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 this 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.

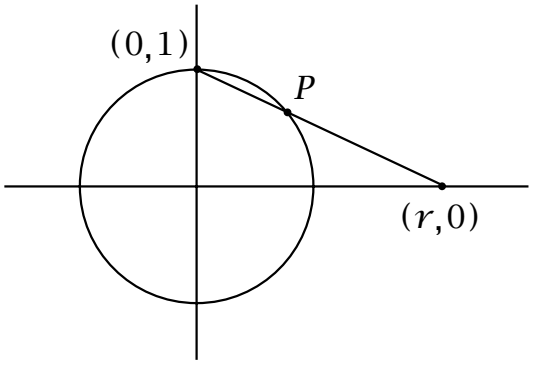
Another case is that n divides a and c. Then n^2 divides a^2 and c^2 so n^2 divides their difference $c^2 - a^2 = b^2$, hence n divides b. In the remaining case that n divides b and c the argument is similar.

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. There are four obvious rational points on the circle we could use to start, the intersections of the circle with the coordinate axes, the points $(\pm1,0)$ and $(0,\pm1)$. It doesn't really matter which one we choose, 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:

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

Plugging $x = \dfrac{2r}{r^2+1}$ into the formula $y = 1 - \frac{x}{r}$, we get

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

Summarizing, we have found that the point P has coordinates

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

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. 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

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

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

This means we obtain Pythagorean triples

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

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 with no common factor and 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.

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 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

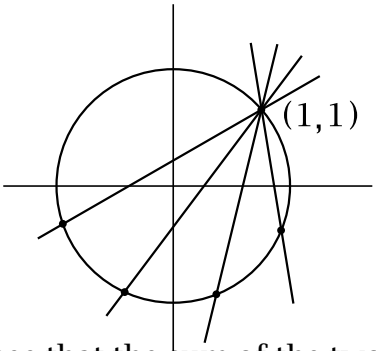
$$\begin{aligned}(a,b,c) &= (2pq, p^2-q^2, p^2+q^2)\\ &= (2(P+Q)(P-Q), (P+Q)^2-(P-Q)^2, (P+Q)^2+(P-Q)^2)\\ &= (2(P^2-Q^2), 4PQ, 2(P^2+Q^2))\\ &= 2(P^2-Q^2, 2PQ, P^2+Q^2)\end{aligned}$$

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.

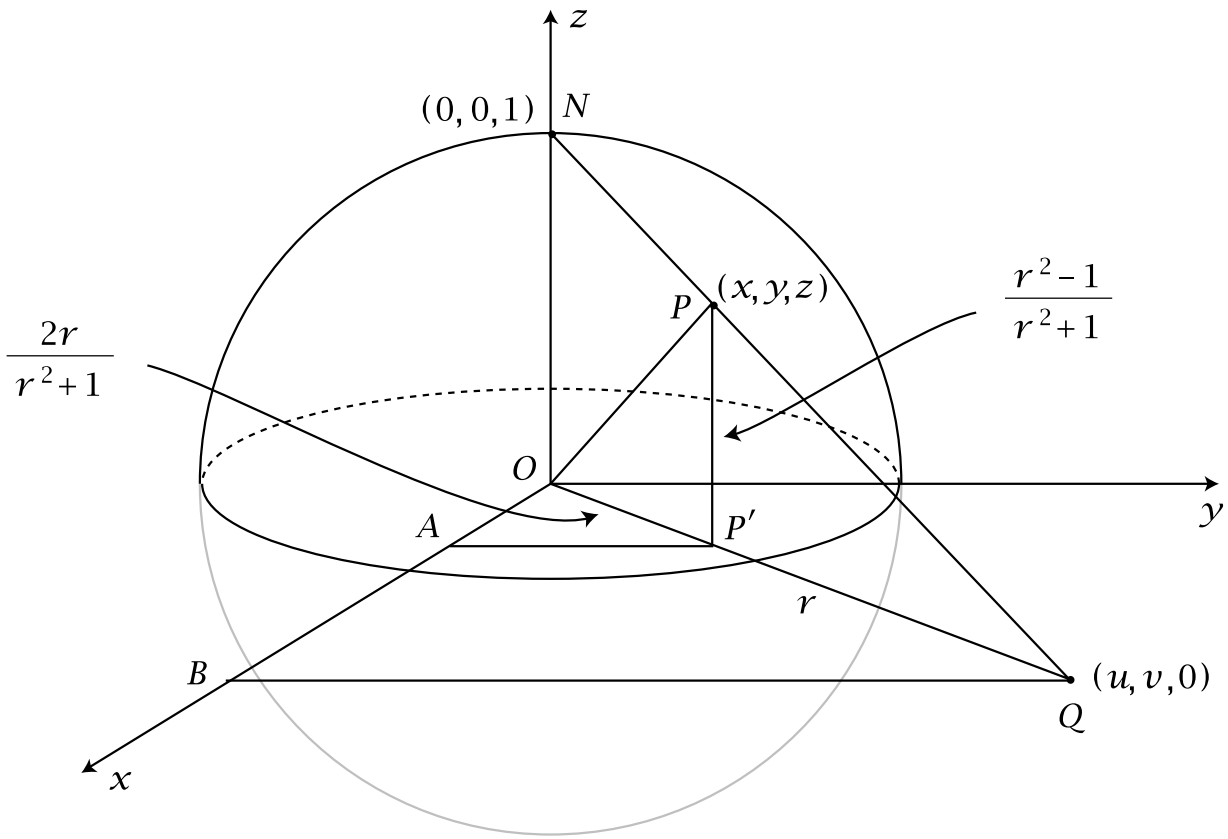
If instead of $x^2 + y^2 = 2$ we consider the circle $x^2 + y^2 = 3$ then there aren't any obvious rational points. In fact this circle contains no rational points at all. For if there were a rational point, this would yield a solution of the equation $a^2 + b^2 = 3c^2$ by integers a, b, and c. We can 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. In theory, an equation could have solutions modulo n for every number n and still have no actual integer solution, and there are cases where this actually happens.

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). We want to find formulas expressing x, y, and z in terms of u and v.



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 all over on 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 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 approach 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 numbers. 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 Chapter 2, 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 Pythagorean triples (a,b,c). We certainly can't realize the number 1 since this would say $a^2 + 1 = c^2$ or

$1 + b^2 = c^2$ but 1 is not the difference between the squares of any two positive integers. For 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 triples are the numbers not congruent to 2 modulo 4. This is indeed true, and can be proved as follows. First note that $2pq$ is even and $p^2 - q^2$ is odd (otherwise both a and b would be even, violating primitivity). Every odd number bigger than 1 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. Note that taking $p = k+1$ and $q = k$ does yield 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 of the form $2pq$, and by taking $q = 1$ we realize any even number $2p$. However, to have a primitive triple we have to have p even since p must have opposite parity from q which is 1. Thus we realize the numbers $a = 4k$ by primitive triples but not the numbers $a = 4k + 2$. This is what we claimed was true. To finish the story for a and b, note that a number $a = 4k + 2$ which can't be realized by a primitive triple can be realized by a nonprimitive triple, at least if $k \geq 1$, since we know we can realize the odd number $2k + 1$ if $k \geq 1$, and by doubling this we realize $4k + 2$. Summarizing this discussion, all numbers greater than 2 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 2 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 have to 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 Chapter 2 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*. 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 Chapter 2. 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:

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

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 3, in particular explaining why the derivation of the formulas above is valid.

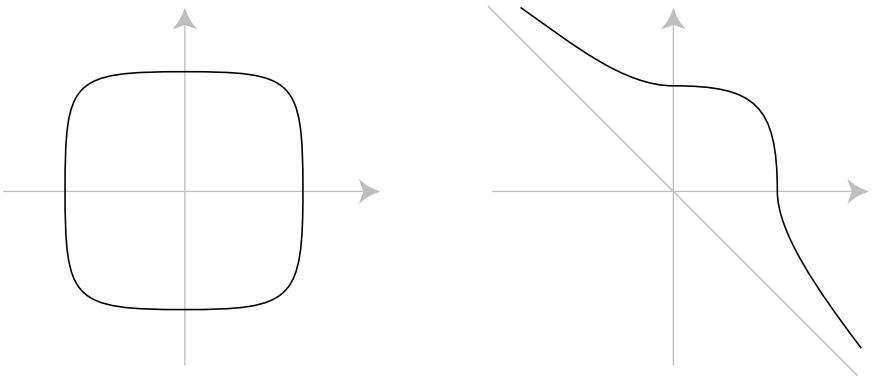
Diophantine Equations

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.

Just as finding integer solutions of $x^2 + y^2 = z^2$ is equivalent to finding rational points on the circle $x^2 + y^2 = 1$, so 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 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. Show that there are no Pythagorean triples (a, b, c) with a being a positive integer multiple of b, or vice versa. ("Show" means "Prove", that is, give a logical argument why the statement is true.)

3. (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.
(c) Find a value of n for which the equation $x^2 - y^2 = n$ has at least 100 different positive integer solutions.

4. Show that there are only a finite number of Pythagorean triples (a, b, c) with a, b, or c equal to a given number n. (Part of the previous problem may be useful.)

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

6. 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.

7. 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.)

8. Find a rational point on the sphere $x^2 + y^2 + z^2 = 1$ whose x, y, and z coordinates are nearly equal. (You can decide what "nearly equal" means, but a point like $(\frac{2}{3}, \frac{2}{3}, \frac{1}{3})$ doesn't qualify.)

9. (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 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.

10. (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?

11. (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 Pythagorean triples (a,b,c) with a and b differing by 3.

12. 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.)