CHAPTER IV

Fermat's last theorem

4.1. Introduction.

In this chapter we look at Fermat's last theorem using elementary methods. We use two methods of proof, which are mutually contradictory, to show 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 factor $\neq 1$, which we call a nontrivial factor. 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 an example of (1) 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 will explain the (mod p) notation now. 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

$$y^p - y = mp, \qquad (3)$$

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). □

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

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. Considering (b – x) and c independent, 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. We will choose b even. 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 ≠ 1. □

Expanding out (1) by the binomial theorem gives

$$b^p - pb^{p-1}x + \ldots + pbx^{p-1} = c^p, \quad (4)$$

or

$$pbx[x^{p-2} - [(p-1)/2]bx^{p-3} + \ldots - b^{p-2}] = c^p - b^p. \quad (5)$$

Applying Fermat's little theorem to equation (1) means it holds also (mod p), giving

$$x + (b - x) = c \pmod p$$

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

for some integer n. If n = 0 then dividing (5) by pbx shows that x^{p-2} has a common factor with b and hence (1) is not in lowest terms. Thus n ≠ 0. Also n is even, since b and c are even.

So using (6), equation (5) 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 or both. 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. Looking at equation (8) we see that the power of 2 in b precisely matches the power of 2 in n^p, otherwise because x is odd, there is a parity mismatch.

If we put

$$b = fg \quad (9)$$

$$n^p = fh \quad (10)$$

where f is the highest common factor between b and n^p, then the term

$$n^pp^{p-1}/b = hp^{p-1}/g \quad (11)$$

is a whole number ≠ 1, and since g has no common factor with h, g divides p^{p-1} completely.

If g = 1, then (9) and (10) imply that n^p and b have a nontrivial common factor containing 2^q, so that if p ≠ q then h is even, which from (11) gives a parity mismatch for odd x in (8). Thus p = q and the even factor in n is given by 2^s, and (6) implies this factor of precisely 2^s is shared by c.

If $g \neq 1$, from equation (11) g contains a factor p, therefore by (9) so does b, and since $b \neq \pm n^p p^{p-1}$, we see from (8) that if g does not contain the factor p^{p-1} then x^{p-1} contains the factor p, and thus x contains the factor p. So here equation (1) cannot be in lowest terms, because b contains p, from (6) c contains p, and we have just said that x contains p.

If g contains p^{p-1} then it equals p^{p-1}, since otherwise by (11) g divides h and f is not a common factor. Thus in this case by (9) b contains a factor of at least p^{p-1}, which implies from (6) that both b and c = 0 (mod p).

The remaining case is $b = \pm n^p p^{p-1}$. But now c in (6) contains a factor np, but by (5) cannot contain a higher factor than np because then x in (5) would be divisible by np, and (1) would not be in lowest terms. Note that $n = 2^r k$, with k odd, since b is even. Thus

$$b = \pm 2^{rp} k^p p^{p-1} \tag{12}$$

and

$$c = \pm 2^r kp(2^{r(p-1)} k^{p-1} p^{p-1} - 1). \tag{13}$$

It now follows that b = 0 (mod p) and c = 0 (mod p) in this case.

The result of all this reasoning is that either we have b and c = 0 (mod p), or the even factor of b is 2^{ps} and of c is 2^s. □

4.3. 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

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

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

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

giving

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

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

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

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

$$C = 2^nC',$$

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

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

For congruence arithmetic where p is prime, just like ordinary arithmetic, numbers fall into two distinct classes, those which are zero (mod p), when any number multiplied by such a number is zero (mod p), and those which are not zero (mod p), when any number which is not zero (mod p) multiplied by it is not zero (mod p). 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 one of the options for this is zero (mod p). This contradiction proves that there are no solutions for this option.

The remaining option is that the right hand side of (2) is 2^pC^p, which by (10) is $2^{(n+1)p}C'^p$, with C' odd. This value can be directly compared with c^p in the previous section, where c contains precisely 2^s and no greater even power of 2. This equality implies that the only value of n in (9) is $(s-1)$. Using equation (9) with $n = (s-1)$ now implies

$$q = ps - 1, \tag{13}$$

giving for equation (10) in this section,

$$U^p - (U + 2^{ps})^p = 2^{ps}C'^p. \tag{14}$$

In the previous section we found that the variable b for this option is

$$b = 2^{ps}b',$$

where we have now introduced a new variable b'. Comparing the Fermat equation (1) of the previous section with equations (1), (5) and (14) of this section, on matching terms

$$U = x \tag{15}$$

$$-(U + 2^{ps}) = 2^{ps}b' - U,$$

so

$$b' = -1. \tag{16}$$

On expanding out (14) by the binomial theorem, we obtain

$$-ps2^{ps}U^{p-1} - [ps(ps-1)/2]2^{2ps}U^{p-2} - \ldots - 2^{psps} = 2^{ps}C'^p,$$

so that on dividing by 2^{ps}

$$-psU^{p-1} - [ps(ps-1)/2]2^{ps}U^{p-2} - \ldots - 2^{ps(ps-1)} = C'^p. \tag{17}$$

Since U and C' are both odd we will write

$$C' = U + 2^rD \tag{18}$$

with D odd. Then (17) becomes

$$-psU^{p-1} - [ps(ps-1)/2]2^{ps}U^{p-2} - \ldots - 2^{ps(ps-1)} = U^p + pU^{p-1}2^rD + \ldots + 2^{rp}D^p, \tag{19}$$

which since U and D are odd implies that s is odd, and if $r \leq ps$ then

$$[U + p(s + 2^rD)]U^{p-1}$$

is divisible by 2^r, which means

$$ps = k2^t - U \tag{20}$$

for some odd k and $t \geq r$. Plugging in this value of ps for its first occurrences in (19) gives

$$-k2^tU^{p-1} - [(k2^t - U)(ps-1)/2]2^{ps}U^{p-2} - \ldots - 2^{ps(ps-1)} = (k2^t - U)U^{p-1}2^rD + \ldots + 2^{rp}D^p, \tag{21}$$

so that on dividing by 2^r, if $ps > r$, if $t > r$ the left hand side is even and the right hand side is odd, a parity mismatch. Hence if $ps > r$ then $t = r$ gives that

$$[U + (k2^r - U)(1 + 2^rD)]U^{p-1} = [(k - UD)2^r + kD2^{r+1}]U^{p-1}$$

is divisible by 2^r, which means since $(k - UD)$ is even the expression is divisible by $2^v = 2^{r+1}$. But now r has escalated and inductively increases without limit, so we must therefore assume that $ps \leq r$.

So $ps \leq r$. Incidentally, if $p < r$ with $t \geq r$ then on dividing (21) by 2^{ps} gives that the term

$$-[(k2^t - U)(p-1)/2]U^{p-2}$$

is even, otherwise there is a parity mismatch. Thus $(ps-1)/2$ is even, or to put it another way, $ps = 1 \pmod 4$.

But if $ps = r \leq t$, (20) implies that $(U + p)$ is divisible by 2^t. If $t > r$, on dividing (21) by 2^{ps} results in $(ps-1)/2 + UD$ is even, thus $(ps-1)/2$ is odd and $ps = 3 \pmod 4$, whereas if $t = r$ the first term in (21) changes this parity, so that $ps = 1 \pmod 4$.

Those aware of the Taylor-Wiles proof of Fermat's last theorem may know there appear to be incompatibilities in the spread of solutions. We will follow this line of inquiry for $ps \leq r$.

We will use equation (18) for $ps \leq r$. From (14), if we choose U positive then both sides of this equation are negative, since $U^p < U^p + 2^p$. This implies D is negative. We will deal with the absolute values of variables in describing the proof. The value of $2^{ps}|C^p|$ from (14) is then $2^{ps}|(U + 2^rD)^p|$ from (18). Since a binomial expansion to the power p has p + 1 terms, and p here is odd, we can partition the expansion of $(U + 2^rD)^p$ in pairs, as

$$\{U^p + pU^{p-1}(2^rD)\} + \{[p(p-1)/2]U^{p-2}(2^rD)^2 + \} \ldots + \{pU(2^rD)^{p-1} + (2^rD)^p\}. \quad (22)$$

From (18) we see that since $C' = -1 + np$ and $n = (s - 1)$ is even but not zero, that

$$|2^rD| - |U| > ps. \quad (23)$$

Thus if $ps \leq r$ then

$$|2^rD| - p - p|2^rD|$$

is negative, and looking at the first two items in (22), we see that

$$\{|U| - p|2^rD|\}U^{p-1}$$

is negative, and we can carry through this observation for all subsequent pairs.

For the left hand side of (17) times 2^{ps}, this can be expanded binomially as

$$-\{psU^{p-1}(2^{ps}) + [ps(ps-1)/2]U^{p-2}(2^{ps})^2\} - \ldots - \{psU(2^{ps})^{p-1} + (2^{ps})^p\}. \quad (24)$$

But on comparing (22) and (24)

$$(psU^{p-2}(2^{ps}))|U + [(ps-1)/2]|(2^{ps}) < (2^p)U^{p-1}|U + p(2^rD)|,$$

where this implies

$$ps|U + [(ps-1)/2]|(2^s) < U|U + p(2^rD)| = U|U + \{[(p-1)/2] + [(p+1)/2]\}(2^rD)|,$$

but

$$(ps - U)|U + [(ps-1)/2]|(2^s) < U|[(p+1)/2](2^rD)| = U|2^{r-1}D + [(p-1)/2](2^rD)|$$

which holds when $ps \leq U$, and when $|2^{r-1}D| \geq ps$ we have by (23) $ps > U$, and conversely.

This comparison can be made for subsequent pairs. It now follows that

$$|U^p - (U + 2^{ps})^p| < |2^{ps}C'^p|$$

in violation of equation (14).

Thus this option is also in contradiction, which proves Fermat's last theorem. □

4.4. The proof using the modularity theorem.