Resource E

Fermat's Last Theorem for $n = 4$

E.1 Pythagorean triples

The equation

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

certainly has solutions, eg $(3, 4, 5)$ and $(5, 12, 13)$. This does not contradict Fermat's Last Theorem, of course, since that only asserts there is no solution *if* $n > 2$.

Pythagoras already knew that this equation (with $n = 2$) had an infinity of solutions; and Diophantus later found all the solutions, following the technique below.

In the first place, we may assume that

$$\gcd(x, y, z) = 1.$$

We may also assume that $x, y, z > 0$. We shall use the term *Pythagorean triple* for a solution with these properties.

Note that modulo 4

$$x^2 \equiv \begin{cases} 0 \bmod 4 & \text{if } x \text{ is even,} \\ 1 \bmod 4 & \text{if } x \text{ is odd.} \end{cases}$$

It follows that x and y cannot both be odd; for then we would have $z^2 \equiv 2 \bmod 4$, which is impossible. Thus just one of x and y is even; and so z must be odd. We can assume without loss of generality that x is even, say $x = 2X$. Our equation can then be written

$$4X^2 = z^2 - y^2 = (z + y)(z - y).$$

We know that $2 \mid z+y,\ 2 \mid z-y$, since y, z are both odd. On the other hand no other factor can divide $z+y$ and $z-y$:

$$\gcd(z+y, z-y) = 2.$$

For

$$d \mid z+y,\ z-y \Longrightarrow d \mid 2y,\ 2z.$$

It follows that

$$z+y = 2u^2, \quad z-y = 2v^2, \quad x = 2uv.$$

Thus

$$(x, y, z) = (2uv, u^2 - v^2, u^2 + v^2).$$

where $\gcd(u, v) = 1$. Note that just one of u, v must be odd; for if both were odd, x, y, z would all be even.

Every Pythagorean triple arises in this way from a unique pair (u, v) with $\gcd(u, v) = 1$, $u > v > 0$, and just one of u, v odd. The uniqueness follows from the fact that

$$(u+v)^2 = z + x, \quad (u-v)^2 = z - x.$$

For this shows that x, y, z determine $u+v$ and $u-v$, and therefore u and v.

E.2 The Case $n = 4$

The only case of his "Theorem" that Fermat actually proved, as far as we know, was the case $n = 4$:

$$x^4 + y^4 = z^4.$$

His proof was based on a technique which he invented: *the Method of Infinite Descent*. Basically, this consists in showing that from any solution of the equation in question one can construct a second, smaller, solution.

Actually, we are going to apply this to the Diophantine equation

$$x^4 + y^4 = z^2.$$

If we can show that this has no solution in non-zero integers, then the same will be true *a fortiori* of Fermat's equation with $n = 4$.

Suppose (x, y, z) is a solution of this equation. As before we may and shall suppose that $\gcd(x, y.z) = 1$. Evidently (x^2, y^2, z) is then a Pythagorean triple, and so can be expressed in the form (swapping x, y if necessary)

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

where a, b are positive integers with $\gcd(a, b) = 1$. Since x is even, $4 \mid x^2$, and therefore just one of a and b must be even.

If a were even and b were odd, then $a^2 - b^2 = 3 \bmod 4$, so the second equation $y^2 = a^2 - b^2$ would be untenable. Thus b is even, and so from the first equation $x^2 = 2ab$ we can write

$$a = u^2, \ b = 2v^2,$$

where $\gcd(u, v) = 1$, and $u, v > 0$.

The second equation now reads

$$y^2 = u^4 - 4v^4.$$

Thus

$$4v^4 + y^2 = u^4,$$

and so $(2v^2, y, u^2)$ is a Pythagorean triple. It follows that we can write

$$2v^2 = 2st, \ y = s^2 - t^2, \ u^2 = s^2 + t^2,$$

where $\gcd(s, t) = 1$. From the first equation we can write

$$s = X^2, \ t = Y^2,$$

where $\gcd(X, Y) = 1$, and $X, Y > 0$; and so on writing Z for u the third equation reads

$$X^4 + Y^4 = Z^2,$$

which is just the equation we started from. So from any solution (x, y, z) of the equation

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

with $\gcd(x, y, z) = 1$, $x, y > 0$ and x even, we obtain a second solution (X, Y, Z) with $\gcd(X, Y, Z) = 1$, $X, Y > 0$ and X even, where

$$x = 2X^2Y, \ y = X^4(1 - 4Y^4), \ z = X^4(1 + 4Y^4).$$

The new solution is evidently smaller than the first in every sense. In particular,

$$X < x;$$

so our infinite chain must lead to a contradiction, and Fermat's Last Theorem is proved for $n = 4$.

Exercises 1 Discriminant

** 1. Show that the even number in a Pythagorea triple $\{x, y, z\}$ is divisible by 4.

** 2. Show that one entry in every Pythagorea triple is divisible by 3.

** 3. Does there exist a Pythagorea triple $\{x, y, z\}$ with hypotenuse $z = 25$?

*** 4. Find all Pythagorea triples $\{x, y, z\}$ with hypotenuse z divisible by 7.

**** 5. Show that the hypotenuse z of a Pythagorea triples $\{x, y, z\}$ is either a prime of the form $4k + 1$ or a product of such primes

*** 6. Can you find consecutive odd numbers in two Pyhagorean triples?

** 7. Which odd integers can appear as the smaller odd number in a Pythagorean triple?

** 8. Find two Pythagorean triples with the same even entry.

**** 9. Can you find positive integers a, b, c such that $a^2 + b^2,\ b^2 + c^2,\ c^2 + a^2$ are all perfect squares?

** 10. Can two consecutive even numbers appear in the same Pythagorean triple?

**** 11. Show that the equation $x^4 - y^4 = z^2$ has no solution in positive integers.