CHAPTER IV

Fermat's last theorem

4.1. Introduction.

In this chapter we prove Fermat's last theorem using elementary methods. We use two methods of proof, which are mutually contradictory, thus showing that there is no solution of the Fermat equation. We then introduce sophisticated methods based on the methods of Taylor and Wiles and the modularity theorem of volume I.

4.2. Fermat's last theorem and elementary methods – first method.

Consider

$$x^p + (b - x)^p = c^p, \qquad (1)$$

and let this be in lowest terms, so that (1) cannot be divided by a nontrivial factor, meaning the factor is $\neq 1$. Let x, b and c be nonzero integers and let p be an odd prime.

The three terms in powers of p in (1) cannot all be even, because then the formula is not in lowest terms, nor can all three terms be odd, which is a 'parity mismatch' – then one side of the equation is even, and the other is odd. So two terms must be of odd parity, and one term is even.

The reason we have chosen p odd prime (p = 2 has Pythagoras theorem solutions), is that if, say, the number was the product of two numbers, pq, with p prime then we would have

$$(x^q)^p + ((b - x)^q)^p = (c^q)^p, \qquad (2)$$

which is the same case with new variables.

All terms to the power p are nonzero integers, so they can be positive or negative. A negative number to an odd power is negative. This means that all possible combinations of positive and negative numbers in (1) are available.

We intend to look at Fermat's last theorem, that there are no such solutions to (1). Our objective in this part is to show that b and c = 0 (mod p) if (1) holds. The proof we develop in the second part shows that this is not the case.

Firstly note that we may choose x odd without restricting the generality of equation (1), and also choose c either even or odd, so that if x and c are odd then (b – x) is even, so b is odd. Likewise, if b is even, then (b – x) is odd and c must also be even. Either of these choices can be made whilst maintaining the generality of (1).

The case for b and c odd is inconvenient in the proof because this includes the case b = 1, which has no further factorisation, and we will need to prove that equation (1) cannot be in lowest terms. Nevertheless, for completeness, we include a proof that b = 1 does not satisfy the conditions of (1).

Let b = 1 and c = (1 – r) where the positive magnitude, called the absolute value, of (1 – r) is |(1 – r)|. Then choosing x arbitrarily as positive in (1), (1 – x) is negative and |(1 – x)| is less than |(1 – r)| so |1 – x| is less than |c|, but |x| is greater than |c| because (1 – x) is negative, thus $|1 - x| < |c| < |x|$, a contradiction for a natural number c. This implies $b \neq 1$. □

Expanding out (1) by the binomial theorem gives

$$b^p - pb^{p-1}x + \ldots + pbx^{p-1} = c^p, \quad (3)$$

or

$$pbx[x^{p-2} - [(p-1)/2]bx^{p-3} + \ldots - b^{p-2}] = c^p - b^p. \quad (4)$$

By Fermat's little theorem, if y is an integer and p is prime, then

$$y^p - y = 0 \pmod p,$$

a notation which means

$$y^p - y = mp, \quad (5)$$

where m is an otherwise unspecified integer. This can be proved by induction. It holds when y = 0 or 1, and if we assume it for y then

$$(y+1)^p - (y+1) = y^p + p\times(\text{integer binomial terms}) + 1 - y - 1,$$

so the same equation holds for (y + 1). □

Applying this to equation (1) gives

$$c = b - np, \quad (6)$$

for some integer n. If n = 0 then dividing (4) by pbx shows that x^{p-2} has a common factor with b and hence (1) is not in lowest terms. Thus $n \neq 0$.

So using (6), equation (4) on cancelling b^p terms becomes

$$pbx[x^{p-2} - [(p-1)/2]bx^{p-3} + \ldots - b^{p-2}] = -(np)^p + np^2b[(np)^{p-2} - [(p-1)/2]b(np)^{p-3} + \ldots - b^{p-2}]. \quad (7)$$

On dividing (7) by pb

$$x[x^{p-2} - [(p-1)/2]bx^{p-3} + \ldots - b^{p-2}] = -(n^pp^{p-1}/b) + np[(np)^{p-2} - [(p-1)/2]b(np)^{p-3} + \ldots - b^{p-2}], \quad (8)$$

and considering the first term after the equals sign, because the left hand side is still an integer, so is the right. We find that b divides n^pp^{p-1}. This means that b and n^p have a common factor or b and p^{p-1} have a common factor, or both.

If $b \neq \pm n^pp^{p-1}$, then since n^pp^{p-1}/b is a whole number, it must contain n or p as a factor. In fact, we have chosen b even, and since p is odd, in this case b cannot entirely divide p^{p-1}, so that b and n^p have a common factor. If we put

$$b = fg$$
$$n^p = fh$$

where f is the highest common factor between b and n^p, we see from (8) that x^{p-1} contains the factor f, and thus x contains a nontrivial subfactor of f, call it j. Thus equation (1) cannot be in lowest terms, because b contains j, from (6) since n contains j, c contains j, and we have just said that x contains j. A more direct derivation is to note that f is even and x is odd.

Thus $b = \pm n^pp^{p-1}$. But now c in (6) contains a factor np, but by (3) cannot contain a higher factor than np because then x in (3) would be divisible by np, and (1) would not be in lowest terms. Note that $n = 2^rk$, with k odd, since b is even. Thus

$$b = \pm 2^{rp}k^pp^{p-1} \quad (9)$$

and

$$c = \pm 2^rkp(2^{r(p-1)}k^{p-1}p^{p-1} - 1). \quad (10)$$

It now follows that b = 0 (mod p) and c = 0 (mod p). □

4.2. Fermat's last theorem and elementary methods – second method.

Consider, using notation which is separate from the previous section

$$U^p - V^p = W^p, \tag{1}$$

and let this be in lowest terms, so that (1) cannot be divided by a nontrivial factor, let U, V and W be nonzero integers and let p be an odd prime.

We will write (1) as

$$(B - A)^p - (B + A)^p = 2^pC^p \tag{2}$$

where A, B and C are integers, C is nonzero, and

$$U = B - A \tag{3}$$

$$V = B + A, \tag{4}$$

which implies

$$V = U + 2A. \tag{5}$$

Since V and U are at this moment arbitrary odd numbers, an integer value of A can always be found satisfying (5).

Expanding out (2) by the binomial theorem gives

$$B^p - pAB^{p-1} + p[(p - 1)/2]A^2B^{p-2} + ... + pA^{p-1}B - A^p$$
$$- B^p - pAB^{p-1} - p[(p - 1)/2]A^2B^{p-2} - ... - pA^{p-1}B - A^p = 2^pC^p,$$

giving

$$- pAB^{p-1} - p[(p - 1)(p - 2)/3!]A^3B^{p-3} - ... - p[(p - 1)/2]A^{p-2}B^2 - A^p = 2^{p-1}C^p. \tag{6}$$

In order that U and V be odd, this means B is odd and A is even in (2), or B is even and A is odd. Then if B is even and A is odd, all terms in (6) except $-A^p$ are even, so there is a parity mismatch.

So consider the remaining case where B is odd and A is even. If A is not a power of 2, then a nontrivial factor of A divides C in (6). Let this factor be k and

$$A = A'm$$

where

$$A'k = C$$

and m does not divide C. Then on dividing by A', (6) becomes

$$- pmB^{p-1} - p[(p - 1)(p - 2)/3!]A'^2m^3B^{p-2} - ... - A'^{p-1}m^p = 2^{p-1}A'^{p-1}k^p. \tag{7}$$

On dividing again now by A'^2,

$$pmB^{p-1}/A'^2$$

is an integer. Because we have chosen the allowable general allocation p prime, then at most $A' = p$ since A'^2 cannot divide p, so A' also divides mB^{p-1}.

If a nontrivial factor A'' of A' divides B then (7) contains a common factor $A'' \neq \pm 1$, this applies to equation (2) and hence equation (1), which violates the nondivisibility condition attached to (1). Hence in this case A' divides m, say $A'j = m$, where j divides m completely, giving

$$(m/j)k = C,$$

$$mk = Cj.$$

So either m has a nontrivial factor dividing C, a contradiction, or m has no factor dividing C, but m divides j completely, again a contradiction.

This means the only scenario we have left is that A is a power of 2.

Let

$$A = 2^q,$$

with q a natural number ≥ 1, and

$$C = 2^n C',$$

with C' odd. Equation (2) now reads

$$(B - 2^q)^p - (B + 2^q)^p = 2^{(n+1)p} C'^p$$

or

$$-pB^{p-1} - \ldots - 2^{q(p-1)} = 2^{(n+1)p-1-q} C'^p. \quad (8)$$

Since all terms are always even after $-pB^{p-1}$ on the left, the above equation is odd both left and right.

We must have

$$2^{(n+1)p-1-q} = 1$$

or

$$q = (n+1)p - 1. \quad (9)$$

We will express (1) under the condition that A is a power of 2, and use Fermat's little theorem to show that this allocation gives a constraint. Equation (1) is now

$$U^p - (U + 2(2^q))^p = 2^{(n+1)p} C'^p. \quad (10)$$

We have shown that Fermat's little theorem states that for prime p and integer y

$$y^p - y = 0 \pmod p, \quad (11)$$

so that (mod p) equation (10) on substituting (9) becomes

$$-2^{(n+1)p} = 2^{(n+1)p} C' \pmod p$$

giving

$$C' = -1 \pmod p. \square \quad (12)$$

Now note that 2 to any power is not zero (mod p), and hence the right hand side of (2) is not zero (mod p). But the previous section has shown that this is zero (mod p). This contradiction proves that there are no such solutions. □

4.3. The proof using the modularity theorem.