

# Diophantine Equations: Integer Solutions

0624729

A Diophantine equation is simply an equation, with at least one variable, where we want to find integer solutions. The name comes from Diophantus of Alexandria, who was a 3rd century mathematician who studied rational solutions but for some reason his name is only associated to the integers [1]. The need for solutions to be within the integers can make simple looking equations very difficult. The comfort of the whole real line makes possible things like inverses, any non-zero division and answers that can't be written with numbers alone. Restricted to just the integers, without these basic methods, a new and completely different approach is necessary. This is despite the fact the problems are almost identical in writing.

This new approach uses number theory and develops techniques that not only solve the equation that they were meant for, but can then be used to solve other different equations. The basics rely heavily on the fundamental theorem of arithmetic. It states that all natural numbers, except the number one, can be expressed uniquely, up to order, as a product of prime numbers. Because of this, instead of having to prove something about all numbers, often we just need prove something about the primes and the result then applies to every integer.

In life we might find it difficult to acquire  $\sqrt{5}$  apples or  $\pi$  slices. Problems that require integer solutions do occur, so the motivation for developing the methods to deal with such problems is clear. Even the rational numbers are heavily related to the integers not just in being countably infinite. Often the solution for integers tells us everything about the solutions from the rational numbers, as is the case for Fermat's last theorem, which I will discuss.

The Diophantine equations I will cover in this essay will all be from  $\mathbb{Z}[x]$ . The reason for this is that although any equation can be considered Diophantine, non-polynomial functions are in general a lot less interesting from a number theory point of view, and will probably still have a solution that is derived from the polynomials discussed.

## 1 The Linear Diophantine Equation

The most basic Diophantine equation is the linear case. For the duration of this essay I will consider letters at the end of the alphabet ( $\dots x, y, z$ ) as the variables.

$$ax + by = c \quad a, b, c \in \mathbb{Z}$$

First we consider the greatest common divisor of the numbers  $a$  and  $b$ , call it  $d$ . This is equivalent to writing  $d = \gcd(a, b)$ . If a solution exists, obviously anything dividing one side of the equation will also divide the other. So  $d$ , which divides both  $a$  and  $b$ , and hence the left side of the equation, must divide

$c$  (short hand  $d \mid c$ ). If not the equality is invalid and therefore no solution exists.

By using the Euclidean algorithm, we know that there exist  $f, g \in \mathbb{Z}$  such that  $d = af + bg$ . Now if  $d \mid c$  then we can write  $c = de$  for some  $e \in \mathbb{Z}$ . Then  $c = de = afe + bge$  and taking  $x = fe$  and  $y = ge$  we have an integer solution. So a solution exists if and only  $\gcd(a, b) \mid c$ .

It would be helpful to categorise all solutions. To start, if  $x_0$  and  $y_0$  are any solution then

$$x_n = x_0 + n \cdot \frac{b}{d} \quad \text{and} \quad y_n = y_0 - n \cdot \frac{a}{d}$$

are also solutions to the equation for  $\forall n \in \mathbb{Z}$ . Substituting will show this. This means where there is one solution there are infinite solutions. Furthermore these are the only solutions, but we have to prove this.

Let  $ax_0 + by_0 = c$  be any solution. Take any other solution for the same  $a, b$  and  $c$ , call them  $x$  and  $y$ . So  $ax_0 + by_0 = c = ax + by$  and  $a(x_0 - x) + b(y_0 - y) = 0$ . Dividing by  $d = \gcd(a, b)$  and rearranging gives  $\frac{a}{d}(x_0 - x) = -\frac{b}{d}(y_0 - y)$ . The only way that  $\frac{b}{d} \mid \frac{a}{d}$  is for  $\frac{b}{d}$  to be one, as they are now coprime ( $\gcd = 1$ ). Therefore  $\frac{b}{d} \mid (x_0 - x)$ . This implies  $(x_0 - x) = n \cdot \frac{b}{d}$  for some  $n$ . Similarly for  $(y_0 - y)$ . The constant  $n$  being the same can be verified by substitution. Now any solution takes the form of above. Therefore any solution is expressible as  $x_n = x_0 + n \cdot \frac{b}{d}$  and  $y_n = y_0 - n \cdot \frac{a}{d}$ .

The linear Diophantine equation is fundamental and helps with the more difficult equations that may be encountered. The next step is to start considering the many types of equations with squared variables.

## 2 Summing Squares: Two Squares

We consider the equations of the form

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

and we want to know for what  $a$  is this equations solvable. Or in other words which numbers can be expressed as the sum of two squares. Obviously at the very least  $a \in \mathbb{N} \cup \{0\}$ .

**Theorem.** *The multiple of two numbers, that are the sum of two squares, is also the sum of two squares.*

*Proof.* We have  $a_1^2 + a_2^2 = a$  and  $b_1^2 + b_2^2 = b$  with  $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ .

$$\begin{aligned} ab &= (a_1^2 + a_2^2)(b_1^2 + b_2^2) = a_1^2 b_1^2 + a_1^2 b_2^2 + a_2^2 b_1^2 + a_2^2 b_2^2 \\ &= a_1^2 b_1^2 + a_2^2 b_2^2 - 2a_1 b_1 a_2 b_2 + 2a_1 b_1 a_2 b_2 + a_2^2 b_1^2 + a_1^2 b_2^2 \\ &= (a_2 b_2 - a_1 b_1)^2 + (a_1 b_2 + a_2 b_1)^2 \end{aligned}$$

Now  $ab = c_1^2 + c_2^2$  for  $c_1 = a_1 b_2 + a_2 b_1$  and  $c_2 = a_2 b_2 - a_1 b_1$  which belong to the integers.  $\square$

Using the fundamental theorem of arithmetic we only need to consider which primes can be expressed as the sum of two squares, and the numbers that are the sum of two squares will be those that are a product of two-square summable primes.

Obviously  $1^2 + 1^2 = 2$ , so we need only consider the odd primes. We break them into two sets.  $p \equiv 1 \pmod{4}$  and  $p \equiv 3 \pmod{4}$ . With modular arithmetic we can simplify the infinity of numbers to as many cases as we want.

All even numbers can be expressed as  $2n$  and all odd numbers as  $2n + 1$  for some  $n \in \mathbb{N}$ . Consider  $(2n)^2 = 4n^2 \equiv 0 \pmod{4}$  and  $(2n + 1)^2 = 4n^2 + 4n + 1 \equiv 1 \pmod{4}$ . It is only possible to make 0, 1 or 2 by summing two of 0 or 1. Therefore it is not possible to express any number equivalent to  $3 \pmod{4}$  and therefore any prime of the form  $4n + 3$  cannot be expressed as the sum of two squares.

**Theorem.** *Any prime equivalent to one modulo four is expressible as the sum of 2 squares.*

This proof is suggested in [9] and is much better than many other proofs that other books have provided. It uses more ring theory than number theory to start, but the two often cross paths. The rest of the proof is an application of the pigeon hole principle

First we must prove the following lemma.

**Lemma.** *For  $p = 4m + 1$ ,  $s^2 \equiv -1 \pmod{p}$  has two distinct solutions belonging to  $\mathbb{Z}_p$ .*

*Proof.* Collect the set  $\{1, 2, \dots, p - 1\} = \mathbb{Z} \setminus \{0\}$  into subsets containing the additive inverse and multiplicative inverse of every element in the set, containing at most four elements. For example  $\{x, -x, \bar{x}, -\bar{x}\}$ . Some of the four elements could be the same, hence it being possible to have less than four.

- $x \equiv -x \pmod{p}$  is impossible since  $p$  is odd.
- $x \equiv \bar{x} \pmod{p} \Rightarrow x^2 \equiv 1 \pmod{p}$  this implies one set  $\{1, p - 1\}$ .
- $x \equiv -\bar{x} \pmod{p} \Rightarrow x^2 \equiv -1 \pmod{p}$  and this may have two solutions, implying the set  $\{x_i, p - x_i\}$ . Or it may have no solutions.

Now the set  $\{1, 2, \dots, p - 1\}$ , which has  $p - 1$  elements, has been divided into sets of four and one set of two and another possible set of two. All of this was to show this last set must exist.  $p = 4m + 1$  means there must be  $4m$  elements in the first set and therefore both sets of two must exist and this includes the two solutions to  $s^2 = -1 \pmod{p}$ . Also notice that a prime of the form  $4n + 3$  has no solutions for  $s$ .  $\square$

On to the proof of the main theorem.

*Proof.* Consider all integer pairs  $(x, y)$  where  $x, y \in \{0, 1, \dots, \lfloor \sqrt{p} \rfloor\}$ . Obviously the total number of distinct pairs is  $(\lfloor \sqrt{p} \rfloor + 1)^2$ . By definition of the floor function we have that  $x < \lfloor x \rfloor + 1$  which implies  $p < (\lfloor \sqrt{p} \rfloor + 1)^2$ . Therefore we have more pairs than elements in  $\mathbb{Z}_p$ , which implies that for any  $s \in \mathbb{Z}$  at least two pairs exist with  $x - sy$  being equivalent to the same number modulo  $p$ . Call these two pairs  $(a', b')$  and  $(a'', b'')$ .

$$a' - sb' \equiv a'' - sb'' \pmod{p} \Rightarrow a' - a'' \equiv s(b' - b'') \pmod{p}$$

Set  $a = |a' - a''|$  and  $b = |b' - b''|$ , and  $(a, b) \in \{0, 1, \dots, \lfloor \sqrt{p} \rfloor\}^2$  and also  $a \equiv \pm sb \pmod{p}$ .  $a$  and  $b$  are not both zero, as that would imply that the two pairs weren't distinct. Let  $s$  be one of the solutions which we have shown to exist by the above lemma.  $s^2 \equiv -1 \pmod{p}$

$$\begin{aligned} a \equiv \pm sb \pmod{p} &\Rightarrow a^2 \equiv s^2 b^2 \pmod{p} \\ \Rightarrow a^2 \equiv -b^2 \pmod{p} &\Rightarrow a^2 + b^2 \equiv 0 \pmod{p} \end{aligned}$$

$0 < a^2 + b^2 < 2p$  from the conditions of  $a$  and  $b$ , and  $a^2 + b^2 = np$  from above. This gives no other option but to have  $n = 1$ .  $a^2 + b^2 = p$  and we are done.  $\square$

One final theorem is necessary to prove which numbers cannot be expressed as the sum of four squares.

**Theorem.** [9] *If a number  $a = b^2 + c^2$ , with  $p$  being a prime that divides  $a$ , such that  $p = 4n + 3$ . Then  $p^2$  divides  $a$ .*

*Proof adapted from [9].* If  $p \mid a$  but  $p$  does not divide both  $a$  and  $b$ , then without loss of generality,  $b \not\equiv 0 \pmod{p}$  then,  $\bar{b}$ , the multiplicative inverse of  $b$  exists. Using that  $b^2 + c^2 \equiv 0 \pmod{p}$ , and then multiplying by  $\bar{b}^2$ , we get that

$$\bar{b}^2 b^2 + \bar{b}^2 c^2 \equiv 0 \pmod{p} \Rightarrow (\bar{b}c)^2 + 1 \equiv 0 \pmod{p}$$

This would give  $(\bar{b}c)^2 \equiv -1 \pmod{p}$ , which we have already proved cannot happen for  $p = 4n + 3$ , in the proof of the previous lemma.

Since  $p \mid b$  and  $p \mid c$ ,  $a = b^2 + c^2 = (pd)^2 + (pe)^2 = p^2 d^2 + p^2 e^2 = p^2 (d^2 + e^2)$  now it is obvious that  $p^2 \mid a$   $\square$

As a consequence of this theorem, to decide whether a number can be expressed as the sum of four squares, we only need to consider its expression in terms of primes. A number is two-square summable if and only if the primes equivalent to three modulo four are to an even power.

### 3 Three Squares

$$x^2 + y^2 + z^2 = a$$

Which numbers are expressible as the sum of three squares? Obviously all numbers that are the sum of two squares are also the sum of three squares. Unfortunately with three squares we lose closure under multiplication. For example  $5 = 2^2 + 1^2 + 0^2$  and  $3 = 1^2 + 1^2 + 1^2$  but 15 is not expressible as the sum of three squares. In place of this there is this useful theorem.

**Lemma.** *If a number,  $n$ , is expressible as the sum of three squares and  $n \mid 4$ , then  $\frac{n}{4}$  is also expressible as the sum of three squares.*

*Proof.*

$$n = 4a = n_1^2 + n_2^2 + n_3^2$$

Assume that at least one of  $n_1$ ,  $n_2$  and  $n_3$  is odd. Since  $n \equiv 0 \pmod{4}$  then  $n_1^2 + n_2^2 + n_3^2 \equiv 0 \pmod{4}$ . Assume without loss of generality that  $n_3$  is odd.

Then  $n_1^2 + n_2^2 \equiv 3 \pmod{4}$ . We already know that this is impossible, as a square can only be equivalent to 0 or 1 modulo 4. Hence we have contradiction. All of  $n_1, n_2$  and  $n_3$  are even. Therefore set  $n_1 = 2a_1, n_2 = 2a_2$  and  $n_3 = 2a_3$ . Now  
 $n = 4a = 4a_1^2 + 4a_2^2 + 4a_3^2$  and  $a = a_1^2 + a_2^2 + a_3^2$   
 $a = \frac{n}{4}$  hence it is the sum of three squares.  $\square$

Now we try to find which numbers cannot be decomposed into three squares in a similar way to the two squares case, this time modulo eight.

**Lemma.** *If  $n \equiv 7 \pmod{8}$  then it is not expressible as the sum of three squares.*

*Proof.*  $(2n)^2 = 4n^2 \equiv 0$  or  $4 \pmod{8}$  and  $(2n+1)^2 = 4n(n+1) + 1 \equiv 1 \pmod{8}$  only as one of  $n$  and  $n+1$  will always be even.

Next  $0+0+0=0, 1+0+0=1, 1+1+0=2, 1+1+1=3, 4+0+0=4, 4+1+0=5, 4+1+1=6, 4+4+1=9 \equiv 1 \pmod{8}$  and  $4+4+4=12 \equiv 4 \pmod{8}$ . Therefore it is not possible to get 7 from three of 0, 1 and 4.  $\square$

Combining the above proves the converse of the following theorem.

**Theorem.** *A number is expressible as the sum of three squares if and only if it is not equal to  $4^x(8y+7)$   $x, y \in \mathbb{N}$ .*

Proving this is much more difficult than what we have already done. I will not give the proof here as it is apparently very lengthy. These steps were suggested as exercises in [1] p201-2.

## 4 Four Squares

Again we have  $w^2 + x^2 + y^2 + z^2 = a$  and we want to know for which  $a$  the equation is solvable using the integers. Helping greatly again is the closure of the set of four-square summable numbers under multiplication.

**Theorem.** *The product of two numbers that are expressible as the sum of four squares is also expressible as the sum of four squares.*

*Proof.*  $a = a_1^2 + a_2^2 + a_3^2 + a_4^2$  and  $b = b_1^2 + b_2^2 + b_3^2 + b_4^2$   $ab = (a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = \sum_{i=1}^4 \sum_{j=1}^4 a_i b_j = (a_1 b_1 + a_2 b_2 + a_3 b_3 + a_4 b_4)^2 + (a_1 b_4 - a_2 b_3 + a_3 b_2 - a_4 b_1)^2 + (a_1 b_2 - a_2 b_1 - a_3 b_4 + a_4 b_3)^2 + (a_1 b_3 + a_2 b_4 - a_3 b_1 - a_4 b_2)^2$  Now  $ab$  has been expressed as a sum of four squares and we have closure.  $\square$

Due to the fundamental theorem of arithmetic, all numbers are the product of prime numbers. So if we can prove that two and the odd primes can be expressed as the sum of four squares, combined with the above theorem, we have proved that all numbers can be expressed in such a way.  $2 = 1^2 + 1^2 + 0^2 + 0^2$  is easy. The odd primes as you may guess are a bit more difficult.

**Theorem.** *Odd primes can be expressed as the sum of four squares.*

*Proof adapted from [1].*  $p$  is an odd prime.

To start the proof first we need to show that  $\mathbb{Z}_p$  has exactly  $\frac{p+1}{2}$  squares modulo  $p$ . Note that zero is always a square of itself for any  $p$ .  $a \not\equiv -a \pmod{p}$  as  $p$  is odd, but  $a^2 = (-a)^2$ . So at most half of the  $p-1$  non-zero elements

can be distinct squares. Assume that two different elements are not additive inverses but result in the same square. Then

$$b^2 \equiv c^2 \pmod{p} \Rightarrow (b+c)(b-c) = b^2 - c^2 \equiv 0 \pmod{p}$$

and  $p$  must divide one of  $(b+c)$  and  $(b-c)$ , because it is prime. If  $p \mid (b+c)$  then  $b+c \equiv 0 \pmod{p}$  and  $c$  is the additive inverse of  $b$ . Otherwise  $p \mid (b-c)$  then  $b-c \equiv 0 \pmod{p} \Rightarrow b \equiv c \pmod{p}$  making  $b$  and  $c$  the same element. Therefore there must be exactly  $\frac{p+1}{2}$  square elements in  $\mathbb{Z}_p$ .

The set  $\{x \in \mathbb{Z}_p \mid x = -1 - y^2, y \in \mathbb{Z}_p\}$  also has  $\frac{p+1}{2}$  elements because each square element results in a distinct element in the above set. Since the set of the squares of  $\mathbb{Z}_p$  and the set above both have more than half of the elements of  $\mathbb{Z}_p$  there must be at least one element in both. Call this element  $a$ .  $a \equiv b^2 \equiv -1 - c^2 \pmod{p}$  for some  $b, c \in \mathbb{Z}_p$ . Set  $b$  and  $c$  so  $|b|, |c| < \frac{p}{2}$ . Now  $b^2 + c^2 + 1 \equiv 0 \pmod{p}$ . We now know  $b^2 + c^2 + 1 = np$  for some  $n$ .  $np = b^2 + c^2 + 1^2 + 0^2$ .  $np = b^2 + c^2 + 1 \leq 2(\frac{p}{2})^2 + 1 = \frac{p^2}{2} + 1 < p^2 \Rightarrow np < p^2$ , therefore  $n < p$ .

There must exist a smallest positive  $m < p$  such that  $mp = i_1^2 + j_1^2 + k_1^2 + l_1^2$  as we already know one such example. If  $m = 1$  then  $p$  is the sum of four squares and we are done. So we assume  $m > 1$ .

If  $m$  were even, then four, two or none of  $i_1, j_1, k_1, l_1$  would be odd. This means they could be collected into pairs of odds or evens. That would restrict to the integers a similar equation to

$$\begin{aligned} \left(\frac{i_1 + j_1}{2}\right)^2 + \left(\frac{i_1 - j_1}{2}\right)^2 + \left(\frac{k_1 + l_1}{2}\right)^2 + \left(\frac{k_1 - l_1}{2}\right)^2 &= \\ = \frac{i_1^2 + j_1^2 + k_1^2 + l_1^2}{2} &= \frac{m}{2} \cdot p \end{aligned}$$

but since  $m$  is the smallest positive integer this cannot happen, so  $m$  must be odd.

$m$  being odd means we can find  $|i_2|, |j_2|, |k_2|, |l_2| < \frac{m}{2}$  with  $i_1 \equiv i_2 \pmod{m}$  and so on. The inequality is not strict if  $m$  can be even.

$$i_2^2 + j_2^2 + k_2^2 + l_2^2 \equiv i_1^2 + j_1^2 + k_1^2 + l_1^2 \equiv 0 \pmod{m}$$

Now for some  $q$ ,  $i_2^2 + j_2^2 + k_2^2 + l_2^2 = qm$  and  $qm = i_2^2 + j_2^2 + k_2^2 + l_2^2 < 4(\frac{m}{2})^2 = m^2$  implies that  $q < m$ .

$$qm \cdot mp = (i_2^2 + j_2^2 + k_2^2 + l_2^2)(i_1^2 + j_1^2 + k_1^2 + l_1^2)$$

which using the formula from the theorem used to prove closure gives

$$\begin{aligned} m^2 qp &= (i_1 i_2 + j_1 j_2 + k_1 k_2 + l_1 l_2)^2 + (i_1 j_2 - j_1 i_2 - k_1 l_2 + l_1 k_2)^2 \\ &\quad + (i_1 k_2 + j_1 l_2 - k_1 i_2 - l_1 j_2)^2 + (i_1 l_2 - j_1 k_2 + k_1 j_2 - l_1 i_2)^2 \end{aligned}$$

By definition of  $i_2$  and so on

$$i_1 i_2 + j_1 j_2 + k_1 k_2 + l_1 l_2 \equiv i_2^2 + j_2^2 + k_2^2 + l_2^2 \equiv 0 \pmod{m}$$

and

$$i_1 j_2 - j_1 i_2 - k_1 l_2 + l_1 k_2 \equiv i_2 j_2 - i_2 j_2 - k_2 l_2 + k_2 l_2 \equiv 0 \pmod{m}$$

and similar for the rest.

So each of the squares is divisible by  $m$  and hence  $m^2$  and by dividing through by  $m^2$  we can find an expression for  $qp$  with four squares. This again contradicts the minimal property of  $m$  because  $q < m$ . Therefore the  $n$  from the beginning must be one. We had an expression for  $p$  as the sum of four squares all along.  $\square$

## 5 Waring's Problem

Constructing numbers from squares is a special case of Waring's problem. Instead of just square numbers Edward Waring considered the general case, thinking about cubes, fourth power numbers and higher. We might wonder how many  $k$ th power numbers it takes to sum any natural number. The maximum number of  $k$ th power positive numbers necessary to construct any number from the naturals is denoted  $g(k)$ . It is likely that Waring used tables of numbers to determine  $g(k)$ , not a method that would stand up to scrutiny today. So in 1906 Hilbert proved that  $g(k)$  exists for all  $k$ , but his proof didn't give any hint to a method that could be used to find such a number [5].

A further aspect of this problem is to think about the minimum number of  $k$ th powers necessary to express any number from the naturals, this number is denoted  $G(k)$ . Obviously since the number one will always be expressible as one  $k$ th power it is important that we stipulate that  $G(k)$  is the minimum for sufficiently large numbers. This property is not very evident from the case of  $k = 2$ , which is the sums of squares case. This is because  $g(2) = G(2) = 4$ .  $G(2) = 4$  because  $8k + 7$  is always a sum of at least four squares for all  $k$ . As we have proven.

## 6 Pythagorean Triples

Different from the previous problems but more traditionally Diophantine are the Pythagorean triples.

A Pythagorean triple is a set of three integers which satisfy  $x^2 + y^2 = z^2$ . They are so called because of Pythagoras and his right angled triangles. A Pythagorean triple gives the lengths in a right angled triangle, the largest value being that of the hypotenuse. Obviously if any of  $x$ ,  $y$  or  $z$  were zero the problem would be trivial, so this is discounted. Also any negative element of a Pythagorean triple can easily give a positive Pythagorean triple by squaring out the minus and vice versa, so it is better to concentrate on only the positive solutions.

We want to categorise all possible positive Pythagorean triples. To start with we note that a Pythagorean triple multiplied by any number is also a Pythagorean triple. So what is needed is to find all solutions that are not a multiple of anything. We call these solutions primitive. A primitive Pythagorean triple,  $\{a, b, c\}$  will have  $\gcd(a, b, c) = 1$ . Otherwise it would be a multiple of the  $\gcd(a, b, c)$ .

Assume  $\{a, b, c\}$  is a primitive triple. Remembering  $(2n)^2 = 2(2n^2)$  and  $(2n + 1)^2 = 2 \cdot 2n(n + 1) + 1$ . This proves squaring keeps even numbers as even and odd numbers as odd. If  $a$  and  $b$  are even then  $c$  must be even by  $a^2 + b^2 = c^2$ .

If this were true they would be all even and hence divisible by two. If  $a$  and  $b$  are both odd then  $c^2 \equiv 2 \pmod{4}$ , which is impossible as  $(2n+1)^2 \equiv 1 \pmod{4}$  and  $(2n)^2 \equiv 0 \pmod{4}$ . So one of  $a$  and  $b$  is odd and the other even. This means  $c$  is also odd. Without loss of generality, assume  $b$  is even. Rearranging we get

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

$c$  and  $a$  are odd, so the sum and their difference are divisible by two. Dividing everything by four overall results in

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

Consider  $\gcd\left(\frac{c-a}{2}, \frac{c+a}{2}\right) = d$ . By above  $d^2 \mid b^2$ , so  $d \mid b$ . Since  $d$  divides  $\frac{c-a}{2}$  and  $\frac{c+a}{2}$ ,  $d$  must also divide their sum  $\left(\frac{c-a}{2} + \frac{c+a}{2} = c\right)$  and their difference  $\left(\frac{c+a}{2} - \frac{c-a}{2} = a\right)$ . So  $d$  divides  $a$ ,  $b$  and  $c$ . Therefore  $d = \gcd(a, b, c) = 1$ . Now since two coprime numbers are multiplied together to make a square, they themselves must be squares. This is easy to show by considering the prime composition of the numbers involved. Finally say  $\frac{c+a}{2} = i^2$  and  $\frac{c-a}{2} = j^2$ . Now  $b = 2ij$ ,  $a = i^2 - j^2$  and  $c = i^2 + j^2$ . Since  $c$  is odd, one of  $i$  and  $j$  is odd and the other even.  $a$  is positive, which also means  $i > j$ .

$i > j$ ,  $\gcd(i, j) = 1$ , one of  $i$  and  $j$  is odd and the other even,

$$a = i^2 - j^2 \quad b = 2ij \quad c = i^2 + j^2$$

Since all of the above was derived from assuming  $\{a, b, c\}$  was any primitive triple, all Pythagorean triples can be expressed in the same way as above. Substituting proves that it is still a Pythagorean triple and we have categorised all primitive, and hence all, Pythagorean triples.

## 7 Fermat's Last Theorem

In his copy of Bachet's translation of *Arithmetica* by Diophantus, in the margin next to the Pythagorean triples, Fermat wrote in Latin:

*However, it is impossible to write a cube as a sum of two cubes, a fourth power as a sum of two fourth powers, and, in general, any power beyond the second as a sum of two similar powers. For this I have discovered a truly wonderful proof, but the margin is too small to contain it.* [5], p167

This was the birth of Fermat's last theorem. A problem that would be beyond mathematicians for the next three hundred years [5].

**Theorem** (Fermat's Last Theorem).  $x^n + y^n = z^n$  has no positive solution for  $n \geq 3$ , where  $xyz \neq 0$

It is, in fact, widely disputed that Fermat himself did have a proof [5]. Over the years many thousands of mathematicians have produced "proof" of this statement ([7], p 5), none of which is considered correct. However, due to the difficulty of the problem, and hence the complexity of proof, it is very difficult to check the validity of such proof. Most famously Lamé announced his proof in 1847. His proof of the equation's insolvability used algebraic numbers to factorise the first half of the equation. The mistake he made was assuming that

elements of the sub-ring  $\mathbb{Z}[\zeta]$  had a *unique* prime power factorisation. This is certainly true for  $\mathbb{Z}$ , but not in the particular subring he was using.

Fermat's Last Theorem doesn't have immediate consequences if it is proved or disproved. The interest in a proof is more because of the challenge. Of course the effort hasn't been useless, because of the search, great advances have been made in number and group theory. An example of one such advance is the idea of ideals. Without the effort such development might not have been achieved. Advances in any field could lead to new or better methods for dealing with other problems. So it is usually beneficial for unsolved problems to be attempted or else development could become difficult.

As previously mentioned the rational numbers are heavily linked to the integers. Fermat's last theorem is an example of this. Imagine any rational solution to Fermat's last theorem.

$$\left(\frac{a}{d}\right)^n + \left(\frac{b}{e}\right)^n = \left(\frac{c}{f}\right)^n \quad a, b, c, d, e, f \in \mathbb{Z} \setminus \{0\} \quad n \geq 3$$

Multiplying both sides by  $(def)^n \neq 0$  gives

$$(aef)^n + (bdf)^n = (cde)^n$$

which is an integer solution to Fermat's last theorem. So every rational solution gives us an integer solution. If we assume Fermat's last theorem to be true for all integers then there is also no rational solution to  $x^n + y^n = z^n$ . If there was, then it would be possible to find an integer solution, and hence contradiction.

If we can have  $n = ab$ ,  $a, b \in \mathbb{N} \setminus \{1\}$ ,

$$x^n + y^n = z^n \iff x^{ab} + y^{ab} = z^{ab} \iff (x^a)^b + (y^a)^b = (z^a)^b$$

and there is a solution for some smaller  $n = b$ . We will always be able to factorise a number  $n \geq 3$  into two smaller natural numbers, unless  $n$  is prime. If  $n$  is not prime and we have a solution, then we can find a solution where  $n$  is prime by the above method. Any  $n \geq 3$  is divisible by an odd prime or four (possibly  $n$  itself). Therefore if we can prove that when  $n$  is 4 or an odd prime  $x^n + y^n = z^n$  is unsolvable. Then we have proved Fermat's last theorem. This is easier said than done, but it is still simpler.

## 8 Descent and n=4

Fermat pioneered a method of proof known as infinite descent. He claimed that all of his proofs used it ([4], p8). It is used to disprove an assumption about positive whole numbers. Assuming a property to be true for any one positive number, it is then necessary to prove that it then holds for a strictly smaller whole number. This would imply that there existed an infinitely descending sequence of positive whole numbers, all with this property we're trying to disprove. It's impossible to have an infinite set of strictly decreasing whole numbers, so therefore the property cannot hold for any number. This is the method of infinite descent. The difficult part of this method is finding the descent, showing that it must hold for a strictly smaller positive integer.

The method of infinite descent can be used to prove Fermat's last theorem for the case when  $n = 4$ . We want to prove  $x^4 + y^4 = z^4$  is impossible with

$x, y, z \in \mathbb{Z} \setminus \{0\}$ . Also note that any negative solution will easily give rise to a positive solution. So we are looking for positive solutions only.

Any solution to  $x^4 + y^4 = z^4$  would also mean there was a solution to  $x^4 + y^4 = w^2$  by taking  $w = z^2$ .

**Lemma.** *No positive integer solution exists for  $x^4 + y^4 = w^2$*

*Proof.* Assume a solution exists, call it  $x_0, y_0$  and  $w_0$ . Let  $d = \gcd(x_0, y_0)$ . Take  $x_1 = \frac{x_0}{d}, y_1 = \frac{y_0}{d}$  and  $w_1 = \frac{w_0}{d^2}$ . Notice that these are all still integers.

$x_1^2, y_1^2$  and  $w_1$  is a primitive Pythagorean triple. Their greatest common divisor now equal to one. Assuming without loss of generality that  $y_1$  is the even part of the triple, it is possible to express them as

$$x_1^2 = i^2 - j^2 \quad y_1^2 = 2ij \quad w_1 = i^2 + j^2$$

with  $\gcd(i, j) = 1$ , only one of  $i$  and  $j$  can be odd,  $i > j$

From this also note that  $x_1^2 + j^2 = i^2$  is also a triple, from rearranging the first equation. Again we can express this second triple using the Pythagorean triple formula. Since  $x_1$  is odd,  $j$  must be even.

$$x_1 = k^2 - l^2 \quad j = 2kl \quad i = k^2 + l^2$$

with the same conditions applying to  $k$  and  $l$ .

From the final equation,  $i = k^2 + l^2$ , we will show that  $i, k$  and  $l$  are square numbers.

$y_1$  and  $j$  are even. So  $\frac{y_1}{2}$  and  $\frac{j}{2}$  are integers and  $(\frac{y_1}{2})^2 = i \cdot \frac{j}{2}$  from the first set of triple equations. Now a square number is equal to two coprime numbers multiplied together. This means that  $i$  and  $\frac{j}{2}$  are square numbers.

Using the same logic again, with the second Pythagorean triple  $\frac{j}{2} = kl$ .  $k$  and  $l$  must be square numbers. Finally that means we can set  $w_2^2 = i, x_1^2 = k$  and  $y_2^2 = l$ , with  $w_2^2 = x_2^4 + y_2^4$ .

$$w_1 = i^2 + j^2 > i^2 \geq i = w_2^2 \geq w_2$$

So  $w_1 > w_2$ . But we can apply the same logic again to get another solution to  $x^4 + y^4 = w^2$ , say  $(x_3, y_3, w_3)$  with  $w_3 < w_2$ . We could keep applying these steps as many times as we want. So if a solution to  $x^4 + y^4 = w^2$  exists then we can construct an infinite, strictly decreasing, sequence of positive integers. Hence contradiction by the method of infinite descent. No solution to  $x^4 + y^4 = w^2$  can exist.  $\square$

Any solution to  $x^4 + y^4 = z^4$  means a solution to  $x^4 + y^4 = w^2$  would exist. Therefore no solutions to Fermat's last theorem are possible in the  $n = 4$  case.

## 9 n=3

In all proof of the odd primes it is necessary to also consider the possible negative solutions. Euler gave a proof of the  $n = 3$  case using Fermat's method of infinite descent, but he commented in one of his letters that the proof was different from the case of  $n = 4$  and that it would be extremely difficult to generalise the proof. The  $n = 4$  case is trivial in comparison to the proofs of other odd primes. Euler's proof illustrates this. It is included in [4].

## 10 Fermat's Last Theorem: The Proof

Fermat's last theorem was finally proven in 1993 [1]. The proof stemmed from the study of elliptic curves. Elliptic curves are polynomials of the form  $f(x, y) = 0$  which have the additional condition of being a torus (similar to a doughnut shape).

A conjecture by Taniyama and Shimura stated that an elliptic curve with rational coefficients must be modular. This conjecture, with work from Frey, Ribet and Serre, was shown to imply Fermat's last theorem. Then in 1993, Andrew Wiles proved all parts of Taniyama and Shimura's conjecture that were necessary for proving Fermat's last theorem and hence finished the proof once and for all. People wanting to know more about the proof of Fermat's last theorem should first read [1] p234-7.

In solving the linear Diophantine equations, we learned how to use the greatest common divisor and the fundamental theorem of arithmetic. Then, from studying the sums of squares developed the use of modular arithmetic and other methods of proof. Combining these tools made categorising the Pythagorean triples possible. This coupled with the method of infinite descent built up to a proof of Fermat's last theorem for the case of  $n = 4$ . This is just a handful of the methods used to solve Diophantine equations. They can contribute to other more difficult Diophantine equations, but often it is not enough and new methods must be created.

## References

- [1] Gareth A. Jones & J. Mary Jones: *Elementary Number Theory*, Springer, 1998
- [2] Graham Everest & Thomas Ward: *An Introduction To Number Theory*, Springer, 2005
- [3] Kenneth Ireland & Michael Rosen: *A Classical Introduction To Modern Number Theory*, Springer-Verlag, 1990
- [4] Harold M. Edwards: *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*, Springer-Verlag, 1977
- [5] James E. Shockley: *Introduction To Number Theory*, Holt Rinehart and Winston Inc., 1967
- [6] Calvin T. Long: *Elementary Introduction To Number Theory*, Heath and Company, 1972
- [7] Harold M. Stark: *An Introduction To Number Theory*, 1970
- [8] Tryggt Nagell: *Introduction To Number Theory*, 1964
- [9] Martin Aigner & Günter M. Ziegler: *Proofs from THE BOOK*, Springer, 2004, §4 only