Chapter 1

Introduction

Suppose a collection of cannonballs is piled in a square pyramid with one ball on the top layer, four on the second layer, nine on the third layer, etc. If the pile collapses, is it possible to rearrange the balls into a square array?

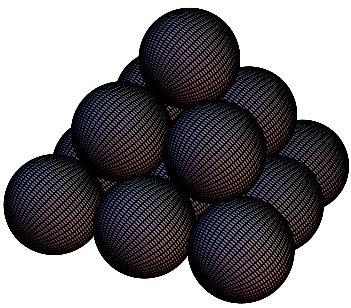

Figure 1.1
A Pyramid of Cannonballs

If the pyramid has three layers, then this cannot be done since there are $1 + 4 + 9 = 14$ balls, which is not a perfect square. Of course, if there is only one ball, it forms a height one pyramid and also a one-by-one square. If there are no cannonballs, we have a height zero pyramid and a zero-by-zero square. Besides theses trivial cases, are there any others? We propose to find another example, using a method that goes back to Diophantus (around 250 A.D.).

If the pyramid has height x, then there are

$$1^2 + 2^2 + 3^2 + \cdots + x^2 = \frac{x(x+1)(2x+1)}{6}$$

balls (see Exercise 1.1). We want this to be a perfect square, which means that we want to find a solution to

$$y^2 = \frac{x(x+1)(2x+1)}{6}$$

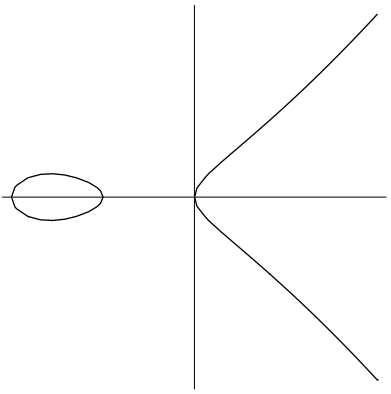

Figure 1.2
$y^2 = x(x+1)(2x+1)/6$

in positive integers x, y. An equation of this type represents an **elliptic curve**. The graph is given in Figure 1.2.

The method of Diophantus uses the points we already know to produce new points. Let's start with the points (0,0) and (1,1). The line through these two points is $y = x$. Intersecting with the curve gives the equation

$$x^2 = \frac{x(x+1)(2x+1)}{6} = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x.$$

Rearranging yields

$$x^3 - \frac{3}{2}x^2 + \frac{1}{2}x = 0.$$

Fortunately, we already know two roots of this equation: $x = 0$ and $x = 1$. This is because the roots are the x-coordinates of the intersections between the line and the curve. We could factor the polynomial to find the third root, but there is a better way. Note that for any numbers a, b, c, we have

$$(x-a)(x-b)(x-c) = x^3 - (a+b+c)x^2 + (ab+ac+bc)x - abc.$$

Therefore, when the coefficient of x^3 is 1, the negative of the coefficient of x^2 is the sum of the roots.

In our case, we have roots $0, 1$, and x, so

$$0 + 1 + x = \frac{3}{2}.$$

Therefore, $x = 1/2$. Since the line was $y = x$, we have $y = 1/2$, too. It's hard to say what this means in terms of piles of cannonballs, but at least we have found another point on the curve. In fact, we automatically have even one more point, namely $(1/2, -1/2)$, because of the symmetry of the curve.

Let's repeat the above procedure using the points $(1/2, -1/2)$ and $(1, 1)$. Why do we use these points? We are looking for a point of intersection somewhere in the first quadrant, and the line through these two points seems to be the best choice. The line is easily seen to be $y = 3x - 2$. Intersecting with the curve yields

$$(3x - 2)^2 = \frac{x(x + 1)(2x + 1)}{6}.$$

This can be rearranged to obtain

$$x^3 - \frac{51}{2}x^2 + \cdots = 0.$$

(By the above trick, we will not need the lower terms.) We already know the roots $1/2$ and 1, so we obtain

$$\frac{1}{2} + 1 + x = \frac{51}{2},$$

or $x = 24$. Since $y = 3x - 2$, we find that $y = 70$. This means that

$$1^2 + 2^2 + 3^2 + \cdots + 24^2 = 70^2.$$

If we have 4900 cannonballs, we can arrange them in a pyramid of height 24, or put them in a 70-by-70 square. If we keep repeating the above procedure, for example, using the point just found as one of our points, we'll obtain infinitely many rational solutions to our equation. However, it can be shown that (24, 70) is the only solution to our problem in positive integers other than the trivial solution with $x = 1$. This requires more sophisticated techniques and we omit the details. See [5].

Here is another example of Diophantus's method. Is there a right triangle with rational sides with area equal to 5? The smallest Pythagorean triple (3,4,5) yields a triangle with area 6, so we see that we cannot restrict our attention to integers. Now look at the triangle with sides (8, 15, 17). This yields a triangle with area 60. If we divide the sides by 2, we end up with a triangle with sides (4, 15/2, 17/2) and area 15. So it is possible to have nonintegral sides but integral area.

Let the triangle we are looking for have sides a, b, c, as in Figure 1.3. Since the area is $ab/2 = 5$, we are looking for rational numbers a, b, c such that

$$a^2 + b^2 = c^2, \qquad ab = 10.$$

A little manipulation yields

$$\left(\frac{a + b}{2}\right)^2 = \frac{a^2 + 2ab + b^2}{4} = \frac{c^2 + 20}{4} = \left(\frac{c}{2}\right)^2 + 5,$$

$$\left(\frac{a - b}{2}\right)^2 = \frac{a^2 - 2ab + b^2}{4} = \frac{c^2 - 20}{4} = \left(\frac{c}{2}\right)^2 - 5.$$

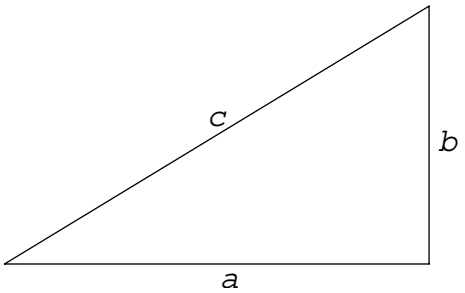

Figure 1.3

Let $x = (c/2)^2$. Then we have

$$x - 5 = ((a-b)/2)^2 \quad \text{and} \quad x + 5 = ((a+b)/2)^2.$$

We are therefore looking for a rational number x such that

$$x - 5, \quad x, \quad x + 5$$

are simultaneously squares of rational numbers. Another way to say this is that we want three squares of rational numbers to be in an arithmetical progression with difference 5.

Suppose we have such a number x. Then the product $(x-5)(x)(x+5) = x^3 - 25x$ must also be a square, so we need a rational solution to

$$y^2 = x^3 - 25x.$$

As above, this is the equation of an elliptic curve. Of course, if we have such a rational solution, we are not guaranteed that there will be a corresponding rational triangle (see Exercise 1.2). However, once we have a rational solution with $y \neq 0$, we can use it to obtain another solution that does correspond to a rational triangle (see Exercise 1.2). This is what we'll do below.

For future use, we record that

$$x = \left(\frac{c}{2}\right)^2, \quad y = ((x-5)(x)(x+5))^{1/2} = \frac{(a-b)(c)(a+b)}{8} = \frac{(a^2-b^2)c}{8}.$$

There are three "obvious" points on the curve: $(-5,0), (0,0), (5,0)$. These do not help us much. They do not yield triangles and the line through any two of them intersects the curve in the remaining point. A small search yields the point $(-4,6)$. The line through this point and any one of the three other points yields nothing useful. The only remaining possibility is to take the line through $(-4,6)$ and itself, namely, the tangent line to the curve at the $(-4,6)$. Implicit differentiation yields

$$2yy' = 3x^2 - 25, \qquad y' = \frac{3x^2-25}{2y} = \frac{23}{12}.$$

The tangent line is therefore

$$y = \frac{23}{12}x + \frac{41}{3}.$$

Intersecting with the curve yields

$$\left(\frac{23}{12}x + \frac{41}{3}\right)^2 = x^3 - 25x,$$

which implies

$$x^3 - \left(\frac{23}{12}\right)^2 x^2 + \cdots = 0.$$

Since the line is tangent to the curve at $(-4, 6)$, the root $x = -4$ is a double root. Therefore the sum of the roots is

$$-4 - 4 + x = \left(\frac{23}{12}\right)^2.$$

We obtain $x = 1681/144 = (41/12)^2$. The equation of the line yields $y = 62279/1728$.

Since $x = (c/2)^2$, we obtain $c = 41/6$. Therefore,

$$\frac{62279}{1728} = y = \frac{(a^2 - b^2)c}{8} = \frac{41(a^2 - b^2)}{48}.$$

This yields

$$a^2 - b^2 = \frac{1519}{36}.$$

Since

$$a^2 + b^2 = c^2 = (41/6)^2,$$

we solve to obtain $a^2 = 400/9$ and $b^2 = 9/4$. We obtain a triangle (see Figure 1.4) with

$$a = \frac{20}{3}, \quad b = \frac{3}{2}, \quad c = \frac{41}{6},$$

which has area 5. This is, of course, the $(40, 9, 41)$ triangle rescaled by a factor of 6.

There are infinitely many other solutions. These can be obtained by successively repeating the above procedure, for example, starting with the point just found (see Exercise 1.4).

The question of which integers n can occur as areas of right triangles with rational sides is known as the **congruent number problem**. Another formulation, as we saw above, is whether there are three rational squares in arithmetic progression with difference n. It appears in Arab manuscripts around 900 A.D. A conjectural answer to the problem was proved by Tunnell in the 1980s [122]. Recall that an integer n is called squarefree if n is not

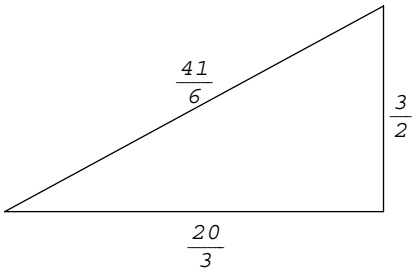

Figure 1.4

a multiple of any perfect square other than 1. For example, 5 and 15 are squarefree, while 24 and 75 are not.

CONJECTURE 1.1

Let n be an odd, squarefree, positive integer. Then n can be expressed as the area of a right triangle with rational sides if and only if the number of integer solutions to

$$2x^2 + y^2 + 8z^2 = n$$

with z even equals the number of solutions with z odd.

Let $n = 2m$ with m odd, squarefree, and positive. Then n can be expressed as the area of a right triangle with rational sides if and only if the number of integer solutions to

$$4x^2 + y^2 + 8z^2 = m$$

with z even equals the number of integer solutions with z odd.

Tunnell [122] proved that if there is a triangle with area n, then the number of odd solutions equals the number of even solutions. However, the proof of the converse, namely that the condition on the number of solutions implies the existence of a triangle of area n, uses the Conjecture of Birch and Swinnerton-Dyer, which is not yet proved (see Chapter 14).

For example, consider $n = 5$. There are no solutions to $2x^2 + y^2 + 8z^2 = 5$. Since $0 = 0$, the condition is trivially satisfied and the existence of a triangle of area 5 is predicted. Now consider $n = 1$. The solutions to $2x^2+y^2+8z^2 = 1$ are $(x, y, z) = (0, 1, 0)$ and $(0, -1, 0)$, and both have z even. Since $2 \neq 0$, there is no rational right triangle of area 1. This was first proved by Fermat by his method of descent (see Chapter 8).

For a nontrivial example, consider $n = 41$. The solutions to $2x^2+y^2+8z^2 = 41$ are

$$(\pm 4, \pm 3, 0), (\pm 4, \pm 1, \pm 1), (\pm 2, \pm 5, \pm 1), (\pm 2, \pm 1, \pm 2), (0, \pm 3, \pm 2)$$

(all possible combinations of plus and minus signs are allowed). There are 32 solutions in all. There are 16 solutions with z even and 16 with z odd. Therefore, we expect a triangle with area 41. The same method as above, using the tangent line at the point $(-9, 120)$ to the curve $y^2 = x^3 - 41^2x$, yields the triangle with sides (40/3, 123/20, 881/60) and area 41.

For much more on the congruent number problem, see [64].

Finally, let's consider the quartic Fermat equation. We want to show that

$$a^4 + b^4 = c^4 \tag{1.1}$$

has no solutions in nonzero integers a, b, c. This equation represents the easiest case of Fermat's Last Theorem, which asserts that the sum of two nonzero nth powers of integers cannot be a nonzero nth power when $n \geq 3$. This general result was proved by Wiles (using work of Frey, Ribet, Serre, Mazur, Taylor, ...) in 1994 using properties of elliptic curves. We'll discuss some of these ideas in Chapter 15, but, for the moment, we restrict our attention to the much easier case of $n = 4$. The first proof in this case was due to Fermat.

Suppose $a^4 + b^4 = c^4$ with $a \neq 0$. Let

$$x = 2\frac{b^2 + c^2}{a^2}, \quad y = 4\frac{b(b^2 + c^2)}{a^3}$$

(see Example 2.2). A straightforward calculation shows that

$$y^2 = x^3 - 4x.$$

In Chapter 8 we'll show that the only rational solutions to this equation are

$$(x, y) = (0, 0),\ (2, 0),\ (-2, 0).$$

These all correspond to $b = 0$, so there are no nontrivial integer solutions of (1.1).

The cubic Fermat equation also can be changed to an elliptic curve. Suppose that $a^3 + b^3 = c^3$ and $abc \neq 0$. Since $a^3 + b^3 = (a + b)(a^2 - ab + b^2)$, we must have $a + b \neq 0$. Let

$$x = 12\frac{c}{a + b}, \qquad y = 36\frac{a - b}{a + b}.$$

Then

$$y^2 = x^3 - 432.$$

(Where did this change of variables come from? See Section 2.5.2.) It can be shown (but this is not easy) that the only rational solutions to this equation are $(x, y) = (12, \pm 36)$. The case $y = 36$ yields $a - b = a + b$, so $b = 0$. Similarly, $y = -36$ yields $a = 0$. Therefore, there are no solutions to $a^3 + b^3 = c^3$ when $abc \neq 0$.

Exercises

1.1 Use induction to show that

$$1^2 + 2^2 + 3^2 + \cdots + x^2 = \frac{x(x+1)(2x+1)}{6}$$

for all integers $x \geq 0$.

1.2 (a) Show that if x, y are rational numbers satisfying $y^2 = x^3 - 25x$ and x is a square of a rational number, then this does not imply that $x + 5$ and $x - 5$ are squares. (*Hint:* Let $x = 25/4$.)

(b) Let n be an integer. Show that if x, y are rational numbers satisfying $y^2 = x^3 - n^2x$, and $x \neq 0, \pm n$, then the tangent line to this curve at (x, y) intersects the curve in a point (x_1, y_1) such that x_1, $x_1 - n$, $x_1 + n$ are squares of rational numbers. (For a more general statement, see Theorem 8.14.) This shows that the method used in the text is guaranteed to produce a triangle of area n if we can find a starting point with $x \neq 0, \pm n$.

1.3 Diophantus did not work with analytic geometry and certainly did not know how to use implicit differentiation to find the slope of the tangent line. Here is how he could find the tangent to $y^2 = x^3 - 25x$ at the point $(-4, 6)$. It appears that Diophantus regarded this simply as an algebraic trick. Newton seems to have been the first to recognize the connection with finding tangent lines.

(a) Let $x = -4 + t$, $y = 6 + mt$. Substitute into $y^2 = x^3 - 25x$. This yields a cubic equation in t that has $t = 0$ as a root.

(b) Show that choosing $m = 23/12$ makes $t = 0$ a double root.

(c) Find the nonzero root t of the cubic and use this to produce $x = 1681/144$ and $y = 62279/1728$.

1.4 Use the tangent line at $(x, y) = (1681/144, 62279/1728)$ to find another right triangle with area 5.

1.5 Show that the change of variables $x_1 = 12x + 6$, $y_1 = 72y$ changes the curve $y_1^2 = x_1^3 - 36x_1$ to $y^2 = x(x + 1)(2x + 1)/6$.