Section 2: Diophantus

Fermat wrote his famous marginal note in a Latin translation of *Arithmetica* by the ancient Greek mathematician Diophantus. That reason alone would be enough motivation for studying Diophantus and his work. But in fact Diophantus was the product of an amazing Greek culture of mathematical achievement and was a talented number theorist in his own right. It could be argued that he was the first true number theorist and he worked with indeterminate equations – now called Diophantine equations in his honor. His work therefore holds a central place in this class, and is well deserving of some attention.

Mathematics as an intellectual discipline began (as most intellectual disciplines did) with the Egyptians and the Babylonians around 2000 BC. While both civilizations did extensive mathematics, almost all of their achievements were empirical in nature. In other words, they did very little abstract mathematics, did very little in the way of theorem-proving, and all problems had real world applications or origins. But something changed over the following 1500 years and the Greek civilization that arose along the rocky shores of the eastern Mediterranean Sea fully embraced abstraction and insisted on deductive reasoning as a basis for finding results. It was no longer enough to verify that a result seemed true by experimentation. Furthermore, problems no longer had to come from commerce, land measurements or other real world situations.

Greek mathematicians were a very accomplished group. The birth of modern deductive reasoning can be traced to Thales (c. 500 BC) and Euclid (c. 300 BC) was the father of geometry and his impressive work *The Elements* was the standard geometry textbook for 2000 years. Think about that for a second! Additionally, in any poll ranking the greatest mathematicians of all time, Archimedes (287-212 BC) is sure to be included among the top 3 or 4. Included in this upper echelon of Greek mathematicians is Diophantus of Alexandria (c. 250 AD).

Diophantus was one of the first abstract number theorists and his work dealt primarily with indeterminate equations. These are polynomial equations in one or more variables for which we are to find either integer or rational solutions. The Pythagorean Theorem $x^2 + y^2 = z^2$ is a good example of such an equation. In his honor, equations of this type are now known as *Diophantine equations*.

One of the goals in Diophantine analysis (solving Diophantine equations) is not just finding one solution in the integers (or rationals), but if possible characterizing all solutions. When trying to generalize all possible solutions to a particular equation, a good place to start is listing out several solutions and examining them for common characteristics. We will examine this process with the Pythagorean Theorem. Let's start by listing some solutions (for this we will restrict ourselves to the integers), called *Pythagorean triples*. One such triple is (3,4,5) since $3^2 + 4^2 = 5^2$. Note that once we have a solution, any multiple will also be a solution. So we will also only look for solutions that have no common factors, these are called *primitive Pythagorean triples*.

Some primitive Pythagorean triples: (3,4,5), (5,12,13), (8,15,17), (7,24,25), (20, 21, 29)

Exercise 1.2.1 Find six more primitive Pythagorean triples.
[Note: You may do research to come up with these, or just use trial and error. There are obviously many more solutions, even many with all three numbers less than 70 or so. We will shortly have a way to generate as many as we wish.]

What do we notice about this short listing of some solutions?

(a) One of x and y is odd and the other is even.
(b) z is always odd.

Once we notice a pattern, of course we have to show that we are right. Can we verify that these conjectures are correct? Suppose both x and y were odd. Then x^2 and y^2 would both be odd as well, making z^2 even. That means z is even also. So in this case, there would be three integers a, b, and c such that:

$$x = 2a+1 \qquad y = 2b+1 \qquad z = 2c\,.$$

If we substitute these in the equation $x^2 + y^2 = z^2$, we get

$$\begin{aligned}(2a+1)^2 + (2b+1)^2 &= (2c)^2\\ 4a^2 + 4a + 1 + 4b^2 + 4b + 1 &= 4c^2\\ 4a^2 + 4a + 4b^2 + 4b + 2 &= 4c^2\end{aligned}$$

Dividing both sides by 2 yields $2a^2 + 2a + 2b^2 + 2b + 1 = 2c^2$, which is clearly an impossibility (left side is odd, right side is even). So x and y cannot both be odd.

Exercise 1.2.2 Prove that in a primitive Pythagorean triple x and y cannot both be even.

Now that we know conjecture (a) is true, conjecture (b) is easy. If exactly one of x and y is odd, the left side of $x^2 + y^2 = z^2$ is odd. So z^2 is odd, which makes z odd. Of course, we can always interchange x and y, so we will always orient our primitive Pythagorean triple so that:

x is odd, y is even, and x, y, z have no common factors.

To continue our analysis in an attempt to characterize all solutions, notice that we can factor

$$x^2 = z^2 - y^2 = (z-y)(z+y)$$

Example 1.2.3 Here are a few examples from the previous primitive Pythagorean triples:

$3^2 = 5^2 - 4^2 = (5-4)(5+4) = 1 \cdot 9$
$5^2 = 13^2 - 12^2 = (13-12)(13+12) = 1 \cdot 25$
$15^2 = 17^2 - 8^2 = (17-8)(17+8) = 9 \cdot 25$ *
$7^2 = 25^2 - 24^2 = (25-24)(25+24) = 1 \cdot 49$
$21^2 = 29^2 - 20^2 = (29-20)(29+20) = 9 \cdot 49$ *

*Note that I reordered the triple so that x was odd.

A couple more conjectures come to mind:

(c) It looks like $z-y$ and $z+y$ are relatively prime (i.e. have no common factors).
(d) It looks like $z-y$ and $z+y$ are always themselves squares.

Exercise 1.2.4 Prove conjecture (c). Hints: Suppose that they have a common factor, call it m, and then show that $m=1$. You may want to use some divisibility facts:

(i) If d divides a and b, then d divides $a+b$ and $a-b$.

(ii) If d divides ab and ac, but b and c are relatively prime, then d divides a.

Once again, the second conjecture follows fairly quickly from the first. If $z-y$ and $z+y$ are relatively prime and their product is a square (recall $(z-y)(z+y)=x^2$), then both factors must be squares themselves. (Think of the prime factorizations of $z-y$ and $z+y$. Every prime in the factorization of $z-y$ will be distinct from every prime in the factorization of $z+y$, yet in the prime factorization of x^2, every prime appears an even number of times. By the way, the existence and uniqueness of prime factorizations is far from obvious. We will discuss this more in Section 2.3.)

So we can write $z-y=s^2$ and $z+y=t^2$ where s and t are odd natural numbers with no common factors. If we solve these two equations for z and y, we get

$$z = \frac{s^2+t^2}{2} \qquad \text{and} \qquad y = \frac{s^2-t^2}{2},$$

and then $x = \sqrt{x^2} = \sqrt{s^2t^2} = st$. That does it. We have just characterized all solutions to $x^2+y^2=z^2$.

Theorem 1.2.5 Every primitive Pythagorean triple is of the form

$$x = st, \quad y = \frac{s^2 - t^2}{2}, \quad z = \frac{s^2 + t^2}{2}$$

for some odd relatively prime natural numbers s and t.

For example, here are the previous primitive Pythagorean triples:

s	t	$x = st$	$y = \frac{s^2-t^2}{2}$	$z = \frac{s^2+t^2}{2}$
3	1	3	4	5
5	1	5	12	13
5	3	15	8	17
7	1	7	24	25
7	3	21	20	29

Exercise 1.2.6 Find 10 more primitive Pythagorean triples (different from my 5 and your previous 6).

Obviously there are many other Diophantine equations that have been studied through the years. Here are a few:

Exercise 1.2.7 In 1738, Euler showed that $x^2 - y^3 = 1$ has only one solution in the natural numbers. Find it. It is also true that $x^3 - y^2 = 2$ has a unique natural solution. Find it also.

(As an aside, in 1932, Atle Selberg showed that $x^4 - y^3 = 1$ has no solutions.)

Exercise 1.2.8 It has been shown that $1 + 2 + \ldots + n = 1^2 + 2^2 + \ldots + k^2$ has only four solutions. The most difficult of the four solutions is $n = 645$ and $k = 85$. Find the other three.

As much as we know about Diophantus' mathematics (thanks to his *Arithmetica*), not much is known about Diophantus and his life. Even the years of his birth and death are not known exactly. Much of what we do know comes from a mathematical puzzle that forms, appropriately, a Diophantine equation. It goes like this:

> Diophantus lived $\frac{1}{6}$ of his life in childhood, $\frac{1}{12}$ in youth, and $\frac{1}{7}$ more as a bachelor. Five years after his marriage was born a son who died 4 years before his father and at half his father's final age.

Exercise 1.2.9 Find the linear equation described by the above puzzle, and solve it to find out how long Diophantus lived.