Parabola Volume 41, Issue 1 (2005)

Beginning Algebraic Number Theory

David Angell[1]

Fermat's Last Theorem is one of the most famous problems in mathematics. Its origin can be traced back to the work of the Greek mathematician Diophantus (third century A.D.), who wrote a treatise on solving various kinds of equations. One of his problems was 'to divide a square into two squares', or, in modern terminology, to solve $x^2 + y^2 = z^2$. Diophantus' *Arithmetica* was translated into Latin in 1621, and hence became available to western European scholars. Pierre de Fermat, a lawyer by profession but nonetheless one of the greatest mathematicians of all time, wrote a note in the margin,

> To divide a cube into two cubes, a fourth power into two fourth powers [and so on] is impossible. I have discovered a marvellous proof of this fact, but there is not enough space to write it in the margin [of the book].

It is important to remember that both Diophantus and Fermat were talking about solving equations in integers (actually, in rational numbers, but in this case it comes to the same thing). So Fermat's claim is, in effect, that

> if n is an integer greater than 2, then the equation $x^n + y^n = z^n$ has no solutions in which x, y and z are positive integers.

This statement has become known as *Fermat's Last Theorem*. Fermat wrote his note in about 1637, but did not leave a proof either in the margin or elsewhere; we can only speculate as to whether or not he actually had a correct proof. Three centuries of work by many mathematicians showed that the problem is actually far harder than (presumably) anyone could have imagined, and opened up new areas of mathematics in the process. Probably we must assume that even Fermat got it wrong sometimes! The Last Theorem was finally proved by Andrew Wiles in 1995.

Pythagorean triples. Let's begin with Diophantus' problem of solving $x^2 + y^2 = z^2$. A solution in positive integers of this equation is known as a Pythagorean triple, because of the obvious connection with Pythagoras' Theorem. There are many well–known solutions, for instance,

$$3^2 + 4^2 = 5^2 \quad \text{and} \quad 5^2 + 12^2 = 13^2 \quad \text{and} \quad 8^2 + 15^2 = 17^2 \, . \tag{1}$$

There is also $4961^2 + 6480^2 = 8191^2$ which was known to the Babylonians (*ca.* 1500 B.C.). Collecting examples, however, is rather unsatisfying, and we would like, if we can, to

[1]David Angell is an Associate Lecturer in the School of Mathematics, University of New South Wales.

find *all* Pythagorean triples. This turns out to be possible through the use of a few basic facts about integers.

First, let's look at a few more Pythagorean triples. We have, for example,

$$6^2 + 8^2 = 10^2 \quad \text{and} \quad 9^2 + 12^2 = 15^2 \quad \text{and} \quad 12^2 + 16^2 = 20^2$$

and so on. These are not very interesting, however, as they are really just 'disguised' versions of $3^2 + 4^2 = 5^2$. So we'll assume initially that x, y and z have no common factor. Then at the end of the problem we can just multiply the common factor back in again, should we wish to write down *all* solutions.

So let's try to find solutions of $x^2 + y^2 = z^2$ in which x, y and z are positive integers with no common factor. Looking at the examples (1), you might notice that in each case x is odd and y even, or *vice versa*. Is this always true? In principle there are two other possibilities.

- Suppose that x and y are both even. Then $x^2 + y^2$ is even, so z^2 is even, so z is even. But this means that x, y and z all have a common factor of 2 (or perhaps more), and we have agreed to ignore this possibility. So this case can be ruled out.

- Could x and y both be odd? If so, then x^2 and y^2 are odd and so z^2 is even. But now consider the remainder when these squares are divided by 4. We have

  $$x^2 = (\text{odd})^2 = (2p+1)^2 = 4p^2 + 4p + 1 = 4(p^2 + p) + 1 \,,$$

  and so the remainder is 1; the same goes for y^2. On the other hand

  $$z^2 = (\text{even})^2 = (2q)^2 = 4q^2 \,,$$

  and the remainder is 0. Altogether, if we divide by 4 then the remainder on the left hand side is 2, while on the right hand side it is 0. This is impossible.

As we have eliminated all possible alternatives, we may conclude that the fact we observed in examples (1) is actually true for all Pythagorean triples with no common factor: one of the numbers x and y is odd, the other even. Which is which? Since x^2+y^2 is the same as $y^2 + x^2$, it doesn't matter. Let's assume that x is odd and y is even; once we have solved to find x and y, if we want *all* solutions we must remember to allow for an interchange of x and y.

Before proceeding, let's also comment that we now know that z is odd too.

What we have done so far really amounts to clearing away some of the minor difficulties. We now turn to the key step, which is to rearrange the equation $x^2 + y^2 = z^2$ and factorise. Using the difference of two squares, we find

$$x^2 = z^2 - y^2 = (z + y)(z - y) \,. \tag{2}$$

Now, what can we deduce from the fact that the product of the numbers $z + y$ and $z - y$ is a square? Clearly one possibility is that the two numbers themselves are both

squares; however by looking at an example we see that this is not the only possibility. For example, 900 is a square; it can be factorised as

$$\boxed{1 \times 900} = 3 \times 300 = \boxed{4 \times 225} = 5 \times 180 = 6 \times 150 = \boxed{9 \times 100}\,,$$

and so on. In some cases (enclosed in boxes) each of the two factors is a square, in other cases not. However, if we look closely at these examples, we may notice that when the factors are not squares, then they have a common factor – thus 3 and 300 are both multiples of 3, while 5 and 180 are both multiples of 5. In fact this is always true; the following result is very important.

Theorem. Suppose that p and q are positive integers, that they have no common factor, and that their product pq is a square. Then both p and q are squares.

Returning to our investigation of Pythagorean triples, (2) tells us that $z+y$ and $z-y$ will both be squares, *if* we can be sure that they have no common factor. Well, suppose that $d > 1$ and d is a factor of both $z + y$ and $z - y$. First, we can say that d is odd; for z is odd and y is even, so $z + y$ and $z - y$ are odd, and odd numbers don't have even factors. Next, d is a factor of the sum and difference of $z + y$ and $z - y$, that is, of $2z$ and $2y$; and since d is odd it must be a factor of both z and y. But this is impossible: it means that d is also a factor of x, and we are back to the case which we have already excluded.

So, now we know that $z + y$ and $z - y$ are both squares, let's give them some appropriate names, say,

$$z + y = a^2 \quad \text{and} \quad z - y = b^2\,.$$

Here a and b are positive integers; they are odd, because $z + y$ and $z - y$ are odd; they have no common factor, as $z + y$ and $z - y$ have none; and $a > b$ because $z + y > z - y$. Moreover, we can now easily find x, y and z in terms of a and b. We have

$$z = \frac{(z+y)+(z-y)}{2} = \frac{a^2+b^2}{2}\,, \quad y = \frac{(z+y)-(z-y)}{2} = \frac{a^2-b^2}{2}\,,$$

and

$$x^2 = (z+y)(z-y) = a^2b^2\,,$$

so $x = ab$. That's it!

Theorem. All solutions of $x^2 + y^2 = z^2$ in which x, y, z are positive integers with no common factor and x is odd, are given by the formulae

$$x = ab\,, \quad y = \frac{a^2-b^2}{2}\,, \quad z = \frac{a^2+b^2}{2}\,,$$

where a and b are odd positive integers with no common factor and $a > b$.

Example. Find a large Pythagorean triple without using trial and error. Take, for instance, $a = 98765$ and $b = 4321$; use the above formulae (and a calculator!) to get

$$426763565^2 + 4867927092^2 = 4886598133^2\,.$$

Exercises.

1. What values of a and b will give the Babylonian triple mentioned on page 15?

2. We should have checked that 98765 and 4321 have no common factor. Confirm this by using the **Euclidean algorithm**. (Look it up, or ask your teacher!)

Another example. The ideas used in studying Pythagorean triples can be extended and used to investigate a wide variety of other equations where we seek solutions in positive integers. A particularly interesting and not excessively difficult example is $x^2 + 2 = y^3$; this is sometimes called *Mordell's equation*, after Louis Mordell, who made an extensive study of equations having the form $x^2 + k = y^3$, where k is a specified integer.

It is not hard by trial and error to find a solution, $x = 5$, $y = 3$, to Mordell's equation. Once again, however, we should like to find all solutions; we'll try to do so by taking advantage of the methods we used above.

So, we wish to find all positive integers x and y which satisfy the equation

$$x^2 + 2 = y^3 \ . \tag{3}$$

Let's jump straight to the "key step" of factorising part of the equation. This doesn't seem to be as easy as the last time since we can't find a difference of two squares. Or can we? How about this?!

$$\big(x + \sqrt{-2}\big)\big(x - \sqrt{-2}\big) = y^3 \ .$$

This might look totally crazy as the factors on the left hand side are not integers (they are not even real numbers!). However, they are elements of the set

$$S = a + b\sqrt{-2} \mid \ a \text{ and } b \text{ are integers} \ ,$$

and it is an extraordinary fact that numbers in S behave in many ways like the usual integers. First we have a result which is very similar to that at in the Theorem on page 16.

Theorem. Suppose that p and q are numbers in S, that they have no common factor, and that their product pq is a cube. Then both p and q are cubes.

Before we can use this theorem we need to know a few things about factors in S. For a start, what does it even mean to say that p is a factor of q in S? It means that the quotient q/p is in S. For example,

$$\frac{7 + \sqrt{-2}}{3 - 2\sqrt{-2}} = 1 + \sqrt{-2} \quad \text{is in } S \ ,$$

so $3 - 2\sqrt{-2}$ is a factor of $7 + \sqrt{-2}$. On the other hand,

$$\frac{1 + 7\sqrt{-2}}{2 - 3\sqrt{-2}} = -\frac{20}{11} + \frac{17}{22}\sqrt{-2} \quad \text{is not in } S \ ,$$

so $2 - 3\sqrt{-2}$ is not a factor of $1 + 7\sqrt{-2}$.

It's probably not too surprising that the number $\sqrt{-2}$ is a particularly important element of S. We'll show that if x and y form a positive integer solution of (3) then $\sqrt{-2}$ is not a factor of x. For if it were, we should have

$$x = \sqrt{-2}\big(a + b\sqrt{-2}\big)$$

for some $a + b\sqrt{-2}$ in S; taking the complex conjugate[2] of both sides gives

$$x = -\sqrt{-2}\big(a - b\sqrt{-2}\big)\ .$$

Multiplying these last two equations, we find that

$$x^2 = 2(a^2 + 2b^2)$$

and so x is even. Hence y is also even; dividing both sides of (3) by 4 leaves a remainder of 2 on the left hand side and 0 on the right hand side, which is impossible. Thus $\sqrt{-2}$ is not a factor of x. Note the similarity of this last step to the argument on page 15.

The next step is to check for any common factors of $x + \sqrt{-2}$ and $x - \sqrt{-2}$, so that we can apply the theorem. Suppose that $a + b\sqrt{-2}$ is a factor of both these numbers; then it is a factor of their difference $2\sqrt{-2}$. (It's a factor of their sum too, but this turns out to be unimportant.) That is,

$$\big(a + b\sqrt{-2}\big)\big(c + d\sqrt{-2}\big) = 2\sqrt{-2}$$

for some $c + d\sqrt{-2}$ in S. As in the previous paragraph we can take conjugates and multiply to obtain

$$(a^2 + 2b^2)(c^2 + 2d^2) = 8\ .$$

Now note that $a^2 + 2b^2$ and $c^2 + 2d^2$ are just positive integers. So this last equation tells us that $a^2 + 2b^2$ is a factor (in the ordinary sense!) of 8, and there are just four possibilities:

$$a^2 + 2b^2 = 1,\ 2,\ 4 \text{ or } 8\ .$$

We could try to eliminate possibilities one by one, but there is a neat short cut which will wipe out three cases at a stroke. If $a^2 + 2b^2$ is even then a is even, say $a = 2e$, and

$$a + b\sqrt{-2} = \sqrt{-2}\big(b - e\sqrt{-2}\big)\ ;$$

then $\sqrt{-2}$ is a factor of $x + \sqrt{-2}$ and hence is a factor of x; but we know that this is impossible. Therefore $a^2 + 2b^2$ cannot be even, and we have $a^2 + 2b^2 = 1$, so $a^2 = 1$ and $b^2 = 0$, so (at last!)

$$a + b\sqrt{-2} = \pm 1\ .$$

[2]The complex conjugate of a number such as $a + b\sqrt{2}$ can be obtained by replacing the plus sign with a minus, i.e. $a - b\sqrt{2}$. Recall also that a and b can be zero! Ed.

What we have just shown is that $x + \sqrt{-2}$ and $x - \sqrt{-2}$ have no common factor except 1 (and -1). Since their product is a cube, each is itself a cube, and so we can write

$$x + \sqrt{-2} = \left(a + b\sqrt{-2}\right)^3 = (a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2}\,.$$

Equating real and imaginary parts[3],

$$x = a^3 - 6ab^2 \quad \text{and} \quad 1 = 3a^2b - 2b^3\,.$$

We have eliminated all the complex numbers (involving the square root of negative real numbers) from the problem and have reduced it to two equations in ordinary integers. The second of these gives a factorisation $1 = b(3a^2 - 2b^2)$. Thus b is a factor of 1, that is, $b = \pm 1$, and in each case we can calculate a, x and y. One possibility is

$$b = 1\,,\ 3a^2 - 2b^2 = 1 \quad \text{and so} \quad a = \pm 1\,,\ x = \pm 5\,,\ y = 3\,;$$

the other, $b = -1$, does not work since (check this for yourself) it does not give integral values for a, x and y. If we are looking for positive solutions we must ignore $x = -5$, and the problem is finished.

Theorem. The only solution of $x^2 + 2 = y^3$ in which x and y are positive integers is $x = 5$, $y = 3$.

Comment. In other words, the equation has no solution except for the one we found by trial and error. This is, perhaps, a surprising contrast to the case of Pythagorean triples, where we found an infinite collection of solutions.

Complications. Our determination of all solutions of Mordell's equation depended on the similarity of numbers $a + b\sqrt{-2}$ to the ordinary integers. If we investigate other equations there are a number of difficulties which may arise. Let's look briefly at two of these.

1. The problem of units. The key result we used in both of our previous investigations went something like this: Suppose that p and q are numbers with no common factor, and that their product pq is an nth power. Then both p and q are nth powers.
As we have seen, this is true if the nth powers it refers to are squares of positive integers, and also if they are cubes of numbers in S. However, in other situations the result is untrue. For example, consider *all* (not only positive) integers. We can write expressions such as

$$900 = (-9) \times (-100)\,, \tag{4}$$

and clearly the factors are not squares. This is quite easy to fix. Suppose that p and q are integers, that they have no common factor, and that their product pq is a square. Then each of p and q is plus–or–minus a square.

[3] A number like $a + b\sqrt{2}$ has two parts: the real part, a which is just a real number, and the imaginary part, which involves the square root of a negative number. Here we are comparing the different parts of the left and right hand sides of the equation. In the case of the imaginary parts, by comparing the coefficients of $\sqrt{2}$. Ed.

However, sometimes there are further difficulties. For example, in the set of numbers

$$T = a + bi \mid a \text{ and } b \text{ are integers} ,$$

where $i^2 = -1$, we have

$$(3 + i)^2 = 8 + 6i = 2(4 + 3i) . \tag{5}$$

The left–hand equality shows that $8 + 6i$ is a square; also, the factors on the right hand side have no common factor; but these factors are not squares.

Exercise. Confirm this by writing $2 = (a + bi)^2$, expanding, solving to find a and b, and showing that they are not integers.
For T, a correct version of our basic result is as follows: Suppose that p and q are in T, that they have no common factor, and that their product pq is a square. Then each of p and q is u times a square, where u is 1, -1, i or $-i$.
Indeed, the problem in example (5) can be resolved by observing that

$$2 = i(1 - i)^2 \quad \text{and} \quad 4 + 3i = -i(1 + 2i)^2 .$$

Numbers such as 1, -1, i and $-i$ in T are called *units*. They are factors of 1 because $1 = (i)(-i)$ and so on, and they are basically unimportant in factorisations. Thus, for example, we can write 21 as

$$21 = 3 \times 7 = (3i) \times (-7i) = (-3) \times (-7) = (-3i) \times (7i) ,$$

and none of these expressions is really a 'better' factorisation than the others. There are even worse problems in the set

$$U = a + b\sqrt{3} \mid a \text{ and } b \text{ are integers} .$$

Here we have

$$1 = \big(2 + \sqrt{3}\big)\big(2 - \sqrt{3}\big) = \big(7 + 4\sqrt{3}\big)\big(7 - 4\sqrt{3}\big)$$

and so all four of the factors shown are units. In fact, U has infinitely many units.

Exercise. Prove it!

Hint. First show that any power of a unit is also a unit.

A version of our key result which applies to many further sets of numbers follows.

Theorem. Suppose that p and q are elements of a set with unique factorisation, that they have no common factor, and that their product pq is an nth power. Then each of p and q is equal to a unit times an nth power.

Exercise. Consider the numbers $p = 2$ and $q = 14 - 5\sqrt{3}$ in U. Show that p and q have no common factors (except for units) and that their product is a square, but that neither p nor q is a square. Reconcile these facts with the above theorem.

2. The problem of non–unique factorisation. To clarify the above theorem we need to explain what is meant by 'a set with unique factorisation'. First, consider again the

ordinary integers. Any integer (except 0) can be decomposed into a product of *prime numbers*, those which cannot be factorised any further. For example,

$$60 = 2 \times 2 \times 3 \times 5 \, .$$

Alternatively, we could write

$$60 = 3 \times 2 \times 5 \times 2 \quad \text{or} \quad 60 = (-3) \times 2 \times (-2) \times 5 \, ;$$

but changing the order and inserting units are not very important, so in a sense these three factorisations are really the same. We shall say that 60 has only one factorisation into primes. As you may already know, this is true not only for 60 but for all non–zero integers. We do have, of course,

$$60 = 4 \times 15 = 6 \times 10 \, , \tag{6}$$

but this is a 'fake' non–unique factorisation since both products can be factorised further, and each will end up as $2 \times 2 \times 3 \times 5$.

Theorem. *The Fundamental Theorem of Arithmetic*. Any non–zero integer can be factorised into primes in one and only one way.

Exercise. What about 1 and -1?

By 'a set with unique factorisation' we mean one in which such a property holds. Thus the integers have unique factorisation; and it is possible to prove that the sets S, T and U considered above also have unique factorisation. It also turns out that the key result we have used in solving Diophantine equations is a consequence of unique factorisation.

Unfortunately, unique factorisation is by no means guaranteed when we study Diophantine equations by the above methods. If we think about a different case of Mordell's equation, $x^2 + 5 = y^3$, the approach used above would lead us to consider

$$V = \{a + b\sqrt{-5} \mid a \text{ and } b \text{ are integers} \, .$$

But consider the following:

$$6 = 2 \times 3 = \big(1 + \sqrt{-5}\big)\big(1 - \sqrt{-5}\big) \, . \tag{7}$$

If we want to reconcile these two expressions by splitting them into primes, we would start by trying to factorise 2 in V. That is, we need

$$\big(a + b\sqrt{-5}\big)\big(c + d\sqrt{-5}\big) = 2 \, ; \tag{8}$$

by the method of taking conjugates and multiplying we obtain

$$(a^2 + 5b^2)(c^2 + 5d^2) = 4 \, .$$

Thus $a^2 + 5b^2$ is a factor of 4. It is not hard to show that $a^2 + 5b^2 = 2$ is impossible; if $a^2 + 5b^2 = 1$ then $a = \pm 1$ and $b = 0$, so

$$a + b\sqrt{-5} = \pm 1 \ ,$$

which is a unit; if $a^2 + 5b^2 = 4$ then $c^2 + 5d^2 = 1$, and by the same argument $c + d\sqrt{-5}$ is a unit. Therefore (8) is not a proper factorisation, as it holds only when one of the factors is a unit. By similar means we show that 3 and $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ cannot be factorised either. Hence, (7) is a genuine example of non–unique factorisation, and is not at all like the 'fake' example (6).

In fact, the theorem at the top of page 23 does not apply at all to the set V.

Exercise. Show that $p = 2 - \sqrt{-5}$ and $q = -2 + 3\sqrt{-5}$ have no common factor in V and that pq is a square, but that neither p nor q is a square or the negative of a square.

The topic of the kinds of numbers which have unique factorisation has been the subject of an immense amount of mathematical research.

We conclude with one more look at *Fermat's Last Theorem.* For $n = 3$ we consider the equation

$$x^3 + y^3 = z^3 \ ; \tag{9}$$

if you are handy with complex numbers you can factorise this as

$$(x + y)(x + \omega y)(x + \omega^2 y) = z^3$$

where $\omega = \cos \frac{2}{3}\pi + i \sin \frac{2}{3}\pi$. To apply the above methods we need to consider

$$W = \{a + b\omega \mid a \text{ and } b \text{ are integers}\} \ ;$$

it turns out that W has unique factorisation, and the same ideas will suffice to show that (9) has no solution, though the details are far from easy. In fact all this will work if the exponent n is from 3 up to 22; unfortunately, when $n = 23$ we need to employ a set which turns out not to have unique factorisation, and the method collapses. To explain how Fermat's Last Theorem was eventually proved in its entirety would be a different, longer and much harder story.