# CHAPTER IV

## Fermat's last theorem

## 4.1. Introduction.

In this chapter we provide two proofs of Fermat's last theorem. The first uses methods available to Fermat, although we cannot be sure whether or not Fermat used them in his proof, if indeed there was a correct one. There have been several recent attempts in the literature to prove Fermat's last theorem by classical methods, although I am not aware of the proof given here being publicised elsewhere. The reader familiar with the elementary methods of [Ad09] will understand why I have tried to find a proof this way. Of course this path is notorious for false proofs. The second uses the modularity theorem and is equivalent to the proof of Taylor and Wiles. We show that every semistable elliptic curve is modular.

## 4.2. A proof of Fermat's last theorem by elementary methods.

We first investigate a generalisation of 'Pythagorean triples', which are a representation of whole numbers satisfying the Pythagoras theorem. We can transform from the whole number, or more generally integer, variables x, y and z in Pythagoras's theorem to variables n and m. Traditionally n and m are thought of as being natural numbers, or more generally integers, but we will extend this idea to n and m real numbers whilst retaining x, y and z as nonzero integers, and discover the properties of these real numbers. We are seeking representations of x and y which hold in all cases, so that when we come across equation (5) below we can use these representations to prove (5) does not hold except in a trivial case.

**Lemma 4.2.1.** *An integer Pythagoras theorem*

$$x^2 + y^2 = z^2 \tag{1}$$

*is satisfied only under the constraints*

$$x = n^2 - m^2 \tag{2}$$

$$y = 2nm \tag{3}$$

$$z = n^2 + m^2. \tag{4}$$

*Proof*. Let (2) to (4) hold, then (1) is satisfied as

$$(n^4 - 2n^2m^2 + n^4) + 4n^2m^2 = (n^4 + 2n^2m^2 + m^4).$$

Conversely let (1) hold. For positive natural numbers $z > x$ if

$$x = A - B$$

$$z = A + B,$$

which is always possible, then

$$x^2 = A^2 - 2AB + B^2$$

$$z^2 = A^2 + 2AB + B^2$$

and thus

$$y^2 = 4AB,$$

which is just (2), (3) and (4) with $A = n^2$ and $B = m^2$. □

This Pythagoras theorem holds for natural numbers if and only if n and m are both natural numbers or say $tn = m$ for t a nonnegative integer where n is a square root. Otherwise, say $n^2$ is not a natural number, this means $x + z$ is not a natural number, a contradiction. But if for all t, $tn \neq m$, this means m is not a root of a whole number and y is not a natural number. □

If the integer Pythagoras theorem holds, then two values of the lengths must be odd and one of the lengths is even. The formulas assume z positive, but if this happens then we can multiply x, y and z by -1, and negative values of x and y are allowed in the formula (1). In what follows we will not need to use this value of z.

Note that we cannot have

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

with x and y odd and z even, because for integers c and d, if

$$x = (2c + 1),$$
$$y = (2d + 1)$$

then

$$x^2 + y^2 = 4(c^2 + c + d^2 + d) + 2,$$

and if g is an odd number, this is of the form 2g, but if z is even, then for a natural number h,

$$z^2 = 4h$$

and so cannot be 2g. □

For a prime p >2, let

$$x^p + y^p = w^p, \qquad (5)$$

expressed in lowest terms, that is, with any natural number common factor divided out. Since y is an integer and p is odd, equation (5) includes the case

$$x^p + (-y)^p = x^p - y^p = w^p.$$

We will prove Fermat's last theorem that there are no integer solutions of (5) with $xyw \neq 0$. Then from the lemma there exists an x and y satisfying (1) such that

$$x^p + y^p = (n^2 - m^2)^p + (2nm)^p$$
$$= n^{2p} - pn^{2p-2}m^2 + [p(p-1)/2]n^{2p-4}m^4 - \ldots + pn^2m^{2p-2} - m^{2p} + 2^p n^p m^p. \qquad (6)$$

Since p is odd the last term does not correspond to any term before it.

In the first scenario, with n and m as given natural numbers, the values of n and m we will substitute in equation (5) must be coprime, because if they contain a nontrivial common factor, then x and y will contain a nontrivial common factor, and so therefore will w, which means (5) can be divided by it.

With n > m, we will prove that n and m are properly coprime, that is, $m \neq 1$. It is possible to swap round m and n if x is negative, so this is not restrictive. Assume the contrary condition that m = 1, with also n a positive integer. Since x is odd, m and n have opposite parity, so n is even, which we write as

$$n = 2r.$$

Since w is odd, we will write this as

$$w = 2s - 1.$$

Equation (5) becomes

$$[(2r)^2 - 1]^p + [4r]^p = [2s - 1]^p,$$

so expanding out by the binomial theorem and dividing by 2 gives the result that s is even. Put

$$s = 2s'.$$

Our equation has now become

$$[4r^2 - 1]^p + [4r]^p = [4s' - 1]^p.$$

Since $4r^2 - 1 > 4r$ and $4s' > 4r^2$, a minimal value of $s'$ is $r^2 + 1$. We will show this minimal value is too big. If we have

$$[4r^2 + 3]^p - [4r^2 - 1]^p = [4r]^p,$$

the expansion is

$$(4r^2)^p - (4r^2)^p + 3p(4r^2)^{p-1} + p(4r^2)^{p-1} + \ldots = (4r)^p,$$

which is clearly impossible. Thus m is properly coprime to n. □

Since y is of the form 2nm, it follows that w is coprime to m and n, otherwise x would have a common factor with m or n or both, and equation (5) would not be in lowest terms.

Then for natural numbers K and L, let

$$w = Kn + Lm \tag{7}$$

uniquely, so that by the Euclidean algorithm it is possible to find unique natural numbers Q, R, T and U such that

$$\begin{aligned} w^p &= (Kn + Lm)^p \\ &= (Qn^2 + Rn + Tm^2 + Um)^p. \end{aligned} \tag{8}$$

Then

$$\begin{aligned} w^p = {} & n^p(Qn + R)^p + pn^{p-1}m(Qn + R)^{p-1}(Tm + u) \\ & + [p(p-1)/2]n^{p-1}m^2(Qn + R)^{p-2}(Tm + u)^2 + \ldots \\ & + pnm^{p-1}(Qn + R)(Tm + u)^{p-1} + m^p(Tm + U)^p. \end{aligned} \tag{9}$$

Since $m \neq n$ (because x is not zero) and using the uniqueness of the expression (7), equating (6) and (9) gives from the first term

$$Q = 1,$$

and from the last term

$$T = -1.$$

There is a pure $n^p$ term which is $R^p$ in (9) and zero in (6), a pure $m^p$ term which is $U^p$ in (9) and zero in (6), but there exists an $n^pm^p$ term in (6) which cannot exist in (9).

This violates the unique expression (7) since if this expression is not unique, then at least two of K, n, L and m are not integers, with either the Kn product an integer, the Lm product an integer, or if not then both summed together are an integer.

Now secondly there remains to consider nt = m with n a square root. Then equation (6) holds as it was before with the terms replaced. The equation becomes

$$\begin{aligned} x^p + y^p &= (n^2 - m^2)^p + (2nm)^p \\ &= n^{2p} - pt^2n^{2p} + [p(p-1)/2]t^4n^{2p} - \ldots + pt^{2p-2}n^{2p} - t^{2p}n^{2p} + 2pt^pn^{2p}. \end{aligned} \tag{10}$$

Equation (7) becomes for the natural number w

$$w = (K + Lt)n. \tag{11}$$

Thus since n is a square root

$$(K + Lt) = un, \tag{12}$$

with u a natural number.

But now what has happened is that the equation (5) is no longer in lowest terms, since it is possible to divide it by $n^{2p}$. Thus this alternative can be discounted. □

## 4.3. The Taylor-Wiles proof of Fermat's last theorem.