CHAPTER IV

Fermat's last theorem

4.1. Introduction.

In this chapter we look at Fermat's last theorem, where we find a constraint using elementary methods. The second method proves it using the modularity theorem, which is equivalent to the proof of Taylor and Wiles showing that every semistable elliptic curve is modular.

4.2. Fermat's last theorem and elementary methods.

Consider

$$u^p - v^p = w^p, \tag{1}$$

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. This is the same form in which r, s and t are positive natural numbers, say r = s = t odd, when (1) can be written as the special case

$$(u'^r)^p - (v'^s)^p = u'^{(rp)} - v'^{(sp)} = w'^{(tp)}.$$

We intend to look at Fermat's last theorem, that there are no such solutions to (1).

No two values of u, v and w can be even, because if say u and v were even, then w would be even, and (1) would not be in lowest terms.

There are no solutions with u, v and w all odd. This is a 'parity mismatch', because the left hand side of (1) would be even, and the right hand side odd.

We must therefore have two values of u, v and w that are odd, and the third even, so we may select w as even, then u and v are odd. All signs of u, v and w are embedded in (1), since these are nonzero integers, where the transformation say $v \to -v$ sends $v^p \to -(v)^p$, p being an odd power.

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 $a' = p$ 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 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

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

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

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

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