence with a more subtle notion of 'shape' for lattices.

As a first step in this direction let us ask whether every ideal in R_Δ is equal to L_Q for some form Q of discriminant Δ. One way to see that this is not true is to observe that the lattices $L_Q = L(a,(b+\sqrt{\Delta})/2)$ have the special property that they contain an element $(b+\sqrt{\Delta})/2$ lying in the first row of the lattice R_Δ above the x axis, but this is not the case for all ideals since we can expand a lattice L by a positive integer factor n to get a new lattice nL consisting of all elements $n\alpha$ for α in L, and nL is an ideal if L is. Thus if we start with an ideal L_Q we obtain another ideal nL_Q which has no elements in the first row of R_Δ above the x axis if $n > 1$. However, nothing more complicated than this can happen:

Proposition 7.13. *Every ideal in R_Δ is equal to nL_Q for some positive integer n and* *some form* $Q(x,y) = ax^2 + bxy + cy^2$ *of discriminant* Δ *with* $a > 0$*.*

Proof: We write R_Δ as $\mathbb{Z}[\tau]$ for $\tau = \sqrt{D}$ when $\Delta = 4D$ and $\tau = (1 + \sqrt{\Delta})/2$ when $\Delta = 4d + 1$. Let L be a lattice in $\mathbb{Z}[\tau]$. Since L is not entirely contained in the x axis there exist elements $m + n\tau$ in L with $n > 0$. Choose such an element $\alpha = m + n\tau$ with minimum positive n, so α lies in the n^{th} row of $\mathbb{Z}[\tau]$ and there are no elements of L in any row between the 0^{th} and the n^{th} rows. Since L is a lattice all elements of L must then lie in rows numbered an integer multiple of n. For example the element $k\alpha$ lies in the kn^{th} row for each integer k. These elements $k\alpha$ lie on a line through the origin, and L must also contain elements not on this line, so some kn^{th} row must contain another element β of L besides $k\alpha$. The difference $\beta - k\alpha$ then lies in the x axis and is a nonzero integer in L. Choosing a minimal positive integer p in L, the lattice property of L implies that the integers in L are precisely the integer multiples of p. It follows that L contains the lattice $L(p,\alpha) = L(p, m + n\tau)$, and in fact L is equal to $L(p, m + n\tau)$ otherwise either p or n would not be minimal.

Now let us assume that L is an ideal in $\mathbb{Z}[\tau]$, not just a lattice. Then $p\tau$ lies in L since p does. Since $p\tau$ is in the p^{th} row of $\mathbb{Z}[\tau]$ we must have $p = an$ for some positive integer a. We also know that $\alpha\tau$ must lie in L where $\alpha = m + n\tau$ as above. In the case $\Delta = 4D$ we have $\tau = \sqrt{D}$ so $\alpha\tau = m\tau + n\tau^2 = m\tau + nD$. This is in the m^{th} row of $\mathbb{Z}[\tau]$ so n must divide m, say $m = nq$. In the case $\Delta = 4d + 1$ we have $\tau^2 = \tau + d$ so $\alpha\tau = (m + n)\tau + nd$. This is in the $(m + n)^{th}$ row of $\mathbb{Z}[\tau]$ so n divides $m + n$ and hence also n so we can again write $m = nq$. Thus $L = L(p, m + n\tau) = L(na, nq + n\tau) = nL(a, q + \tau)$. Note that $L(a, q + \tau)$ is an ideal since L is an ideal.

To finish the proof we would like to find integers b and c such that $q + \tau = (b + \sqrt{\Delta})/2$ and $\Delta = b^2 - 4ac$ since then $L(a, q + \tau)$ will be L_Q for $Q = ax^2 + bxy + cy^2$ with discriminant Δ. Consider first the case $\Delta = 4D$ so $q + \tau = q + \sqrt{D}$. This is an element of the ideal $L(a, q + \sqrt{D})$ so if we multiply it by $q - \sqrt{D}$ we get an integer $q^2 - D$ lying in $L(a, q + \sqrt{D})$. Thus $q^2 - D$ must be a multiple of a which is the smallest positive integer in $L(a, q + \sqrt{D})$, so we get an equation $q^2 - D = ac$ for some integer c. Hence we have $(2q)^2 - 4D = 4ac$, and since $4D = \Delta$ this can be rewritten as $\Delta = b^2 - 4ac$ for $b = 2q$. We also have $q + \tau = q + \sqrt{D} = (b + \sqrt{\Delta})/2$ so this finishes the case $\Delta = 4D$.

In the other case $\Delta = 4d + 1$ we again look at the product $(q + \tau)(q - \tau)$. By the same reasoning this must be a multiple of a, so $(q + \tau)(q - \tau) = ac$ for some integer c. Writing this out, we have

$$\begin{aligned} \Big(q + \frac{1 + \sqrt{\Delta}}{2}\Big)\Big(q + \frac{1 - \sqrt{\Delta}}{2}\Big) &= ac \\ (2q + 1 + \sqrt{\Delta})(2q + 1 - \sqrt{\Delta}) &= 4ac \\ (2q + 1)^2 - \Delta &= 4ac \end{aligned}$$

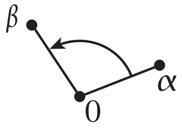
so if we take $b = 2q + 1$ we have $\Delta = b^2 - 4ac$ and $q + \tau = q + \frac{1+\sqrt{\Delta}}{2} = \frac{b+\sqrt{\Delta}}{2}$. □

We have seen how to go from a quadratic form Q to an ideal L_Q, and it will be useful to go in the opposite direction as well, from an ideal L in R_Δ to a quadratic form Q_L of discriminant Δ. As motivation we can start with the earlier formula $aQ(x,y) = N(ax + \frac{b+\sqrt{\Delta}}{2}y)$ which says that, up to the constant factor a, the form Q is given by restricting the usual norm in R_Δ to the elements $ax + \frac{b+\sqrt{\Delta}}{2}y$ in the ideal L_Q. We can try the same thing for any lattice $L = L(\alpha,\beta)$ in R_Δ, defining a quadratic form

$$Q(x,y) = N(\alpha x + \beta y) = (\alpha x + \beta y)(\overline{\alpha}x + \overline{\beta}y) = \alpha\overline{\alpha}x^2 + (\alpha\overline{\beta} + \overline{\alpha}\beta)xy + \beta\overline{\beta}y^2$$

Here the coefficients of x^2, xy, and y^2 are integers since they are equal to their conjugates. The form Q depends on the choice of the basis α, β for L. Another basis α', β' can be expressed as linear combinations $\alpha' = p\alpha + q\beta$, $\beta' = r\alpha + s\beta$ with integer coefficients. Since the change of basis can be reversed, going from α', β' back to α, β, the 2×2 matrix $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$ has determinant ± 1, and conversely any such matrix gives a valid change of basis for L. Changing the basis also produces a change of variables in the form $Q(x,y)$ since $N(\alpha' x + \beta' y) = N((p\alpha + q\beta)x + (r\alpha + s\beta)y) = N(\alpha(px+ry) + (\beta(qx+sy)) = Q(px+ry, qx+sy)$. Here the matrix is the transpose $\left(\begin{smallmatrix} p & r \\ q & s \end{smallmatrix}\right)$, with the same determinant ± 1. Thus changing the basis for L produces an equivalent form, and every equivalent form can be realized by some change of basis for L.

The form $N(\alpha x + \beta y)$ depends on the ordering for the two basis elements α and β since reversing their order interchanges x and y, which gives a mirror image topograph. We can eliminate this ambiguity by ordering α and β so that the angle from the ray from 0 passing through α to the ray from 0 passing through β is between 0 and π. We call this order the *positive* order. If we only use positively ordered bases, then the change of basis matrices have determinant $+1$ since they correspond to orientation-preserving linear transformations of the plane. Thus if we always use positively ordered bases, the lattice L gives rise to a proper equivalence class of quadratic forms.



The norm form $N(\alpha x + \beta y)$ associated to a lattice $L = L(\alpha,\beta)$ in R_Δ might not have discriminant Δ. For example, if we replace L by $nL = L(n\alpha, n\beta)$ this multiplies the norm form by n^2 and so the discriminant is multiplied by n^4. We can always rescale a form to have any discriminant we want just by multiplying it by a suitable positive constant, but this may lead to forms with non-integer coefficients. To illustrate this potential difficulty, suppose we take $\Delta = -4$ so $R_\Delta = \mathbb{Z}[i]$. The lattice $L(2,i)$ in $\mathbb{Z}[i]$ yields the form $N(2x + iy) = 4x^2 + y^2$ of discriminant -16, but to rescale this to have discriminant -4 we would have to take the form $2x^2 + \frac{1}{2}y^2$.

Fortunately this problem does not occur if we consider only lattices that are ideals. By Proposition 7.13 each ideal L in R_Δ is equal to a multiple $nL_Q = L(na, n\frac{b+\sqrt{\Delta}}{2})$ for some form $Q(x,y) = ax^2 + bxy + cy^2$ of discriminant Δ with $a > 0$. We have

$aQ(x,y) = N(ax + \frac{b+\sqrt{\Delta}}{2}y)$, hence $n^2aQ(x,y) = N(nax + n\frac{b+\sqrt{\Delta}}{2}y)$ which is the norm form for L in the basis $na, n\frac{b+\sqrt{\Delta}}{2}$. This basis is positively ordered since $a > 0$. By dividing this norm form for L by n^2a we get a form with integer coefficients and discriminant Δ, namely the form Q. If we change the basis $na, n\frac{b+\sqrt{\Delta}}{2}$ for L to some other positively ordered basis α, β, it is still true that the form $\frac{1}{n^2a}N(\alpha x + \beta y)$ has integer coefficients and discriminant Δ since this just changes Q to a properly equivalent form. [[[Clarify this??]]]

The scaling factor n^2a has a nice geometric interpretation as the number of parallel translates of the lattice L (including L itself) that are needed to completely cover the larger lattice R_Δ. In the special case $n = 1$ this is obvious since a basis for L in this case is $a, \frac{b+\sqrt{\Delta}}{2}$ with the latter point lying in the first row of R_Δ above the x axis, so we only need to translate L horizontally by the numbers $0, 1, \cdots, a-1$ to cover all of R_Δ. The case $n > 1$ follows from this case since this just amounts to rescaling the whole plane by a factor of n, and it takes n^2 parallel copies of nR_Δ to cover all of R_Δ.

For a lattice L in R_Δ the number of parallel translates of L needed to cover all of R_Δ is called the *norm* of L and written $N(L)$. Notice that this does not depend on choosing a basis for L. The preceding arguments prove:

Proposition 7.14. *For an ideal L in R_Δ with basis α, β the form $\frac{1}{N(L)}N(\alpha x + \beta y)$ has integer coefficients and discriminant Δ.* □

For an ideal L with positively ordered basis α, β the form $\frac{1}{N(L)}N(\alpha x + \beta y)$ will be denoted by Q_L, although a more precise notation might be $Q_{L(\alpha,\beta)}$ since the form depends on the choice of basis.

Different ideals L in R_Δ can give properly equivalent forms Q_L. Obviously a rescaling nL of L gives the same form Q_L. More generally, suppose we multiply all elements of an ideal $L(\alpha, \beta)$ by a fixed element γ of R_Δ to get a new lattice $\gamma L(\alpha, \beta) = L(\gamma\alpha, \gamma\beta)$ which is again an ideal. Taking norms, we have $N(\gamma\alpha x + \gamma\beta y) = N(\gamma)N(\alpha x + \beta y)$, so if $N(\gamma) > 0$ the new form $N(\gamma\alpha x + \gamma\beta y)$ is just a rescaling of $N(\alpha x + \beta y)$, with rescaling factor $N(\gamma L) = N(\gamma)N(L)$. Thus after rescaling to get discriminant Δ we have $Q_{\gamma L} = Q_L$ when $N(\gamma) > 0$. As a technical point, we should check that $\gamma\alpha, \gamma\beta$ is positively ordered if α, β is, which we can do in the following way. In $\mathbb{Q}(\sqrt{\Delta})$ we have $(a + b\sqrt{\Delta})(x + y\sqrt{\Delta}) = (ax + b\Delta y) + (ay + bx)\sqrt{\Delta}$ so multiplication by $a + b\sqrt{\Delta}$ is a linear transformation with matrix $\left(\begin{smallmatrix} a & b\Delta \\ b & a \end{smallmatrix}\right)$. This has determinant $a^2 - b^2\Delta = N(a + b\sqrt{\Delta})$ so it preserves orientation when $N(a + b\sqrt{\Delta}) > 0$. This means that $\gamma\alpha, \gamma\beta$ is positively oriented if α, β is positively oriented and $N(\gamma) > 0$.

In view of these observations we will say that two ideals L and L' in R_Δ are *strictly equivalent*, written $L \sim L'$, if $L' = \gamma L$ for some γ with $N(\gamma) > 0$, where the word 'strictly' is added to emphasize the condition $N(\gamma) > 0$. It makes no essential difference whether we require γ to be in R_Δ or just in $\mathbb{Q}(\sqrt{\Delta})$ since in the latter case there is some positive integer multiple $n\gamma$ that lies in R_Δ, so we can realize the equivalence $L \sim \gamma L$ as a composition of two equivalences $L \sim n\gamma L \sim \gamma L$ which only involve multiplication by elements of R_Δ, namely $n\gamma$ and n.

Now we can state the main result in this section:

Theorem 7.15. *There is a one-to-one correspondence between the set of strict equivalence classes of ideals in R_Δ and the set of proper equivalence classes of quadratic forms of discriminant Δ. Under this correspondence an ideal L with a positively ordered basis α, β corresponds to the form $Q_L = \frac{1}{N(L)}N(\alpha x + \beta y)$. (When $\Delta < 0$ we are restricting attention just to forms with positive values, as usual.)*

Thus for negative discriminants the proper equivalence classes of forms correspond to the various shapes of lattices that are ideals, up to rotation and rescaling since this is how two lattices L and αL are related when α is a complex number. For example, for the nine negative discriminants where all forms are equivalent (hence properly equivalent), all ideals have the same shape. We already saw this for the discriminants $-3, -4, -7, -8, -11$ where there is a Euclidean algorithm, but the theorem says it is also true for discriminants $-19, -43, -67, -163$.

Proof of Theorem 7.15: We have seen that there is a well-defined function Φ from strict equivalence classes of ideals to proper equivalence classes of forms, induced by sending an ideal L to the form Q_L. The function Φ is onto since in each proper equivalence class of forms there are forms $Q(x,y) = ax^2 + bxy + cy^2$ with $a > 0$ (this is automatic for negative discriminants) and then as we saw above, $Q = Q_L$ for the lattice $L = L_Q$.

To show that Φ is one-to-one, suppose we have two ideals L and L' with positively ordered bases α, β and α', β' such that the forms Q_L and $Q_{L'}$ with respect to these bases are properly equivalent. We can assume the basis α, β is chosen so that $Q_L(1,0) > 0$ since this is automatic when $\Delta < 0$, and when $\Delta > 0$ the form Q_L is hyperbolic with both positive and negative values in its topograph. Since Q_L and $Q_{L'}$ are properly equivalent we can choose α', β' so that we have actual equality $Q_L(x,y) = Q_{L'}(x,y)$ for all x and y.

The norm forms $N(\alpha x + \beta y)$ and $N(\alpha' x + \beta' y)$ are rescalings of each other since they rescale to $Q_L(x,y)$ and $Q_{L'}(x,y)$ which are equal. We have $N(\alpha) > 0$ and $N(\alpha') > 0$ since $Q_L(1,0) = Q_{L'}(1,0) > 0$. Let $\gamma = \beta/\alpha$ and $\gamma' = \beta'/\alpha'$, elements of $\mathbb{Q}(\sqrt{\Delta})$. We have $N(\alpha x + \beta y) = N(\alpha)N(x + \gamma y)$ and likewise $N(\alpha' x + \beta' y) = N(\alpha')N(x + \gamma' y)$ so the two forms $N(x + \gamma y)$ and $N(x + \gamma' y)$ are also rescalings of each other. Note that these two forms have rational coefficients, not necessarily integers. Since the forms $N(x + \gamma y)$ and $N(x + \gamma' y)$ are rescalings of each other and take the same value at $(x,y) = (1,0)$, namely $N(1) = 1$, they must actually be equal.

Next we show that in fact $\gamma = \gamma'$. Let $\gamma = r + s\sqrt{\Delta}$ and $\gamma' = r' + s'\sqrt{\Delta}$ with

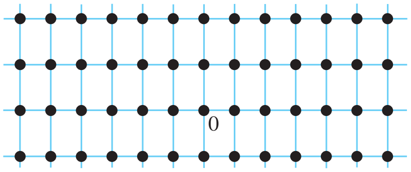
r, s, r', s' in $\mathbb{Q}$. Consider the difference $N(1+\gamma)-N(\gamma)$ which equals $((r+1)^2-s^2\Delta)-(r^2-s^2\Delta) = 2r+1$. Similarly $N(1+\gamma')-N(\gamma') = 2r'+1$. Since the forms $N(x+\gamma y)$ and $N(x+\gamma' y)$ are equal we must therefore have $r = r'$. We also have $N(\gamma) = N(\gamma')$ by evaluating both forms at $(x,y) = (0,1)$. Thus $r^2 - s^2\Delta = r'^2 - s'^2\Delta$, and from $r = r'$ we deduce that $s = \pm s'$. The bases $1, \gamma$ and $1, \gamma'$ are positively ordered since this was true for α, β and α', β' and multiplication by α and α' preserves orientation of the plane since $N(\alpha) > 0$ and $N(\alpha') > 0$. Since both $1, \gamma$ and a, γ' are positively ordered we must have $s = +s'$. Thus $\gamma = \gamma'$ as claimed.

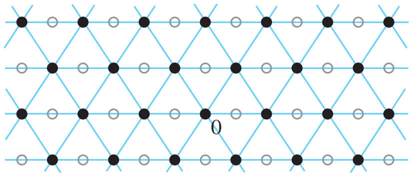
The lattice $L(1,\gamma)$ may not lie in R_Δ since γ is only an element of $\mathbb{Q}(\sqrt{\Delta})$, but we can rescale $L(1,\gamma)$ to a lattice $nL(1,\gamma) = L(n, n\gamma)$ in R_Δ by multiplying by a positive integer n such that $n\gamma$ is in R_Δ. Then $nL(\alpha,\beta) = \alpha L(n, n\gamma)$ since $L(\alpha,\beta) = \alpha L(1,\gamma)$. Likewise we have $nL(\alpha',\beta') = \alpha' L(n, n\gamma')$ with the same scaling factor n since $\gamma = \gamma'$. Thus if we use the symbol $\sim$ to denote strict equivalence, we have

$$L = L(\alpha,\beta) \sim nL(\alpha,\beta) \sim L(n,n\gamma) = L(n,n\gamma') \sim nL(\alpha',\beta') \sim L(\alpha',\beta') = L'$$

This finishes the proof that Φ is one-to-one. □

The correspondence between forms and ideals includes nonprimitive forms as well as primitive forms, but the ideals corresponding to primitive and nonprimitive forms behave somewhat differently. Let us illustrate this by the example of discriminant $\Delta = -12$ where there are two equivalence classes of forms, given by the primitive form $x^2 + 3y^2$ and the nonprimitive form $2x^2 + 2xy + 2y^2$. The ideal for $x^2 + 3y^2$ is $L(1, \sqrt{-3}) = \mathbb{Z}[\sqrt{-3}] = R_\Delta$ while for $2x^2 + 2xy + 2y^2$ the ideal is $L(2, 1 + \sqrt{-3})$.





The ideal for $2x^2+2xy+2y^2$ is a lattice of equilateral triangles, and it has the special property that it is taken to itself not just by multiplication by elements of $\mathbb{Z}[\sqrt{-3}]$ but also by the 60 degree rotation given by multiplication by the element $\omega = (1+\sqrt{-3})/2$ in the larger ring $\mathbb{Z}[\omega]$ which is R_Δ for $\Delta = -3$. Hence the lattice $L(2, 1+\sqrt{-3})$ is taken to itself by all elements of $\mathbb{Z}[\omega]$ and so this lattice is an ideal in $\mathbb{Z}[\omega]$, not just in the original ring $\mathbb{Z}[\sqrt{-3}] = R_\Delta$.

More generally, suppose we start with a form $Q = ax^2 + bxy + cy^2$ of discriminant Δ and then consider the nonprimitive form $kQ = kax^2 + kbxy + kcy^2$ of discriminant $k^2\Delta$ for some integer $k > 1$. The associated ideal L_{kQ} is then $L(ka, \frac{kb+k\sqrt{\Delta}}{2}) = kL(a, \frac{b+\sqrt{\Delta}}{2}) = kL_Q$. This is an ideal not just in $R_{k^2\Delta}$ but also in the larger ring R_Δ since it is k times an ideal in R_Δ, namely k times L_Q.

Let us say that an ideal L in R_Δ is *primitive* if it is not an ideal in any larger ring than R_Δ in $\mathbb{Q}(\sqrt{\Delta})$. For L to be nonprimitive means therefore that L is an ideal in some strictly larger ring than R_Δ in $\mathbb{Q}(\sqrt{\Delta})$.

Proposition 7.16. *A form Q of discriminant Δ is primitive if and only if the corresponding ideal L_Q is primitive in R_Δ.*

Proof: We observed above that a nonprimitive form Q of discriminant Δ gives a nonprimitive ideal L_Q in R_Δ. To show the converse, that a primitive form Q gives a primitive ideal L_Q, suppose that $Q = ax^2 + bxy + cy^2$ is a primitive form of discriminant Δ. We wish to show that L_Q is not an ideal in any larger ring than R_Δ in $\mathbb{Q}(\sqrt{\Delta})$. Let us write $L_Q = L(a,\tau)$ for $\tau = (b+\sqrt{\Delta})/2)$. Note that $R_\Delta = \mathbb{Z}[\tau]$ since b has the same parity as Δ. Also $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\tau)$.

Suppose we have an element $\alpha = r + s\tau$ in $\mathbb{Q}(\tau)$ such that $\alpha L(a,\tau)$ is contained in $L(a,\tau)$. Here r and s are rational numbers. Our goal is to show that Q being primitive forces r and s to be integers. This will say that α is in $\mathbb{Z}[\tau] = R_\Delta$, and hence that $L(a,\tau)$ is a primitive ideal in R_Δ.

For $\alpha L(a,\tau)$ to be contained in $L(a,\tau)$ means that both αa and $\alpha\tau$ are in $L(a,\tau)$. We have $\alpha a = ra + sa\tau$, and for this to be in $L(a,\tau)$ which consists of the linear combinations $xa + y\tau$ with x and y integers means that r is an integer and sa is an integer. It remains to see that s itself is an integer, using the condition that $\alpha\tau$ is in $L(a,\tau)$.

To compute $\alpha\tau$ we use the fact that τ is a root of the equation $x^2 - bx + ac = 0$ so $\tau^2 = b\tau - ac$. Then we have

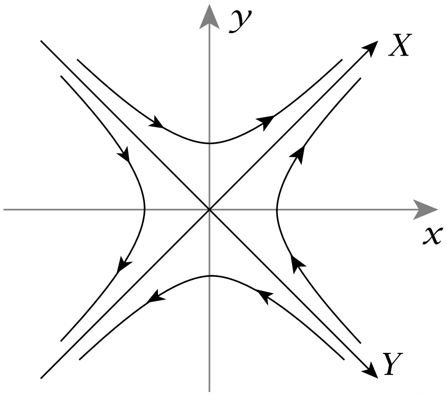
$$\alpha\tau = r\tau + s\tau^2 = r\tau + s(b\tau - ac) = -sac + (r+sb)\tau$$

For this to be in $L(a,\tau)$ means that sc and $r + sb$ are integers. We already know that r is an integer, so $r + sb$ being an integer is equivalent to sb being an integer. Thus we know that all three of sa, sb, and sc are integers. From this we can deduce that s is an integer since a, b, and c have no common divisors (except 1) by the assumption that the form Q is primitive. Namely, let us write s as a fraction $\frac{m}{n}$ in lowest terms. Then sa being an integer says that n divides a. Similarly sb and sc being integers says that n divides b and c. But 1 is the only common divisor of a, b and c so $n = 1$. Thus s is an integer and we are done. □

For negative discriminants the relation of strict equivalence of ideals corresponds geometrically to rotation and rescaling of lattices. There is an analogous interpretation for positive discriminants but it involves replacing rotations by somewhat more complicated motions of the plane, as we shall now see.

What we want is a geometric description of the transformation T_γ of $\mathbb{Q}(\sqrt{\Delta})$ defined by multiplying by a fixed nonzero element γ, so $T_\gamma(\alpha) = \gamma\alpha$. For a positive discriminant Δ we are regarding $\mathbb{Q}(\sqrt{\Delta})$ as a subset of the plane by giving an element $\alpha = a + b\sqrt{\Delta}$ the coordinates $(x,y) = (a, b\sqrt{\Delta})$. The norm $N(\alpha) = a^2 - \Delta b^2$ is then equal to $x^2 - y^2$ and T_γ takes each hyperbola $x^2 - y^2 = k$ to a hyperbola $x^2 - y^2 = N(\gamma)k$ since $N(\gamma\alpha) = N(\gamma)N(\alpha)$.

To understand linear transformations of the plane that take hyperbolas $x^2 - y^2 = k$ to hyperbolas $x^2 - y^2 = k'$ it is convenient to changes the coordinates x and y to $X = x + y$ and $Y = x - y$. This changes the hyperbolas $x^2 - y^2 = k$ to the hyperbolas $XY = k$ whose asymptotes are the X and Y axes, at a 45 degree angle from the x and y axes.



Notice that since $(x, y) = (a, b\sqrt{\Delta})$, the coordinate $X = x + y$ is just $a + b\sqrt{\Delta}$, the real number α we started with, while $Y = x - y = a - b\sqrt{\Delta}$ is its conjugate $\overline{\alpha}$.

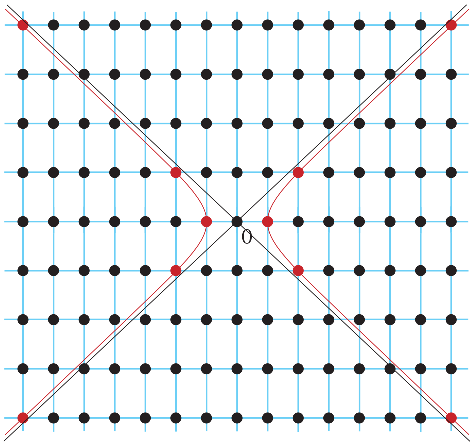
The transformation T_γ sends α to $\gamma\alpha$ so T_γ multiplies the X coordinate α by γ. To see how T_γ acts on the Y coordinate, observe that since the Y coordinate of α is $\overline{\alpha}$, the Y coordinate of $T_\gamma(\alpha)$ is $\overline{T_\gamma(\alpha)} = \overline{\gamma\alpha} = \overline{\gamma}\,\overline{\alpha}$, which means that the Y coordinate of $T_\gamma(\alpha)$ is $\overline{\gamma}$ times the Y coordinate of α. Thus T_γ multiplies the Y coordinate by $\overline{\gamma}$, so we have the simple formula $T_\gamma(X, Y) = (\gamma X, \overline{\gamma}Y)$.

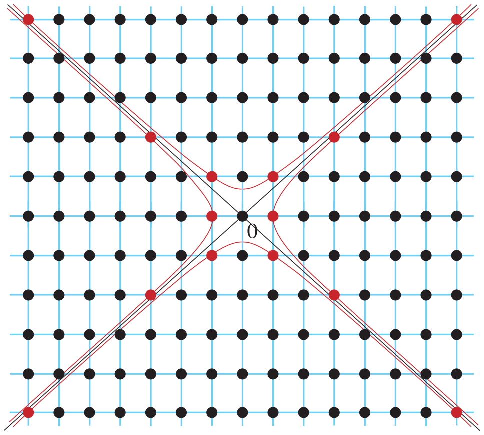
A consequence of the formula $T_\gamma(X, Y) = (\gamma X, \overline{\gamma}Y)$ is that T_γ takes the X axis to itself since the X axis is the points (X, Y) with $Y = 0$. Similarly, T_γ takes the Y axis to itself, the points where $X = 0$. In general, linear transformations taking both the X and Y axes to themselves have the form $T(X, Y) = (\lambda X, \mu Y)$ for real constants λ and μ. As a special case, when $\mu = \lambda^{-1}$ the transformations $T(X, Y) = (\lambda X, \lambda^{-1}Y)$ take each hyperbola $XY = k$ to itself. When $\lambda > 1$ the X axis is stretched by a factor of λ and the Y axis is shrunk by λ. Thus we are sliding each hyperbola along itself in the direction indicated by the arrows in the figure above. When λ is between 0 and 1 the situation is reversed and the Y axis is stretched while the X axis is shrunk.

When $\lambda > 0$ and $\mu > 0$ we can rescale the transformation $T(X, Y) = (\lambda X, \mu Y)$ to $\frac{1}{\sqrt{\lambda\mu}}T(X, Y) = (\sqrt{\lambda/\mu}\,X, \sqrt{\mu/\lambda}\,Y)$ which is a transformation of the type considered in the preceding paragraph, sliding each hyperbola along itself. Thus a transformation $T(X, Y) = (\lambda X, \mu Y)$ with λ and μ positive is a composition of a 'hyperbola-slide' and a rescaling. This is analogous to compositions of rotations and rescalings in the situation of negative discriminants. Allowing λ or μ to be negative then allows reflections across the X or Y axes as well. If both λ and μ are negative the composition of these two reflections is a 180 degree rotation of the plane.

Now we specialize to the situation of a transformation T_γ of R_Δ given by multiplication by an element γ in R_Δ with $N(\gamma) > 0$. The condition $N(\gamma) > 0$ implies that T_γ preserves the orientation of the plane and also the sign of the norm so it either takes each quadrant of the XY plane (north, south, east, or west) to itself or to the opposite quadrant. In the former case T_γ is a composition of a hyperbola-slide and a rescaling, while in the latter case there is also a composition with a 180 degree rotation of the plane, which is just T_γ for $\gamma = -1$. The sign of γ distinguishes these two cases since if $\gamma > 0$ the transformation T_γ takes positive numbers to positive numbers so the positive X axis goes to itself, while if $\gamma < 0$ the positive X axis goes to the negative X axis.

If γ is a unit with $N(\gamma) = +1$ then each hyperbola $x^2 - y^2 = k$ is taken to itself by T_γ. The two branches of the hyperbola are distinguished by the sign of X, so if γ is positive then T_γ slides each branch along itself while if γ is negative this slide is combined with a 180 degree rotation of the plane. If we choose γ to be the smallest unit greater than 1 with $N(\gamma) = +1$ then the powers γ^n for integers n lie along the right-hand branch of the hyperbola $x^2 - y^2 = 1$, becoming farther and farther apart as one moves away from the origin, and T_γ slides each one of these points along the hyperbola to the next one, increasing the X coordinate. The case $\Delta = 12$ is shown in the first figure below, with $R_\Delta = \mathbb{Z}[\sqrt{3}]$. The basic unit γ is $2 + \sqrt{3}$, and the figure shows the units $\pm\gamma^n$ for $|n| \le 2$ positioned along the hyperbola $x^2 - y^2 = 1$, with $\gamma^2 = 7 + 4\sqrt{3}$ in the upper right corner of the figure.





For some discriminants there are units γ with $N(\gamma) = -1$ in addition to those with $N(\gamma) = +1$. The transformation T_γ for the smallest $\gamma > 1$ of norm -1 is a composition of a hyperbola slide and reflection across the X axis. The powers γ^n then lie alternately on $x^2 - y^2 = +1$ and $x^2 - y^2 = -1$. This happens for example in $\mathbb{Z}[\sqrt{2}]$ with $\gamma = 1 + \sqrt{2}$ as shown in the second figure above, where $\gamma^2 = 3 + 2\sqrt{2}$ and $\gamma^3 = 7 + 5\sqrt{2}$.

Each ideal in R_Δ is taken into itself by the transformations T_γ for γ in R_Δ, but when γ is a unit each ideal is taken *onto* itself since the inverse transformation $(T_\gamma)^{-1}$ is just $T_{\gamma^{-1}}$ which also takes the ideal to itself. Thus all ideals in R_Δ have “hyperbolic symmetries", the hyperbola-preserving transformations T_γ for units γ.

Although we can describe geometrically in terms of hyperbola slides and rescaling how the ideals corresponding to properly equivalent quadratic forms of positive discriminant are related, the result is somehow less satisfying than in the negative discriminant case. Hyperbola slides are not nearly as simple visually as rotations, making it harder to see at a glance whether two lattices are related by hyperbola slides and rescaling or not. This may be a reflection of the fact that hyperbolic forms do not have a canonical reduced form as elliptic forms do, making it a little more difficult to determine whether two hyperbolic forms are equivalent.

The Class Group

The main reason we have introduced ideals is because there is a nice way to define a multiplicative structure in the set of all ideals in R_Δ. Thus every pair of ideals L and M in R_Δ has a product LM which is again an ideal. Using the correspondence between ideals and forms, this leads to a group structure in the set of proper equivalence classes of primitive forms of discriminant Δ, resulting in the class group $CG(\Delta)$ that was described briefly in a few examples in the first section of Chapter 6. This group structure was originally defined by Gauss directly on forms without introducing ideals, but the direct definition is more complicated and has been largely supplanted by the approach via ideals, especially since the latter approach has broader applicability.

A key property of multiplication of forms is that it corresponds to multiplication of the numbers represented by the forms. A consequence of this will be that once one knows which primes are represented by which forms in a given discriminant, one can then deduce which nonprimes are represented by each form, at least in the case of fundamental discriminants. This depends on the basic fact that all ideals in R_Δ factor uniquely into prime ideals when Δ is a fundamental discriminant.

In order to form the product LM of two ideals L and M in R_Δ one's first guess might be to let LM consist of all products $\alpha\beta$ of elements α in L and β in M. This sometimes works but not always, as we will see in an example later. The difficulty is that for two products $\alpha_1\beta_1$ and $\alpha_2\beta_2$ the sum $\alpha_1\beta_1 + \alpha_2\beta_2$ might not be equal to a product $\alpha\beta$ of an element of L with an element of M, as it would have to be if the set of all products $\alpha\beta$ was to be an ideal. This difficulty can be avoided by defining LM to be the set of all sums $\alpha_1\beta_1 + \cdots + \alpha_n\beta_n$ with each α_i in L and each β_i in M. With this definition LM is obviously closed under addition as well as subtraction. Also, multiplying such a sum $\sum_i \alpha_i\beta_i$ by an element γ in R_Δ gives an element of LM since $\gamma\sum_i \alpha_i\beta_i = \sum_i(\gamma\alpha_i)\beta_i$ and the latter sum is in LM since each term $\gamma\alpha_i$ is in L because L is an ideal. To finish the verification that LM is an ideal we need to check that it is a lattice since we defined ideals in R_Δ to be lattices that are taken to themselves by multiplication by arbitrary elements of R_Δ. To check that LM is a lattice we need to explain a few more things about lattices.

We defined a lattice in R_Δ to be a set $L(\alpha,\beta)$ of elements $x\alpha+y\beta$ as x and y range over all integers, where α and β are two fixed nonzero elements of R_Δ that do not lie on the same line through the origin. More generally we could define $L(\alpha_1,\cdots,\alpha_n)$ to be the set of all linear combinations $x_1\alpha_1+\cdots+x_n\alpha_n$ with coefficients x_i in $\mathbb{Z}$, where not all the α_i's lie on the same line through the origin (so in particular at least two α_i's are nonzero). It is not immediately obvious that $L(\alpha_1,\cdots,\alpha_n)$ is a lattice, but this is true and can be proved by the following procedure which also gives a way of computing what the lattice is.

There are three ways in which the set of generators α_i for $L(\alpha_1,\cdots,\alpha_n)$ can be modified without changing the set $L(\alpha_1,\cdots,\alpha_n)$:

(1) Replace one generator α_i with $\alpha_i+k\alpha_j$, adding an integer k times some other α_j to α_i.

(2) Replace some α_i by $-\alpha_i$.

(3) Interchange two generators α_i and α_j, or more generally permute the α_i's in any way.

After a modification of type (1) each integer linear combination of the new generators is also a linear combination of the old generators so the new $L(\alpha_1,\cdots,\alpha_n)$ is a subset of the old one, but the process can be reversed by another type (1) operation subtracting $k\alpha_j$ from the new α_i so the new $L(\alpha_1,\cdots,\alpha_n)$ also contains the old one hence must equal it. For the operations (2) and (3) this is also true, more obviously.

Lemma 7.17. *By applying some sequence of operations* (1)–(3) *to a set of generators* α_i *for* $L(\alpha_1,\cdots,\alpha_n)$ *it is always possible to produce a new set of generators* $\beta_1,\cdots,\beta_n$ *which are all zero except for* β_1 *and* β_2*. In particular* $L(\alpha_1,\cdots,\alpha_n)$ *is a lattice.*

Proof: Let us write R_Δ as $\mathbb{Z}[\tau]$ in the usual way. Each α_i can be written as $a_i+b_i\tau$ for integers a_i and b_i. We can then form a $2\times n$ matrix $\begin{pmatrix} a_1 & \cdots & a_n \\ b_1 & \cdots & b_n \end{pmatrix}$ whose columns correspond to the α_i's. The operations (1)–(3) correspond to adding an integer times one column to another column, changing the sign of a column, and permuting columns.

Our aim is to use these three column operations to simplify the matrix until only the first two columns are nonzero. First we focus on the second row. This must have a nonzero entry since the α_i's are not all contained in the x axis. The nonzero entries in the second row can be made all positive by changing the sign of some columns. Choose a column with smallest positive entry b_i. By subtracting suitable multiples of this column from other columns with positive b_j's we can make all other b_j's either zero or positive integers smaller than b_i. This process can be repeated using columns with successively smaller second entries until only one nonzero b_i remains. Switching this column with the first column, we can then assume that $b_i=0$ for all $i>1$.

Now we do the same procedure for columns 2 through n using the entries a_i rather than b_i. Since these columns have $b_i = 0$, nothing changes in the second row. After this step is finished, only the first two columns will be nonzero. Note that neither of these columns can have both entries zero since otherwise $L(\alpha_1, \cdots, \alpha_n)$ would be entirely contained in a line through the origin. □

If we apply the procedure just described to a lattice $L = L(\alpha, \beta)$ that already has just two generators, it will produce a 2×2 matrix with one entry in the second row equal to zero, so we may assume the matrix is $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$, and we can further assume that $a > 0$ and $c > 0$. By adding a suitable integer multiple of the first column to the second column we can then arrange that $0 \le b < a$. This gives a basis $a, b + c\tau$ for L that is called a *reduced basis*. A reduced basis is unique since a is the smallest positive integer in L and the first row of L above the x axis is in the c^{th} row of $\mathbb{Z}[\tau]$, with the elements of L in this row equally spaced a units apart so there is a unique such element $b + c\tau$ with $0 \le b < a$. Thus one can determine whether two lattices are equal by computing a reduced basis for each and seeing whether these are equal. (The reader might compare the procedure we have just described with what we did in the first paragraph of the proof of Proposition 7.13 by a more geometric argument.)

For a lattice L with reduced basis $a, b+c\tau$ it is easy to compute the norm $N(L)$ as the product ac. This can be seen in two steps. First, it takes a horizontal translates of L to cover all the integers on the x-axis, and these translates also cover the c^{th} row of R_Δ as well as all rows labeled by an integer multiple of c. All the rows between these rows contain no elements of L so to cover all of R_Δ it then takes c translates in the direction of τ of all the rows covered so far. Thus a total of ac translates of L are needed to cover all of R_Δ, which means that $N(L) = ac$.

Notice that ac is the determinant of the matrix $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$ associated to the reduced basis $a, b + c\tau$. More generally for an arbitrary basis $\alpha = a + b\tau, \beta = c + d\tau$ for $L = L(\alpha, \beta)$ we have $N(L) = |ad - bc|$, the absolute value of the determinant of the associated matrix $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$. This is because the operations (1)–(3) that transform an arbitrary basis into a reduced basis leave the determinant unchanged, up to sign, and $N(L)$ is always positive by its definition as the number of translates of L needed to cover R_Δ.

One could ask whether broadening the definition of $L(\alpha_1, \cdots, \alpha_n)$ to allow an infinite number of generators α_i would lead to anything new, and the answer is No. Consider the effect of adding one more generator α_{n+1} to $L(\alpha_1, \cdots, \alpha_n)$. After finding a reduced basis $a, b + c\tau$ for $L(\alpha_1, \cdots, \alpha_n)$ we can then apply the reduction process to the matrix obtained from $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$ by adding a third column corresponding to α_{n+1}. This could replace a or c by smaller positive integers, but this can happen for only finitely many values of n and eventually the values of a and c must stabilize. The value of b could not then change by enlarging $L(a, b + c\tau)$ by adding a new generator since the enlarged lattice would have two elements $b + c\tau$ and $b' + c\tau$ with $|b - b'| < a$, so $|b - b'|$ would be a positive integer in the enlarged lattice smaller than a, which is impossible.

Let us restrict attention now to lattices that are ideals. One way to generate such a lattice is to start with elements $\alpha_1, \cdots, \alpha_n$ in R_Δ which can assume are nonzero and then consider the set of all elements $\sum_i \gamma_i \alpha_i$ for arbitrary coefficients γ_i in R_Δ rather than just taking integer coefficients as we would be doing for the lattice $L(\alpha_1, \cdots, \alpha_n)$. The usual notation for this set of all sums $\sum_i \gamma_i \alpha_i$ is $(\alpha_1, \cdots, \alpha_n)$. As a lattice this is the same as $L(\alpha_1, \alpha_1\tau, \alpha_2, \alpha_2\tau, \cdots, \alpha_n, \alpha_n\tau)$ where $R_\Delta = \mathbb{Z}[\tau]$ since each coefficient γ_i can be written as $x_i + y_i\tau$ for integers x_i and y_i. To be sure that $(\alpha_1, \cdots, \alpha_n)$ really is a lattice, even when $n = 1$, we can check that α_1 and $\alpha_1\tau$ do not lie on the same line through the origin. To see that this is so, observe first that all points of the full lattice R_Δ that lie on the line through the origin passing through α_1 are rational multiples of α_1. However, if $\alpha_1\tau$ were a rational multiple $r\alpha_1$ we would have $\tau = r$ since we assume α_1 is not zero. However this is impossible since τ is not a rational number.

Observe that if a lattice $L(\alpha_1, \cdots, \alpha_n)$ is an ideal, then $L(\alpha_1, \cdots, \alpha_n)$ is equal to $(\alpha_1, \cdots, \alpha_n)$ since every product $\gamma\alpha_i$ with γ in R_Δ can be rewritten as an integer linear combination of $\alpha_1, \cdots, \alpha_n$ if $L(\alpha_1, \cdots, \alpha_n)$ is an ideal. A consequence of this, using Lemma 7.17, is that every ideal $(\alpha_1, \cdots, \alpha_n)$ with $n > 2$ can be rewritten as an ideal (β_1, β_2).

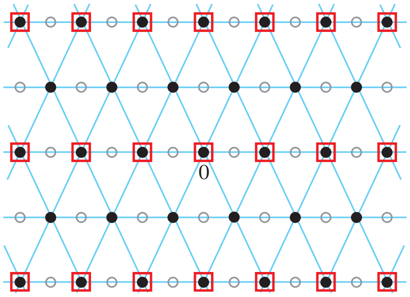
While every ideal in R_Δ can be written as (α, β) with two generators, only certain special ideals can be written as (α) with a single generator, so $(\alpha) = \alpha R_\Delta$. Such an ideal (α) is called a *principal ideal.* Under the correspondence between ideals in R_Δ and quadratic forms of discriminant Δ, principal ideals (α) with $N(\alpha) > 0$ correspond to forms equivalent to the principal form since the principal form $ax^2 + bxy + cy^2$ has $a = 1$ so the associated ideal $(a, \frac{b+\sqrt{\Delta}}{2})$ contains 1 and hence equals $R_\Delta = (1)$, and then for a form Q equivalent to the principal form (hence properly equivalent to it since the principal form has mirror symmetry) the associated ideal L_Q will be $\alpha R_\Delta = (\alpha)$ for some α with $N(\alpha) > 0$. In the case of negative discriminant the condition $N(\alpha) > 0$ holds automatically, and a principal ideal is a lattice having the same shape as the full lattice R_Δ since the lattice αR_Δ is obtained from R_Δ by rotation and rescaling.

For positive discriminants a principal ideal (α) can have $N(\alpha) < 0$ and then the corresponding form might not be equivalent to the principal form. For example for $\Delta = 12$ with $R_\Delta = \mathbb{Z}[\sqrt{3}]$ the form $3x^2 - y^2$ is not equivalent to the principal form $x^2 - 3y^2$ but rather to its negative, and the ideal associated to $3x^2 - y^2$ is $(3, \sqrt{3})$ which equals the principal ideal $(\sqrt{3})$ since $3 = \sqrt{3}\sqrt{3}$ lies in $(\sqrt{3})$. Here $N(\sqrt{3}) = -3 < 0$. By contrast, when $\Delta = 8$ with $R_\Delta = \mathbb{Z}[\sqrt{2}]$ the principal ideal $(\sqrt{2})$ has $N(\sqrt{2}) < 0$ but the associated form $2x^2 - y^2$ does happen to be equivalent to the principal form. This can be explained by the fact that the fundamental unit in $\mathbb{Z}[\sqrt{2}]$ is $1+\sqrt{2}$ which has norm -1. In general, if we multiply an ideal L by a unit ε then $\varepsilon L = L$, so multiplying the ideal $(\sqrt{2})$ by the unit $1+\sqrt{2}$ gives the same ideal back again but now expressed as $(2+\sqrt{2})$ with $N(2+\sqrt{2}) > 0$. In the previous case of $\mathbb{Z}[\sqrt{3}]$ the fundamental unit is $2+\sqrt{3}$ of norm 1 so all units have norm 1. This means that we cannot express $(\sqrt{3})$ as (α) with $N(\alpha) > 0$ since it is a general fact about principle ideals that $(\alpha) = (\beta)$ exactly when $\beta = \varepsilon\alpha$ for some unit ε. (This is easy to show.)

When the class number for a given discriminant is one all forms are equivalent to the principal form, hence properly equivalent to it, so all ideals are strictly equivalent and can therefore be expressed as $\alpha(1) = (\alpha)$ with $N(\alpha) > 0$ hence are principal ideals. For negative discriminants the converse is also true since the condition $N(\alpha) > 0$ is automatic, but for positive discriminants it can happen that all ideals are principal even though the class number is greater than 1. An example is the case $\Delta = 12$ that we just considered. Here the class number is 2 and every form is equivalent to either $x^2 - 3y^2$ or $3x^2 - y^2$ so every ideal is either $\alpha(1)$ or $\alpha(\sqrt{3})$ for some α with $N(\alpha) > 0$ so in particular every ideal is principal.

Now we return to products of ideals. For ideals $L = (\alpha_1, \alpha_2)$ and $M = (\beta_1, \beta_2)$ the product LM is the ideal $(\alpha_1\beta_1, \alpha_1\beta_2, \alpha_2\beta_1, \alpha_2\beta_2)$ since each of the four products $\alpha_i\beta_j$ is in LM and every element of LM is a sum of terms $\alpha\beta$ for $\alpha = \gamma_1\alpha_1 + \gamma_2\alpha_2$ and $\beta = \delta_1\beta_1 + \delta_2\beta_2$, so $\alpha\beta$ is a linear combination of the products $\alpha_i\beta_j$ with coefficients in R_Δ. Similarly the product of ideals $(\alpha_1, \cdots, \alpha_n)$ and $(\beta_1, \cdots, \beta_k)$ is the ideal generated by all the products $\alpha_i\beta_j$.

As an example let us compute the product of the ideals $L = (2, 1+\sqrt{-5})$ and $M = (2, 1-\sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$. The product $LM = (2, 1+\sqrt{-5})(2, 1-\sqrt{-5})$ is then the ideal $(4, 2+2\sqrt{-5}, 2-2\sqrt{-5}, 6)$. In this ideal each generator is a multiple of 2 so we can pull out a factor of 2 to get $LM = 2(2, 1+\sqrt{-5}, 1-\sqrt{-5}, 3)$. The ideal $(2, 1+\sqrt{-5}, 1-\sqrt{-5}, 3)$ contains 3 and 2 so it contains their difference 1. Once an ideal contains 1 it must be the whole ring, so $(2, 1+\sqrt{-5}, 1-\sqrt{-5}, 3) = (1) = \mathbb{Z}[\sqrt{-5}]$ hence $LM = 2(1) = (2)$. The figure below shows these ideals as lattices, with $(2, 1+\sqrt{-5})$ indicated by the heavy dots. This happens to be the same as $(2, 1-\sqrt{-5})$, so (2) is the square of the ideal $(2, 1+\sqrt{-5})$. This is the sublattice indicated by the dots in squares.



This example illustrates the general fact that a product LM of two ideals L and M is always a sublattice of both L and M since each term of a typical element $\sum_i \alpha_i\beta_i$ of LM lies in both L and M by the defining property of ideals.

This example also illustrates the fact that a product LM of two ideals need not consist merely of all products $\alpha\beta$ of an element of L with an element of M since the number 2 belongs to LM but if we had $2 = \alpha\beta$ then, computing norms, we would have $4 = N(\alpha)N(\beta)$. There are no elements of $\mathbb{Z}[\sqrt{-5}]$ of norm ± 2 since $N(x + y\sqrt{-5}) = x^2 + 5y^2 = \pm 2$ has no integer solutions. Thus either α or β would have norm ± 1 and hence be a unit ± 1 in $\mathbb{Z}[\sqrt{-5}]$, but neither 1 nor -1 is in $(2, 1 \pm \sqrt{-5})$, as one can see in the figure.

We have defined the norm of an ideal L in R_Δ geometrically as the number of parallel translates of L, including L itself, that are needed to fill up all of R_Δ, but for primitive ideals there is another interpretation of the norm $N(L)$ that is more like the definition of the norm of an element α as $N(\alpha) = \alpha\overline{\alpha}$. This is given by:

Proposition 7.18. *If L is a primitive ideal in R_Δ with conjugate $\overline{L}$ then $L\overline{L} = (N(L))$, the principal ideal generated by the norm $N(L)$.*

Proof: By Proposition 7.13 the ideal L is equal to $nL(a, \frac{b+\sqrt{\Delta}}{2})$ for some integer $n \geq 1$ and some form $ax^2 + bxy + cy^2$ of discriminant Δ with $a > 0$. It will suffice to prove the Proposition in the case $n = 1$ since replacing L by nL does not affect primitivity and it multiplies $N(L)$ by n^2, so both sides of the equation $L\overline{L} = (N(L))$ are multiplied by n^2. Thus we may take $L = L(a, \frac{b+\sqrt{\Delta}}{2})$ for the rest of the proof. Since L is primitive, so is the form $ax^2 + bxy + cy^2$ by Proposition 7.16.

Let $\tau = \frac{b+\sqrt{\Delta}}{2}$ so τ is a root of the equation $x^2 - bx + ac = 0$. Then $L = (a, \tau)$ and $\overline{L} = (a, \overline{\tau})$ so

$$L\overline{L} = (a^2, a\tau, a\overline{\tau}, \tau\overline{\tau}) = (a^2, a\tau, a\overline{\tau}, ac) = a(a, \tau, \overline{\tau}, c)$$

The ideal $(a, \tau, \overline{\tau}, c)$ contains the ideal $(a, \tau + \overline{\tau}, c) = (a, b, c)$. The latter ideal is all of R_Δ since it contains all integral linear combinations $ma + nb + qc$ and there is one such combination that equals 1 since the greatest common divisor of a, b, and c is 1 because the form $ax^2 + bxy + cy^2$ is primitive. (We know from Chapter 2 that the greatest common divisor d of a and b can be written as $d = ma + nb$, and then the greatest common divisor of d and c, which is the greatest common divisor of a, b, and c, can be written as an integral linear combination of d and c and hence also of a, b, and c.)

Thus the ideal $(a, \tau, \overline{\tau}, c)$ contains R_Δ and so must equal it. Hence we have $L\overline{L} = aR_\Delta = (a)$ and this equals $(N(L))$ since $N(L) = a$ for $L = L(a, \frac{b+\sqrt{\Delta}}{2})$. □

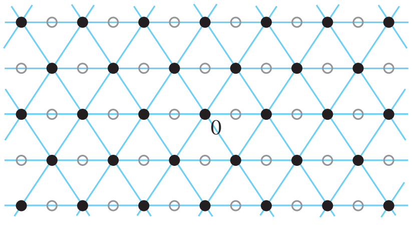
Proposition 7.19. *An ideal L in R_Δ is primitive if and only if there exists an ideal M in R_Δ such that LM is a principal ideal.*

Proof: The forward implication follows from Proposition 7.18 by choosing $M = \overline{L}$. For the opposite implication, suppose that $LM = (\alpha)$, and let β be an element of $\mathbb{Q}(\sqrt{\Delta})$ such that βL is contained in L. Then $\beta(\alpha) = \beta LM$ is contained in $LM = (\alpha)$. In particular this says that $\beta\alpha$ is in (α) so $\beta\alpha = \gamma\alpha$ for some element γ of R_Δ. Since α is nonzero this implies $\beta = \gamma$ and so β is an element of R_Δ. This shows that L is primitive. □

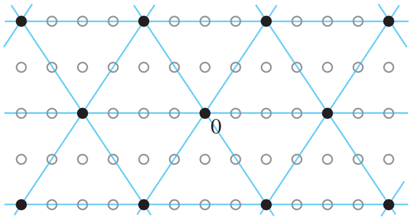
Proposition 7.20. *If L and M are primitive ideals in R_Δ then $N(LM) = N(L)N(M)$.*

Proof: If L and M are primitive then so is LM by Proposition 7.19 since the product of two principal ideals is principal. Thus we have $L\overline{L} = (N(L))$, $M\overline{M} = (N(M))$, and $LM\overline{LM} = (N(LM))$. Since $LM\overline{LM} = L\overline{L}M\overline{M}$ we therefore have $(N(LM)) = (N(L))(N(M)) = (N(L)N(M))$. This implies $N(LM) = N(L)N(M)$ since for an ideal (n) with $n > 0$, the smallest positive integer in (n) is n, as is evident from the fact that (n) is the lattice $L(n, n\tau)$ for $R_\Delta = \mathbb{Z}[\tau]$. □

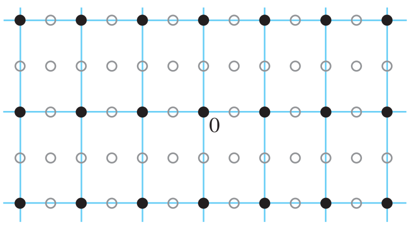
Interestingly enough, the formula $L\overline{L} = (N(L))$ and the multiplicative property $N(LM) = N(L)N(M)$ for primitive ideals can fail to hold for nonprimitive ideals. A simple example is provided by the ideal $L = (2, 1 + \sqrt{-3})$ in $\mathbb{Z}[\sqrt{-3}]$ which we considered earlier in this section as an example of a nonprimitive ideal corresponding to the nonprimitive form $2x^2 + 2xy + 2y^2$ of discriminant -12. Here $L = \overline{L}$ and the ideal $L^2 = L\overline{L}$ is $(2, 1 + \sqrt{-3})(2, 1 - \sqrt{-3}) = (4, 2 + 2\sqrt{-3}, 2 - 2\sqrt{-3}, 4)$. Of these four generators we can obviously drop the repeated 4, and we can also omit the third generator which is expressible in terms of the first two generators as the first generator minus the second generator. We are left with the ideal $(4, 2 + 2\sqrt{-3}) = 2(2, 1 + \sqrt{-3})$. Thus we have $L^2 = L\overline{L} = 2L$. Looking at the figure, we see that $N(L) = 2$ and hence $N(2L) = 2^2 N(L) = 8$ so $N(L^2) \neq N(L)^2$. This shows that $N(LM)$ need not equal $N(L)N(M)$ for nonprimitive ideals. Also we see from the figure that $L\overline{L} \neq (N(L))$ since $2L \neq (2)$. In fact $L\overline{L}$ is not even a principal ideal since $2L$ is a lattice of equilateral triangles while principal ideals have the same shape as the rectangular lattice $\mathbb{Z}[\sqrt{-3}]$.



L



$L^2 = 2L$



(2)

Now at last we come to the construction of the class group $CG(\Delta)$. As a set, $CG(\Delta)$ is the set of proper equivalence classes of primitive forms of discriminant Δ. The group structure will come from the one-to-one correspondence in Theorem 7.15 and Proposition 7.16 between proper equivalence classes of primitive forms of discriminant Δ and strict equivalence classes of primitive ideals in R_Δ. Thus it will suffice to define a group structure on the set of strict equivalence classes of primitive ideals in R_Δ.

We will use the notation $[L]$ to denote the strict equivalence class of a primitive ideal L in R_Δ and we will view elements of $CG(\Delta)$ as such classes $[L]$. The multiplication operation in $CG(\Delta)$ is defined by taking products of ideals, so we set $[L][M] = [LM]$. To check that this is well defined we need to see that choosing different elements $L' = \alpha L$ and $M' = \beta M$ of the classes $[L]$ and $[M]$ does not affect $[LM]$. This is true because $L'M' = \alpha\beta LM$ so $[LM] = [L'M']$. Here we are dealing with strict equivalence classes of ideals so we are assuming $N(\alpha) > 0$ and $N(\beta) > 0$ and hence $N(\alpha\beta) > 0$. (As always this condition is automatic when Δ is negative.)

Proposition 7.21. *$CG(\Delta)$ is a commutative group with respect to the multiplication $[L][M] = [LM]$.*

Proof: The commutativity property $[L][M] = [M][L]$ is easy since this amounts to saying $[LM] = [ML]$, which holds since multiplication of ideals is commutative, $LM = ML$, because multiplication in R_Δ is commutative.

To have a group there are three things to check. First, the multiplication should be associative, so $([L][M])[N] = [L]([M][N])$. By the definition of the product in $CG(\Delta)$ this is equivalent to saying $[LM][N] = [L][MN]$ which in turn means $[(LM)N] = [L(MN)]$, so it suffices to check that multiplication of ideals is associative, $(LM)N = L(MN)$. The claim is that each of these two products consists of all the finite sums $\sum_i \alpha_i\beta_i\gamma_i$ with α_i, β_i, and γ_i elements of L, M, and N respectively. Every such sum is in both $(LM)N$ and $L(MN)$ since each term $\alpha_i\beta_i\gamma_i$ is in both of the ideals $(LM)N$ and $L(MN)$. Conversely, each element of $(LM)N$ is a sum of terms $(\sum_j \alpha_j\beta_j)\gamma$ so it can be written as a sum $\sum_i \alpha_i\beta_i\gamma_i$, and similarly each element of $L(MN)$ can be written as a sum $\sum_i \alpha_i\beta_i\gamma_i$. Thus we have $(LM)N = L(MN)$.

Next, a group must have an identity element, and the class $[(1)]$ of the ideal $(1) = R_\Delta$ obviously serves this purpose since $(1)L = L$ for all ideals L, hence $[(1)][L] = [L]$. There is no need to check that $[L][(1)] = [L]$ as one would have to do for a noncommutative group since we have already observed that multiplication in $CG(\Delta)$ is commutative.

The last thing to check is that each element of $CG(\Delta)$ has a multiplicative inverse, and this is where we use the condition that we are considering only primitive ideals in the definition of $CG(\Delta)$. As we showed in Proposition 7.18, each primitive ideal L satisfies $L\overline{L} = (n)$ where the integer n is the norm of L. Then we have $[L][\overline{L}] = [(n)] = [(1)]$ where this last equality holds since the ideals (n) and (1) are strictly equivalent, the norm of n being n^2, a positive integer. Thus the multiplicative inverse of $[L]$ is $[\overline{L}]$. Again commutativity of the multiplication means that we do not have to check that we have an inverse for multiplication both on the left and on the right. □

There is a variant of the class group in which the relation of strict equivalence of ideals is modified by deleting the word “strict”, so an ideal L is considered equivalent to αL for all nonzero elements α of R_Δ without the condition that $N(\alpha) > 0$. The preceding proof that $CG(\Delta)$ is a group applies equally well in this setting by just omitting any mention of norms being positive. Sometimes the resulting group is called the class group while $CG(\Delta)$ is called the strict class group or narrow class group. However, for studying quadratic forms the better notion is strict equivalence, which is why we are using this for the class group $CG(\Delta)$.

Unique Factorization of Ideals

In this section we will be restricting our attention exclusively to discriminants Δ that are fundamental discriminants, so all forms will be primitive and hence all ideals in R_Δ will also be primitive. This means that we will be able to make free use of the formulas $N(LM) = N(L)N(M)$ and $L\overline{L} = (N(L))$.

Our main goal in this section is to show that all ideals in R_Δ, with the trivial exception of R_Δ itself, have unique factorizations as products of prime ideals, where an ideal P different from R_Δ is called *prime* if whenever it is expressed as a product LM of two ideals in R_Δ, either L or M must equal R_Δ, so the factorization becomes the trivial factorization $P = R_\Delta P$ that every ideal has. Note that R_Δ, considered as an ideal in itself, satisfies this condition but we do not call R_Δ a prime ideal, just as the number 1 is not considered a prime number.

For an element α of R_Δ we know that α is prime if its norm $N(\alpha)$ is a prime in $\mathbb{Z}$ (though the converse is not always true). The analog for ideals also holds: If the norm $N(P)$ of an ideal P is a prime in $\mathbb{Z}$ then P is a prime ideal. The argument is similar: Suppose $P = LM$. Then $N(P) = N(L)N(M)$. If we assume $N(P)$ is prime in $\mathbb{Z}$, then since both $N(L)$ and $N(M)$ are positive integers, one of them must equal 1. But the only ideal of norm 1 is R_Δ since having norm 1 means that a single untranslated copy of the ideal covers all of R_Δ, making the ideal equal R_Δ. Thus we conclude that either L or M is R_Δ and so P is a prime ideal.

Let us now work through an example to see how prime factorization of ideals can resolve the problem of nonunique prime factorization of elements. The example will be one we looked at earlier in the chapter, the factorizations

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

in $R_\Delta = \mathbb{Z}[\sqrt{-5}]$ with $\Delta = -20$. We saw that 2, 3, and $1 \pm \sqrt{-5}$ were prime elements of $\mathbb{Z}[\sqrt{-5}]$, and the two factorizations do not differ just by units since the only units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1.

The transition from elements of R_Δ to ideals in R_Δ is achieved by associating to each nonzero element α in R_Δ the principal ideal (α). Under this transition multiplication of elements corresponds to multiplication of ideals since $(\alpha\beta) = (\alpha)(\beta)$.

Another basic observation is that $(\alpha) = (\beta)$ if and only if α and β differ only by multiplication by a unit. For if $\beta = \varepsilon\alpha$ for some unit ε then (ε) contains $\varepsilon\varepsilon^{-1} = 1$ so $(\varepsilon) = R_\Delta$ hence $(\beta) = (\varepsilon\alpha) = (\varepsilon)(\alpha) = (\alpha)$. Conversely, if $(\alpha) = (\beta)$ then since β is in (α) we have $\beta = \varepsilon\alpha$ for some $\varepsilon \in R_\Delta$ and similarly we have $\alpha = \eta\beta$ for some $\eta \in R_\Delta$. Thus $\alpha = \eta\beta = \eta\varepsilon\alpha$ hence $\eta\varepsilon = 1$ so ε and η are units, showing that α and β differ just by a unit.

There is also a simple relation between the norm $N((\alpha))$ of the ideal (α) and the norm $N(\alpha)$ of the element α, namely $N((\alpha)) = |N(\alpha)|$, where the absolute value is needed since norms of ideals are always positive. We can derive this formula from the formula $L\overline{L} = (N(L))$, so in particular we have $(\alpha)(\overline{\alpha}) = (N((\alpha)))$. The left side of this equation equals $(\alpha\overline{\alpha})$ which is $(N(\alpha))$. Thus the two principal ideals $(N((\alpha)))$ and $(N(\alpha))$ are equal so the two integers $N((\alpha))$ and $N(\alpha)$ differ only by a unit. If an integer times a unit in R_Δ is an integer, that unit must also be an integer. The only integer units are ±1, so we conclude that $N((\alpha)) = |N(\alpha)|$.

Returning to our example, we now have two different factorizations of the ideal (6) as a product of two ideals:

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

We would like to determine whether the ideals (2), (3), and $(1 \pm \sqrt{-5})$ are prime, and if they are not, factor them into prime ideals. One way the ideal (2) might factor is as $P\overline{P} = (N(P)) = (2)$ if there is an ideal P in $\mathbb{Z}[\sqrt{-5}]$ of norm 2. Since 2 is prime, P would then be a prime ideal, as would $\overline{P}$, so we would have a prime factorization $(2) = P\overline{P}$.

To find an ideal P of norm 2 consider a reduced basis $a, b + c\sqrt{-5}$ for P. The norm of the lattice $L(a, b + c\sqrt{-5})$ is ac, and we must have $b < a$ so the only possibilities for the lattice are $L(2, \sqrt{-5})$, $L(2, 1 + \sqrt{-5})$, and $L(1, 2\sqrt{-5})$. The last of these is ruled out since it contains 1 hence the ideal P would be the whole ring $\mathbb{Z}[\sqrt{-5}]$. The first lattice $L(2, \sqrt{-5})$ is not an ideal since it is not taken to itself by multiplication by $\sqrt{-5}$ since $\sqrt{-5}\sqrt{-5} = -5$ is not in the lattice $L(2, \sqrt{-5})$. The remaining lattice $L(2, 1 + \sqrt{-5})$ however is an ideal since $\sqrt{-5} \cdot 2 = -2 + 2(1 + \sqrt{-5})$ and $\sqrt{-5} \cdot (1 + \sqrt{-5}) = \sqrt{-5} - 5 = -3 \cdot 2 + (1 + \sqrt{-5})$.

Thus we have factored the ideal (2) as $P\overline{P}$ for the prime ideal $P = (2, 1 + \sqrt{-5})$. In a similar way one can discover that (3) factors as $Q\overline{Q}$ for the ideal $Q = (3, 1 + \sqrt{-5})$ of norm 3, so Q is also prime. (Later we will find a more efficient way of obtaining these factorizations.) As a result we have a prime factorization of the ideal (6) as $(P\overline{P})(Q\overline{Q})$. These four factors could also be grouped as $(PQ)(\overline{PQ})$. We have $PQ = (2, 1 + \sqrt{-5})(3, 1 + \sqrt{-5}) = (6, 2 + 2\sqrt{-5}, 3 + 3\sqrt{-5}, -4 + 2\sqrt{-5})$ which simplifies to $(6, 1 + \sqrt{-5})$. In fact 6 is in the ideal $(1 + \sqrt{-5})$ since $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$ and we coclde that $PQ = (1 + \sqrt{-5})$. Taking conjugates we also have $\overline{PQ} = (1 - \sqrt{-5})$.

The conclusion of all this is that the two factorizations of (6) as $(2)(3)$ and $(1 +$

$\sqrt{-5})(1-\sqrt{-5})$ are simply two ways of grouping the four prime factors as $(P\overline{P})(Q\overline{Q})$ and as $(PQ)(\overline{PQ})$. One might wonder whether the grouping $(P\overline{Q})(\overline{P}Q)$ would give a third factorization of (6) but it happens that $P = \overline{P}$ so this grouping gives nothing new.

It will be helpful to have a criterion for when one ideal L in R_Δ divides another ideal M, meaning that $M = LK$ for some ideal K. For individual elements of R_Δ it is easy to tell when one element divides another since α divides β exactly when the quotient β/α lies in R_Δ. For ideals, however, the criterion is rather different:

Proposition 7.22. *An ideal L in R_Δ divides an ideal M if and only if L contains M.*

One can remember this as 'to divide is to contain' (which sounds like some sort of competitive strategy). At first glance this result may seem a little puzzling since for ordinary numbers the divisors of a number n, apart from n itself, are smaller than n while for ideals the divisors are larger, where 'larger' for sets means that one set contains the other.

The proposition gives some insight into the choice of the ideals P and Q in the preceding example where we factored the ideal (6) in $\mathbb{Z}[\sqrt{-5}]$ as $(P\overline{P})(Q\overline{Q})$ and as $(PQ)(\overline{PQ})$. Since we want $P\overline{P} = (2)$ and $PQ = (1+\sqrt{-5})$, this means that P should divide both (2) and $(1+\sqrt{-5})$. By the proposition this is the same as saying that P should contain both (2) and $(1+\sqrt{-5})$. An obvious ideal with this property is the ideal $(2, 1+\sqrt{-5})$. Similarly one would be led to try $Q = (3, 1+\sqrt{-5})$. Then one could check that these choices for P and Q actually work.

Before proving the proposition let us derive a fact which will be used in the proof, a cancellation property of multiplication of ideals: If $LM_1 = LM_2$ then $M_1 = M_2$. To see this, first multiply the equation $LM_1 = LM_2$ by $\overline{L}$ to get $\overline{L}LM_1 = \overline{L}LM_2$. Since $\overline{L}L = (n)$ for $n = N(L)$, a positive integer, we then have $(n)M_1 = (n)M_2$. The ideal $(n)M_1$ is just a rescaling of M_1 by a factor of n since if we write $M_1 = (\alpha, \beta)$ then $(n)M_1 = (n\alpha, n\beta)$. Similarly $(n)M_2$ is a rescaling of M_2 by the same factor n. Since $(n)M_1 = (n)M_2$ these rescalings are equal, so after rescaling again by the factor $1/n$ we conclude that $M_1 = M_2$.

Now let us prove the proposition.

Proof: Suppose first that L divides M, so $M = LK$ for some ideal K. A typical element of LK is a sum $\sum_i \alpha_i\beta_i$ with $\alpha_i \in L$ and $\beta_i \in K$. Since L is an ideal, each term $\alpha_i\beta_i$ is then in L and hence so is their sum. This shows that L contains $LK = M$.

For the converse, suppose L contains M. Then $L\overline{L}$ contains $M\overline{L}$. Since $L\overline{L} = (n)$ for $n = N(L)$ this says that (n) contains $M\overline{L}$, so every element of $M\overline{L}$ is a multiple of n by some element of R_Δ. This means that if we write $M\overline{L} = (\alpha, \beta)$ then we can define an ideal K by letting $K = (\alpha/n, \beta/n)$.

Now we have $(n)K = (n)(\alpha/n, \beta/n) = (\alpha, \beta) = M\overline{L}$. Multiplying by L we then have $(n)KL = M\overline{L}L = M(n)$. Canceling the factor (n) gives the equation $KL = M$, which says that L divides M, finishing the proof of the converse. □

When we proved unique prime factorization for $\mathbb{Z}$ and those rings R_Δ which have a Euclidean algorithm, a key step was showing that if a prime p divides a product ab then p must divide either a or b. Now we prove the corresponding fact for ideals:

Lemma 7.23. *If a prime ideal P divides a product LM of two ideals, then P must divide either L or M.*

Proof: An equivalent statement is that if P divides LM but not L, then P divides M, and this is what we will prove. To do this, consider the set $P+L$ of all sums $\alpha+\beta$ of elements $\alpha \in P$ and $\beta \in L$. This set $P+L$ is an ideal since if $P=(\alpha_1,\alpha_2)$ and $L=(\beta_1,\beta_2)$ then $P+L=(\alpha_1,\alpha_2,\beta_1,\beta_2)$. The ideal $P+L$ is strictly larger than P since our assumption that P does not divide L means that P does not contain L, so any element of L not in P is in $P+L$ but not P. Thus $P+L$ contains P, hence divides P, but is not equal to P so since P is prime we must have $P+L=R_\Delta$.

In particular $P+L$ contains 1 so we can write $1=\alpha+\beta$ for some $\alpha\in P$ and $\beta \in L$. For an arbitrary element $\gamma \in M$ we then have $\gamma=\alpha\gamma+\beta\gamma$. The term $\alpha\gamma$ is in P since α is in P and P is an ideal. The term $\beta\gamma$ is in LM since β is in L and γ is in M. We assume P divides LM so P contains LM and it follows that $\beta\gamma$ is in P. Thus both terms on the right side of the equation $\gamma=\alpha\gamma+\beta\gamma$ are in P so γ is in P. Since γ was an arbitrary element of M this shows that M is contained in P, or in other words P divides M, which is what we wanted to prove. □

Now we can prove our main result:

Theorem 7.24. *Every ideal in R_Δ other than R_Δ itself factors as a product of prime ideals, and this factorization is unique up to the order of the factors.*

Proof: We first show the existence of a prime factorization for each ideal $L \neq R_\Delta$. If L is prime itself there is nothing to prove, so suppose L is not prime, hence there is a factorization $L=KM$ with neither factor equal to R_Δ. Taking norms, we have $N(L)=N(K)N(M)$. Both $N(K)$ and $N(M)$ are greater than 1 since R_Δ is the only ideal of norm 1. Hence $N(K)<N(L)$ and $N(M)<N(L)$. By induction on the norm, both K and M have prime factorizations, hence so does $L=KM$. We can start the induction with the case $N(L)=2$, a prime, hence L is prime. (The case $N(L)=1$ does not arise since $L\neq R_\Delta$.)

For the uniqueness, suppose an ideal L has prime factorizations $P_1\cdots P_k$ and $Q_1\cdots Q_l$. We can assume $k\le l$ by a notational change if necessary. The prime ideal P_1 divides the product $Q_1(Q_2\cdots Q_l)$ so by the preceding lemma it must divide either Q_1 or $Q_2\cdots Q_l$. In the latter case the same reasoning shows it must divide either Q_2 or $Q_3\cdots Q_l$. Repeating this argument enough times we eventually deduce that P_1 must divide some Q_i, and after permuting the factors of $Q_1\cdots Q_l$ we can assume that P_1 divides Q_1. When one prime ideal divides another prime ideal they must be equal. (Proof: If P divides Q then $Q = PM$ for some M, but Q being prime implies either $P = R_\Delta$, which is impossible if P is prime, or $M = R_\Delta$, hence $P = Q$ as claimed.)

Once we have $P_1 = Q_1$ we can cancel this common factor of $P_1 \cdots P_k$ and $Q_1 \cdots Q_l$ to get $P_2 \cdots P_k = Q_2 \cdots Q_l$. Repeating this process often enough we eventually get, after suitably permuting the Q_i's, that $P_1 = Q_1$, $P_2 = Q_2$, $\cdots$, $P_{k-1} = Q_{k-1}$, and $P_k = Q_k \cdots Q_l$. Since P_k is prime, as are the Q_i's, the equation $P_k = Q_k \cdots Q_l$ can have only one term on the right side, so $k = l$ and $P_k = Q_k$. This finishes the proof of the uniqueness of prime factorizations of ideals. □

Corollary 7.25. *If the class number for the fundamental discriminant Δ is one, then all elements of R_Δ other than units and 0 have unique factorizations as products of prime elements, where the uniqueness is up to order and multiplication by units.*

Proof: If the class number is one then all ideals are principal. The result then follows immediately from the theorem and the fact that principal ideals in R_Δ correspond exactly to nonzero elements of R_Δ up to multiplication by units, as described earlier in this section. □

Proposition 7.26. *If P is a prime ideal in R_Δ then P contains a unique prime positive integer p, and either $P = (p)$ with $N(P) = p^2$ or $P\overline{P} = (p)$ with $N(P) = p$.*

Proof: We have $P\overline{P} = (N(L))$. Factor the positive integer $N(P)$ as a product $p_1 \cdots p_k$ of primes p_i, so $P\overline{P} = (p_1)\cdots(p_k)$. Thus P divides $(p_1)\cdots(p_k)$ and since P is prime it must divide one of the factors, say (p_i). This means P contains (p_i), so in particular P contains p_i. Let $p_i = p$. If P contained another prime q it would have to contain 1 since p and q are coprime and hence $mp + nq = 1$ for some integers m and n. Thus we would have $P = R_\Delta$ which is impossible since P is a prime ideal. This shows that p is the only prime positive integer in P.

Since P divides (p) we have $PQ = (p)$ for some ideal Q. Then $N(P)N(Q) = N((p)) = p^2$, which implies that either $N(P) = p$ or $N(P) = p^2$. In the first case we would have $P\overline{P} = (N(P)) = (p)$ and in the second case we would have $N(Q) = 1$ and hence $Q = R_\Delta$ so $P = (p)$. □

Our next proposition will give more information on how an ideal (p) factors into prime ideals in R_Δ when p is an odd prime. The result will be stated in terms of the integer d which is defined to equal Δ when $\Delta \equiv 1$ mod 4 and $\Delta/4$ when $\Delta \equiv 0$ mod 4. Since we are assuming that Δ is a fundamental discriminant it follows that d is a product of distinct primes. (Otherwise, if d was divisible by 4 then it would be a discriminant and $\Delta = 4d$ would not be fundamental, while if d was divisible by q^2 for some odd prime q then we would have $q^2 \equiv 1$ mod 4 and hence $\Delta \equiv \Delta/q^2$ mod 4 so Δ/q^2 would be a discriminant, making Δ again nonfundamental.)

Proposition 7.27. *Let p be an odd prime. Then:*
(a) If p does not divide d and the Legendre symbol $\left(\frac{d}{p}\right) = +1$ then $(p) = P\overline{P}$ with P a prime ideal in R_Δ and $P \neq \overline{P}$. Specifically, $P = (p, b + \sqrt{d})$ and $\overline{P} = (p, b - \sqrt{d})$ or vice versa, where $b^2 \equiv d \bmod p$.
(b) If p divides d then $(p) = P^2$ with P prime. Specifically, $P = (p, \sqrt{d})$.
(c) If p does not divide d and $\left(\frac{d}{p}\right) = -1$ then (p) is a prime ideal in R_Δ.

Proof: For part (a), since we assume $\left(\frac{d}{p}\right) = +1$ there exists an integer b with $b^2 \equiv d$ mod p. Here p does not divide b since we assume it does not divide d. Let $P = (p, b + \sqrt{d})$. Then $P\overline{P} = (p^2, pb + p\sqrt{d}, pb - p\sqrt{d}, b^2 - d) = p(p, b + \sqrt{d}, b - \sqrt{d}, \frac{b^2-d}{p})$, where the fraction $\frac{b^2-d}{p}$ is an integer since $b^2 \equiv d$ mod p. The ideal $(p, b + \sqrt{d}, b - \sqrt{d}, \frac{b^2-d}{p})$ contains the numbers p and $2b$ which are coprime since p does not divide b and $p \neq 2$. Hence this ideal contains 1 and so equals R_Δ. Thus we have $P\overline{P} = (p)$. In particular this says that $N(P) = p$ so P is prime (as is $\overline{P}$).

If $P = \overline{P}$ then P would contain $b + \sqrt{d}$ and $b - \sqrt{d}$ so it would contain $2b$. It also contains p so by the reasoning in the preceding paragraph we would have $P = R_\Delta$, which is impossible for a prime ideal. Thus $P \neq \overline{P}$, which finishes part (a).

For (b), if p divides d we let $P = (p, \sqrt{d})$, so $\overline{P} = (p, -\sqrt{d}) = P$. We have $P^2 = (p, \sqrt{d})^2 = (p^2, p\sqrt{d}, d) = p(p, \sqrt{d}, \frac{d}{p})$. The ideal $(p, \sqrt{d}, \frac{d}{p})$ contains the integers p and $\frac{d}{p}$ which are coprime since d is a product of distinct primes, hence this ideal is R_Δ and so $P^2 = (p)$. Notice that this proof of (b) also works when $p = 2$.

For (c) we will prove the logically equivalent contrapositive statement that if $(p) = P\overline{P}$ then either p divides d or $\left(\frac{d}{p}\right) = +1$. Let $a, b + c\tau$ be a reduced basis for P. We have $N(P) = ac = p$ so a is either 1 or p, but if $a = 1$ we would have $P = R_\Delta$ so we must have $a = p$ and hence $c = 1$. Thus the second reduced basis element is $\beta = b + \tau$. We have $N(\beta) = \beta\overline{\beta}$ and this lies in P since β does. All the integers in $P = L(p, b + \tau)$ are multiples of p so p divides $N(\beta)$.

We now split the argument into two cases according to whether Δ is 0 or 1 mod 4. If $\Delta \equiv 0$ mod 4 then $d = \Delta/4$ and $\tau = \sqrt{d}$. Since p divides $N(\beta) = (b + \sqrt{d}) \cdot (b - \sqrt{d}) = b^2 - d$ we must have $b^2 \equiv d$ mod p. Thus either p divides d or $\left(\frac{d}{p}\right) = +1$, which is what we wanted to prove. In the opposite case $\Delta \equiv 1$ mod 4 we have $\Delta = d$ and $\tau = \frac{1+\sqrt{d}}{2}$. Now p divides $N(\beta) = (b + \tau) \cdot (b + \overline{\tau}) = b^2 + b(\tau + \overline{\tau}) + \tau\overline{\tau} = b^2 + b + \frac{1-d}{4}$. Multiplying this last expression by 4 we see that p also divides $4b^2 + 4b + 1 - d$, hence $(2b + 1)^2 \equiv d$ mod p. Thus d is a square mod p so again either p divides d or $\left(\frac{d}{p}\right) = +1$. □

There is an alternative argument for part (c) using quadratic forms. If $(p) = P\overline{P}$ then p is in P and the value that the quadratic form Q_P associated to P takes on this element of P is $Q_P(p) = N(p)/N(P) = p^2/p = p$. Thus p is representable by a form of discriminant Δ so either p divides Δ or $\left(\frac{\Delta}{p}\right) = +1$, by Lemma 6.5. Since Δ

is either d or $4d$ and p is odd, this is equivalent to saying that either p divides d or $\left(\frac{d}{p}\right) = +1$.

In the analog of the preceding proposition for the prime $p = 2$ it turns out that the answer depends on the value of d mod 8. Since d is not divisible by 4, its value mod 8 cannot be 0 or 4. The remaining six possibilities are enumerated below:

Proposition 7.28. *The factorization of* (2) *into prime ideals in* R_Δ *is given by:*
(a) $(2) = P\overline{P}$ *for* $P = (2, \frac{1+\sqrt{d}}{2})$ *if* $d \equiv 1$ *mod* 8*, and in this case* $P \neq \overline{P}$*.*
(b) $(2) = P^2$ *for* $P = (2, \sqrt{d})$ *if* $d \equiv 2$ *or* 6 *mod* 8*.*
(c) $(2) = P^2$ *for* $P = (2, 1 + \sqrt{d})$ *if* $d \equiv 3$ *or* 7 *mod* 8*.*
(d) (2) *is prime in* R_Δ *if* $d \equiv 5$ *mod* 8*.*

Notice that if Δ is odd then $\Delta = d$ and we are in the cases (a) or (d) above, while if Δ is even then $\Delta = 4d$ and we are in the cases (b) or (c) depending on the parity of d. Thus when (2) factors in R_Δ, the two factors are the same or different depending on whether 2 divides Δ or not. This is exactly the same way that (p) factors when p is an odd prime, as described in Proposition 7.27.

Proof: For (a), note first that Δ is odd so $\frac{1+\sqrt{d}}{2}$ is an element of R_Δ. We have $P\overline{P} = (2, \frac{1+\sqrt{d}}{2})(2, \frac{1-\sqrt{d}}{2}) = (4, 2\frac{1+\sqrt{d}}{2}, 2\frac{1-\sqrt{d}}{2}, \frac{1-d}{4}) = 2(2, \frac{1+\sqrt{d}}{2}, \frac{1-\sqrt{d}}{2}, \frac{1-d}{8})$. Here $\frac{1-d}{8}$ is an integer since we assume $d \equiv 1$ mod 8. The ideal $(2, \frac{1+\sqrt{d}}{2}, \frac{1-\sqrt{d}}{2}, \frac{1-d}{8})$ contains $\frac{1+\sqrt{d}}{2} + \frac{1-\sqrt{d}}{2} = 1$ so it is R_Δ, hence $P\overline{P} = (2)$. If $P = \overline{P}$ then P would contain both $\frac{1+\sqrt{d}}{2}$ and $\frac{1-\sqrt{d}}{2}$ so it would contain their sum 1 and we would have $P = R_\Delta$ which is impossible, so $P \neq \overline{P}$.

In case (b) the number d is even and the proof of part (b) of Proposition 7.27 applies, as noted there.

For (c) we have $d \equiv 3$ mod 4 so we can write $d = 4k + 3$ for some integer k. Then $P^2 = (2, 1 + \sqrt{d})^2 = (4, 2 + 2\sqrt{d}, 1 + d + 2\sqrt{d}) = (4, 2 + 2\sqrt{d}, 4k + 4 + 2\sqrt{d}) = 2(2, 1 + \sqrt{d}, 2k + 2 + \sqrt{d})$. The ideal $(2, 1 + \sqrt{d}, 2k + 2 + \sqrt{d})$ contains 2 so it contains all even integers. In particular it contains $2k + 2$ so we can subtract this from the last generator $2k + 2 + \sqrt{d}$ to see that this ideal contains $\sqrt{d}$. Then from the second generator $1 + \sqrt{d}$ we see that the ideal contains 1, making it all of R_Δ, and we conclude that $P^2 = (2)$.

For (d) we argue by contradiction, so suppose that (2) is not prime. Then $(2) = P\overline{P}$ for some ideal P with $N(P) = 2$. Since P divides (2) it contains (2) and so it contains 2. On this element 2 in P the associated quadratic form Q_P has the value $N(2)/N(P) = 2^2/2 = 2$. Thus there is a form of discriminant Δ that represents 2. From Chapter 6 we know that this implies $\Delta \not\equiv 5$ mod 8. But $\Delta = d$ in part (d) so we have reached the desired contradiction. □

Exercises

1. (a) Show that if α and β are elements of $\mathbb{Z}[\sqrt{D}]$ such that α is a unit times β, then $N(\alpha) = \pm N(\beta)$.

(b) Either prove or give a counterexample to the following statement: If α and β are Gaussian integers with $N(\alpha) = N(\beta)$ then α is a unit times β.

2. Show that a Gaussian integer $x + yi$ with both x and y odd is divisible by $1 + i$ but not by $(1 + i)^2$.

3. There are four different ways to write the number $1105 = 5 \cdot 13 \cdot 17$ as a sum of two squares. Find these four ways using the factorization of 1105 into primes in $\mathbb{Z}[i]$. [Here we are not counting $5^2 + 2^2$ and $2^2 + 5^2$ as different ways of expressing 29 as the sum of two squares. Note that an equation $n = a^2 + b^2$ is equivalent to an equation $n = (a + bi)(a - bi)$.]

4. (a) Find four different units in $\mathbb{Z}[\sqrt{3}]$ that are positive real numbers, and find four that are negative.

(b) Do the same for $\mathbb{Z}[\sqrt{11}]$.

5. Make a list of all the Gaussian primes $x + yi$ with $-7 \le x \le 7$ and $-7 \le y \le 7$. (The only actual work here is to figure out the primes $x + yi$ with $0 \le y \le x \le 7$, then the rest are obtainable from these by symmetry properties.)

6. Factor the following Gaussian integers into primes in $\mathbb{Z}[i]$: $3 + 5i$, $8 - i$, $10 + i$, $5 - 12i$, $35i$, $-35 + 120i$, $253 + 204i$.

7. In this problem we consider $\mathbb{Z}[\sqrt{-2}]$. To simplify notation, let $\omega = \sqrt{-2}$, so elements of $\mathbb{Z}[\omega]$ are sums $x + y\omega$ with $x, y \in \mathbb{Z}$ and with $\omega^2 = -2$. We have $N(x + y\omega) = x^2 + 2y^2 = (x + y\omega)(x - y\omega)$.

(a) Draw the topograph of $x^2 + 2y^2$ including all values less than 70 (by symmetry, it suffices to draw just the upper half of the topograph). Circle the values that are prime (prime in $\mathbb{Z}$, that is). Also label each region with its x/y fraction.

(b) Which primes in $\mathbb{Z}$ factor in $\mathbb{Z}[\omega]$?

(c) Using the information in part (a), list all primes in $\mathbb{Z}[\omega]$ of norm less than 70.

(d) Draw a diagram in the xy-plane showing all elements $x + y\omega$ in $\mathbb{Z}[\omega]$ of norm less than 70 as small dots, with larger dots or squares for the elements that are prime in $\mathbb{Z}[\omega]$. (There is symmetry, so the primes in the first quadrant determine the primes in the other quadrants.)

(e) Show that the only primes $x + y\omega$ in $\mathbb{Z}[\omega]$ with x even are $\pm\omega$. (Your diagram in part (d) should give some evidence that this is true.)

(f) Factor $4 + \omega$ into primes in $\mathbb{Z}[\omega]$.

8. (a) According to Proposition 7.11, unique factorization fails in $\mathbb{Z}[\sqrt{D}]$ when $D = -3$ since the number $D(D - 1) = 12$ has two distinct prime factorizations in $\mathbb{Z}[\sqrt{D}]$. On the other hand, when we enlarge $\mathbb{Z}[\sqrt{-3}]$ to $\mathbb{Z}[\omega]$ for $\omega = \frac{1+\sqrt{-3}}{2}$ unique factorization is restored. Explain how the two prime factorizations of 12 in $\mathbb{Z}[\sqrt{-3}]$ give rise to the same prime factorization in $\mathbb{Z}[\omega]$ (up to units).

(b) Do the same thing for the case $D = -7$.

9. Find a recursive formula for a primitive solution of $x^2 + 7y^2 = 2^k$, showing how a solution for one value of k gives rise to a solution for the next larger value of k.

Bibliography

J. H. CONWAY and R. K. GUY, *The Book of Numbers*, Springer-Verlag, 1996.

— *A delightful potpourri showing off many of the wonders of numbers.*

J. H. CONWAY, *The Sensual Quadratic Form*, MAA, 1997.

— *Where topographs first appeared. Very enjoyable reading.*

H. DAVENPORT, *The Higher Arithmetic*, Cambridge U. Press, fifth ed. 1982 (orig. 1952).

— *A classical and accessible introduction to number theory.*

H. STARK, *An Introduction to Number Theory*, Markham, 1970.

— *A well-written standard textbook by a master of the subject.*

J. STILLWELL, *Numbers and Geometry*, Springer, 1998.

— *A pleasing intermingling of algebra and geometry.*

D. E. FLATH, *Introduction to Number Theory*, Wiley, 1989.

— *One of the few elementary treatments of binary (two-variable) quadratic forms. Unfortunately out of print and somewhat difficult to find.*

H. COHN, *Advanced Number Theory*, Dover, 1980.

— *First published in 1962 under the more fitting title "A Second Course in Number Theory".*

A. WEIL, *Number Theory: An Approach Through History*, Birkhäuser, 1984.

— *A scholarly historical study by one of the 20th century greats.*

J. H. SILVERMAN and J. TATE, *Rational Points on Elliptic Curves*, Springer-Verlag, 1992.

— *The next step after studying quadratic curves.*

J.-P. SERRE, *A Course in Arithmetic*, Springer-Verlag, 1973 (French orig. 1970).

— *A masterful expositor writing at the graduate level, in spite of the title.*

D. A. COX, *Primes of the form $x^2 + ny^2$*, Wiley, 1989.

— *Gives the complete answer to the question of which primes can be written in the form $x^2 + ny^2$. Quite a bit of deep mathematics is involved.*

And finally two historical references:

C. F. GAUSS, *Disquisitiones Arithmeticae*, English trans. Springer-Verlag, 1986 (Latin orig. 1801).

— *The first book ever written about quadratic forms, presenting the author's groundbreaking research.*

A. HURWITZ, Über die Reduktion der binären quadratischen Formen, *Math. Annalen* 45 (1894), 85–117.

— *This article (in German) is where the Farey diagram first appeared.*

Index