Chapter 2

Pythagorean Triples

The Pythagorean Theorem, that “beloved” formula of all high school geometry students, says that the sum of the squares of the sides of a right triangle equals the square of the hypotenuse. In symbols,

$$a^2 + b^2 = c^2$$

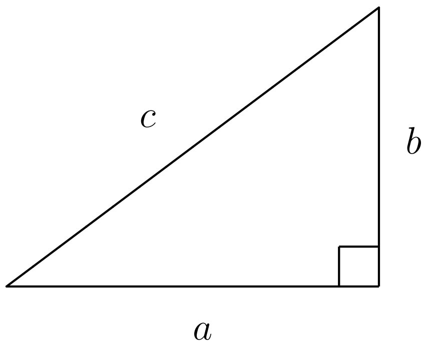
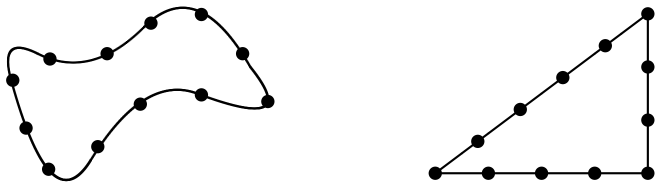


Figure 2.1: A Pythagorean Triangle

Since we’re interested in number theory, that is, the theory of the natural numbers, we will ask whether there are any Pythagorean triangles all of whose sides are natural numbers. There are many such triangles. The most famous has sides 3, 4, and 5. Here are the first few examples:

$$3^2 + 4^2 = 5^2, \quad 5^2 + 12^2 = 13^2, \quad 8^2 + 15^2 = 17^2, \quad 28^2 + 45^2 = 53^2.$$

The study of these *Pythagorean triples* began long before the time of Pythagoras. There are Babylonian tablets that contain lists of such triples, including quite large ones, indicating that the Babylonians probably had a systematic method for producing them. Pythagorean triples were also used in ancient Egypt. For example, a rough-and-ready way to produce a right angle is to take a piece of string, mark it into 12 equal segments, tie it into a loop, and hold it taut in the form of a 3-4-5 triangle, as illustrated in Figure 2.2. This provides an inexpensive right angle tool for use on small construction projects (such as marking property boundaries or building pyramids). Even more amazing is the fact that the Babylonians created tables of quite large Pythagorean triples, which they may have used as primitive trigonometric tables.



String with 12 knots String pulled taut

Figure 2.2: Using a knotted string to create a right triangle

The Babylonians and Egyptians had practical reasons for studying Pythagorean triples. Do such practical reasons still exist? For this particular problem, the answer is “probably not.” However, there is at least one good reason to study Pythagorean triples, and it’s the same reason why it is worthwhile studying the art of Rembrandt and the music of Beethoven. There is a beauty to the ways in which numbers interact with one another, just as there is a beauty in the composition of a painting or a symphony. To appreciate this beauty, one has to be willing to expend a certain amount of mental energy. But the end result is well worth the effort. Our goal in this book is to understand and appreciate some truly beautiful mathematics, to learn how this mathematics was discovered and proved, and maybe even to make some original contributions of our own.

Enough blathering, you are undoubtedly thinking. Let’s get to the real stuff. Our first naive question is whether there are infinitely many *Pythagorean triples*, that is triples of natural numbers (a, b, c) satisfying the equation $a^2 + b^2 = c^2$. The answer is “YES” for a very silly reason. If we take a Pythagorean triple (a, b, c) and multiply it by some other number d, then we obtain a new Pythagorean triple (da, db, dc). This is true because

$$(da)^2 + (db)^2 = d^2(a^2 + b^2) = d^2c^2 = (dc)^2.$$

Clearly these new Pythagorean triples are not very interesting. So we will concentrate our attention on triples with no common factors. We will even give them a name:

> A *primitive Pythagorean triple* (or PPT for short) is a triple of numbers (a, b, c) so that a, b, and c have no common factors[1] and satisfy
>
> $$a^2 + b^2 = c^2.$$

Recall our checklist from Chapter 1. The first step is to accumulate some data. I used a computer to substitute in values for a and b and checked if $a^2 + b^2$ is a square. Here are some primitive Pythagorean triples that I found:

$$\begin{array}{llll}(3,4,5), & (5,12,13), & (8,15,17), & (7,24,25),\\ (20,21,29), & (9,40,41), & (12,35,37), & (11,60,61),\\ (28,45,53), & (33,56,65), & (16,63,65). & \end{array}$$

A few conclusions can easily be drawn even from such a short list. For example, it certainly looks like one of a and b is odd and the other even. It also seems that c is always odd.

It's not hard to prove that these conjectures are correct. First, if a and b are both even, then c would also be even. This means that a, b, and c would have a common factor of 2, so the triple would not be primitive. Next, suppose that a and b are both odd, which means that c would have to be even. This means that there are numbers x, y, and z so that

$$a = 2x + 1, \qquad b = 2y + 1, \qquad \text{and} \qquad c = 2z.$$

We can substitute these into the equation $a^2 + b^2 = c^2$ to get

$$\begin{aligned}(2x + 1)^2 + (2y + 1)^2 &= (2z)^2,\\ 4x^2 + 4x + 4y^2 + 4y + 2 &= 4z^2.\end{aligned}$$

Now divide by 2,

$$2x^2 + 2x + 2y^2 + 2y + 1 = 2z^2.$$

This last equation says that an odd number is equal to an even number, which is impossible, so a and b cannot both be odd. Since we've just checked that they cannot both be even and cannot both be odd, it must be true that one is even and

[1] A *common factor* of a, b, and c is a number d so that each of a, b and c is a multiple of d . For example, 3 is a common factor of 30, 42, and 105, since $30 = 3 \cdot 10$, $42 = 3 \cdot 14$, and $105 = 3 \cdot 35$, and indeed it is their largest common factor. On the other hand, the numbers 10, 12, and 15 have no common factor (other than 1). Since our goal in this chapter is to explore some interesting and beautiful number theory without getting bogged down in formalities, we will use common factors and divisibility informally and trust our intuition. In Chapter 5 we will return to these questions and develop the theory of divisibility more carefully.

the other is odd. It's then obvious from the equation $a^2 + b^2 = c^2$ that c is also odd.

We can always switch a and b, so our problem now is to find all solutions in natural numbers to the equation

$$a^2 + b^2 = c^2 \qquad \text{with} \quad \begin{cases} a \text{ odd}, \\ b \text{ even}, \\ a, b, c \text{ having no common factors.} \end{cases}$$

The tools we will use are *factorization* and *divisibility*.

Our first observation is that if (a, b, c) is a primitive Pythagorean triple, then we can factor

$$a^2 = c^2 - b^2 = (c - b)(c + b).$$

Here are a few examples from the list given earlier, where note that we always take a to be odd and b to be even:

$$\begin{aligned} 3^2 &= 5^2 - 4^2 = (5 - 4)(5 + 4) = 1 \cdot 9, \\ 15^2 &= 17^2 - 8^2 = (17 - 8)(17 + 8) = 9 \cdot 25, \\ 35^2 &= 37^2 - 12^2 = (37 - 12)(37 + 12) = 25 \cdot 49, \\ 33^2 &= 65^2 - 56^2 = (65 - 56)(65 + 56) = 9 \cdot 121. \end{aligned}$$

It looks like $c - b$ and $c + b$ are themselves always squares. We check this observation with a couple more examples:

$$\begin{aligned} 21^2 &= 29^2 - 20^2 = (29 - 20)(29 + 20) = 9 \cdot 49, \\ 63^2 &= 65^2 - 16^2 = (65 - 16)(65 + 16) = 49 \cdot 81. \end{aligned}$$

How can we prove that $c - b$ and $c + b$ are squares? Another observation apparent from our list of examples is that $c - b$ and $c + b$ seem to have no common factors. We can prove this last assertion as follows. Suppose that d is a common factor of $c - b$ and $c + b$; that is, d divides both $c - b$ and $c + b$. Then d also divides

$$(c + b) + (c - b) = 2c \qquad \text{and} \qquad (c + b) - (c - b) = 2b.$$

Thus, d divides $2b$ and $2c$. But b and c have no common factor because we are assuming that (a, b, c) is a primitive Pythagorean triple. So d must equal 1 or 2. But d also divides $(c - b)(c + b) = a^2$, and a is odd, so d must be 1. In other words, the only number dividing both $c - b$ and $c + b$ is 1, so $c - b$ and $c + b$ have no common factor.

We now know that $c - b$ and $c + b$ have no common factor, and that their product is a square since $(c-b)(c+b) = a^2$. The only way that this can happen is if $c - b$ and $c + b$ are themselves squares.[2] So we can write

$$c + b = s^2 \qquad \text{and} \qquad c - b = t^2,$$

where $s > t \geq 1$ are odd integers with no common factors. Solving these two equations for b and c yields

$$c = \frac{s^2 + t^2}{2} \quad \text{and} \quad b = \frac{s^2 - t^2}{2},$$

and then

$$a = \sqrt{(c-b)(c+b)} = st.$$

We have finished our first proof! The following theorem records our accomplishment.

Theorem 2.1 (Pythagorean Triples Theorem). *You will get every primitive Pythagorean triple (a, b, c) with a odd and b even by using the formulas*

$$a = st, \qquad b = \frac{s^2 - t^2}{2}, \qquad c = \frac{s^2 + t^2}{2},$$

where $s > t \geq 1$ are chosen to be any odd integers with no common factors.

For example, if we take $t = 1$, then we get a triple $\left(s, \frac{s^2-1}{2}, \frac{s^2+1}{2}\right)$ whose b and c entries differ by 1. This explains many of the examples we listed above. The following table gives all possible triples with $s \leq 9$.

s	t	$a = st$	$b = \dfrac{s^2 - t^2}{2}$	$c = \dfrac{s^2 + t^2}{2}$
3	1	3	4	5
5	1	5	12	13
7	1	7	24	25
9	1	9	40	41
5	3	15	8	17
7	3	21	20	29
7	5	35	12	37
9	5	45	28	53
9	7	63	16	65

[2] This is intuitively clear if you consider the factorization of $c - b$ and $c + b$ into primes, since the primes in the factorization of $c - b$ will be distinct from the primes in the factorization of $c + b$. However, the existence and uniqueness of the factorization into primes is by no means as obvious as it appears. We will discuss this further in Chapter 7.

A Notational Interlude

Mathematicians have created certain standard notations as a shorthand for various quantities. We will keep our use of such notation to a minimum, but there are a few symbols that are so commonly used and are so useful that it is worthwhile to introduce them here. They are

$$\begin{aligned}\mathbb{N} &= \text{the set of natural numbers} = 1, 2, 3, 4, \ldots\;,\\ \mathbb{Z} &= \text{the set of integers} = \ldots -3, -2, -1, 0, 1, 2, 3, \ldots\;,\\ \mathbb{Q} &= \text{the set of rational numbers (i.e., fractions).}\end{aligned}$$

In addition, mathematicians often use $\mathbb{R}$ to denote the real numbers and $\mathbb{C}$ for the complex numbers, but we will not need these. Why were these letters chosen? The choice of $\mathbb{N}$, $\mathbb{R}$, and $\mathbb{C}$ needs no explanation. The letter $\mathbb{Z}$ for the set of integers comes from the German word "Zahlen," which means numbers. Similarly, $\mathbb{Q}$ comes from the German "Quotient" (which is the same as the English word). We will also use the standard mathematical symbol $\in$ to mean "is an element of the set." So, for example, $a \in \mathbb{N}$ means that a is a natural number, and $x \in \mathbb{Q}$ means that x is a rational number.

Exercises

2.1. (a) We showed that in any primitive Pythagorean triple (a, b, c), either a or b is even. Use the same sort of argument to show that either a or b must be a multiple of 3.

(b) By examining the above list of primitive Pythagorean triples, make a guess about when a, b, or c is a multiple of 5. Try to show that your guess is correct.

2.2. A nonzero integer d is said to *divide* an integer m if $m = dk$ for some number k. Show that if d divides both m and n, then d also divides $m - n$ and $m + n$.

2.3. For each of the following questions, begin by compiling some data; next examine the data and formulate a conjecture; and finally try to prove that your conjecture is correct. (But don't worry if you can't solve every part of this problem; some parts are quite difficult.)

(a) Which odd numbers a can appear in a primitive Pythagorean triple (a, b, c)?

(b) Which even numbers b can appear in a primitive Pythagorean triple (a, b, c)?

(c) Which numbers c can appear in a primitive Pythagorean triple (a, b, c)?

2.4. In our list of examples are the two primitive Pythagorean triples

$$33^2 + 56^2 = 65^2 \qquad \text{and} \qquad 16^2 + 63^2 = 65^2.$$

Find at least one more example of two primitive Pythagorean triples with the same value of c. Can you find three primitive Pythagorean triples with the same c? Can you find more than three?

2.5. In Chapter 1 we saw that the n^{th} triangular number T_n is given by the formula

$$T_n = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

The first few triangular numbers are 1, 3, 6, and 10. In the list of the first few Pythagorean triples (a, b, c), we find $(3, 4, 5)$, $(5, 12, 13)$, $(7, 24, 25)$, and $(9, 40, 41)$. Notice that in each case, the value of b is four times a triangular number.

(a) Find a primitive Pythagorean triples (a, b, c) with $b = T_5$. Do the same for $b = T_6$ and with $b = T_7$.

(b) Do you think that for every triangular number T_n, there is a primitive Pythagorean triple (a, b, c) with $b = 4T_n$? If you believe that this is true, then prove it. Otherwise, find some triangular number for which it is not true.

2.6. If you look at the table of primitive Pythagorean triples in this chapter, you will see many triples in which c is 2 greater than a. For example, the triples $(3, 4, 5)$, $(15, 8, 17)$, $(35, 12, 37)$, and $(63, 16, 65)$ all have this property.

(a) Find two more primitive Pythagorean triples (a, b, c) having $c = a + 2$.

(b) Find a primitive Pythagorean triple (a, b, c) having $c = a + 2$ and $c > 1000$.

(c) Try to find a formula that describes all primitive Pythagorean triples (a, b, c) having $c = a + 2$.

2.7. For each primitive Pythagorean triple (a, b, c) in the table in this chapter, compute the quantity $2c - 2a$. Do these values seem to have some special form? Try to prove that your observation is true for all primitive Pythagorean triples.

2.8. (a) Read about the Babylonian number system and write a short description, including the symbols for the numbers 1 to 10 and the multiples of 10 from 20 to 50.

(b) Read about the Babylonian tablet called Plimpton 322 and write a brief description, including its approximate date of origin and some of the large Pythagorean triples that it contains.

Chapter 3

Pythagorean Triples and the Unit Circle

In the previous chapter we described all solutions to

$$a^2 + b^2 = c^2$$

in whole numbers a, b, c. If we divide this equation by c^2, we obtain

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1.$$

So the pair of rational numbers $(a/c, b/c)$ is a solution to the equation

$$x^2 + y^2 = 1.$$

Everyone knows what the equation $x^2 + y^2 = 1$ looks like: It is a circle C of radius 1 with center at $(0, 0)$. We are going to use the geometry of the circle C to find all the points on C whose xy-coordinates are rational numbers. Notice that the circle has four obvious points with rational coordinates, $(\pm 1, 0)$ and $(0, \pm 1)$. Suppose that we take any (rational) number m and look at the line L going through the point $(-1, 0)$ and having slope m. (See Figure 3.1.) The line L is given by the equation

$$L : y = m(x + 1) \qquad \text{(point–slope formula).}$$

It is clear from the picture that the intersection $C \cap L$ consists of exactly two points, and one of those points is $(-1, 0)$. We want to find the other one.

To find the intersection of C and L, we need to solve the equations

$$x^2 + y^2 = 1 \qquad \text{and} \qquad y = m(x + 1)$$

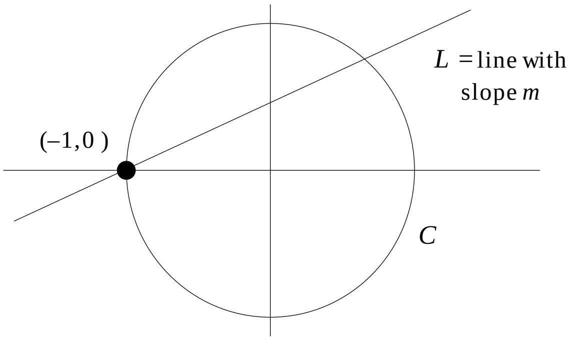


Figure 3.1: The Intersection of a Circle and a Line

for x and y. Substituting the second equation into the first and simplifying, we need to solve

$$\begin{aligned} x^2 + \big(m(x+1)\big)^2 &= 1 \\ x^2 + m^2(x^2+2x+1) &= 1 \\ (m^2+1)x^2 + 2m^2x + (m^2-1) &= 0. \end{aligned}$$

This is just a quadratic equation, so we could use the quadratic formula to solve for x. But there is a much easier way to find the solution. We know that $x=-1$ must be a solution, since the point $(-1,0)$ is on both C and L. This means that we can divide the quadratic polynomial by $x+1$ to find the other root:

$$\begin{array}{r} (m^2+1)x + (m^2-1) \\ x+1 \,\big)\overline{(m^2+1)x^2 + 2m^2x + (m^2-1)} \;. \end{array}$$

So the other root is the solution of $(m^2+1)x + (m^2-1) = 0$, which means that

$$x = \frac{1-m^2}{1+m^2}.$$

Then we substitute this value of x into the equation $y = m(x+1)$ of the line L to find the y-coordinate,

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

Thus, for every rational number m we get a solution in rational numbers

$$\left(\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2}\right) \quad \text{to the equation} \quad x^2+y^2=1.$$

On the other hand, if we have a solution (x_1, y_1) in rational numbers, then the slope of the line through (x_1, y_1) and $(-1, 0)$ will be a rational number. So by taking all possible values for m, the process we have described will yield every solution to $x^2 + y^2 = 1$ in rational numbers [except for $(-1, 0)$, which corresponds to a vertical line having slope "$m = \infty$"]. We summarize our results in the following theorem.

Theorem 3.1. *Every point on the circle*

$$x^2 + y^2 = 1$$

whose coordinates are rational numbers can be obtained from the formula

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

by substituting in rational numbers for m. [Except for the point $(-1, 0)$, which is the limiting value as $m \to \infty$.]

How is this formula for rational points on a circle related to our formula for Pythagorean triples? If we write the rational number m as a fraction v/u, then our formula becomes

$$(x, y) = \left(\frac{u^2 - v^2}{u^2 + v^2}, \frac{2uv}{u^2 + v^2}\right),$$

and clearing denominators gives the Pythagorean triple

$$(a, b, c) = (u^2 - v^2, 2uv, u^2 + v^2).$$

This is another way of describing all Pythagorean triples, although to describe only the primitive ones would require some restrictions on u and v. You can relate this description to the formula in Chapter 2 by setting

$$u = \frac{s + t}{2} \qquad \text{and} \qquad v = \frac{s - t}{2}.$$

Exercises

3.1. As we have just seen, we get every Pythagorean triple (a, b, c) with b even from the formula

$$(a, b, c) = (u^2 - v^2, 2uv, u^2 + v^2)$$

by substituting in different integers for u and v. For example, $(u, v) = (2, 1)$ gives the smallest triple $(3, 4, 5)$.

(a) If u and v have a common factor, explain why (a, b, c) will not be a primitive Pythagorean triple.

(b) Find an example of integers $u > v > 0$ that do not have a common factor, yet the Pythagorean triple $(u^2 - v^2, 2uv, u^2 + v^2)$ is not primitive.

(c) Make a table of the Pythagorean triples that arise when you substitute in all values of u and v with $1 \leq v < u \leq 10$.

(d) Using your table from (c), find some simple conditions on u and v that ensure that the Pythagorean triple $(u^2 - v^2, 2uv, u^2 + v^2)$ is primitive.

(e) Prove that your conditions in (d) really work.

3.2. (a) Use the lines through the point $(1, 1)$ to describe all the points on the circle

$$x^2 + y^2 = 2$$

whose coordinates are rational numbers.

(b) What goes wrong if you try to apply the same procedure to find all the points on the circle $x^2 + y^2 = 3$ with rational coordinates?

3.3. Find a formula for all the points on the hyperbola

$$x^2 - y^2 = 1$$

whose coordinates are rational numbers. [*Hint*. Take the line through the point $(-1, 0)$ having rational slope m and find a formula in terms of m for the second point where the line intersects the hyperbola.]

3.4. The curve

$$y^2 = x^3 + 8$$

contains the points $(1, -3)$ and $(-7/4, 13/8)$. The line through these two points intersects the curve in exactly one other point. Find this third point. Can you explain why the coordinates of this third point are rational numbers?