CHAPTER V

Fermat's last theorem

5.1 Introduction.

We discuss elementary methods approaches to Fermat's last theorem, in which the game is we do not use complex numbers. In this chapter we use 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 methods given here being publicised elsewhere. Of course this path is notorious for false proofs.

5.2 Fermat's last theorem and elementary methods.

Fermat's last theorem (FLT) remained unsolved for 350 years. It would indeed be surprising if the methods available to Fermat could now be shown to be successful in proving this theorem. Nevertheless, it is the case that for the substantial period during which this problem remained unresolved, the principal techniques were derived from Kummer theory, which if its ancestry were to be traced, had its source in Euler's solution of the theorem for $p = 3$ using the cubic and complex numbers. During this period, there was no intimation except from the mathematically naive, that elementary methods could be successful where the more sophisticated Kummer techniques had failed.

This point of view is emphasised in Manin and Panchiskin's 'Modern number theory', where they point out that it may be proved that some results using complex numbers cannot be attained by elementary methods. However, on this last comment, I have seen no proof of this assertion, which is true when analytical results are available to sophisticated methods but not elementary ones. Indeed, by use of the hyperintricate techniques in my eBook 'Innovation in mathematics' complex number techniques may be reduced to questions on $2^n \times 2^n$ matrices with real coefficients, more specifically 2×2 matrices, and even a subset of these. It thus appears on general grounds that techniques on complex numbers may be reduced to questions about some aspect of linear transformations on real numbers.

Some contemporary mathematicians – Harold Edwards is an example – question the assertion that hypersophisticated methods are necessary for such an ostensibly simple problem (at least to state).

It appears that previous techniques were unsuccessful because they did not appropriate new ideas that are necessary for a resolution of this problem. We therefore invert the method of solution and ask the following question: Is it possible to prove by elementary methods that every semi-stable elliptic curve is modular – the central assertion of the Taylor-Wiles proof of Fermat's last theorem – sometimes reformulated with wider scope as the 'modularity theorem'?

In order to develop a program of research to answer this question, it is relevant to ask what distinct techniques have been developed to tackle FLT, and how can they be reformulated in terms of elementary methods. Only after this has been accomplished does it seem sensible, given the difficulty of the problem, to ask whether any of these techniques are superfluous or can be trimmed.

The relevant topics are

Galois theory
Modular forms
p-adic numbers
Grossencharacters
Elliptic curves.

Galois theory is a theory of solvability, and since FLT can be solved, it seems secure to assume that the extensions of Galois techniques necessary for solution of the problem revert to solvable cases. Indeed, Galois theory in solvable cases reduces to the study of linear transformations as an expression of these solutions.

Modular forms revert, possibly, to a simple feature of multiplicative groups: the presence of division. We therefore expect any elementary proof of FLT to use in some general sense the idea of division, and that if this is not present, it will not work.

For p-adic numbers, this reduces to algebra (mod p^n) – and this is developed in the work on Totient reciprocity (but we may only need Euler's totient theorem in its elementary generalisation) given in our work already quoted.

For Grossencharacters, and this is sometimes expressed in terms of what are known as adeles, we can reduce these to the study of exponential powers, both additive and multiplicative, including if necessary complex powers.

For elliptic curves, and FLT uses an explicit result on the Cremona tables – on cusp forms of weight 2 – it has recently occurred to me that some features of this general case are contained in my 2009 work on Exponentiation, and it is possible that these elementary methods can be developed further.

The situation now arises that, with work, it may indeed be possible to capture all necessary features of the contemporary proof of FLT by elementary methods. However, since elementary methods are usually more difficult to implement than sophisticated ones, the question may be raised as to whether this is desirable.

5.3 The 'e = 1' case.

We investigate Fermat's last theorem, given in equation (1), by methods available to Fermat and prove by elementary methods under an assumption called 'e = 1' that Fermat's last theorem holds: the equation

$$x^p + y^p = z^p$$

implies xyz = 0 for integers x, y and z and a whole number p > 2.

For e = 1, the proof of Fermat's theorem by the means devised shows that z below cannot consist entirely of prime factors to a single power 1. In this situation, the case given below, of m = 1, can be trivially dismissed.

With e = 1 the restriction on z reduces equation (2) to

$$(m + n)^p + (m – n)^p = 2^p m^p.$$

It is straightforward to prove this is a contradiction, so Fermat's last theorem is valid here.

As a diversion, we then discuss Fermat's little theorem.

We have not been able to prove Fermat's last theorem by these techniques in the general case, but under the assumption $e \neq 1$, we carry the investigation further. We reduce Fermat's equation (1), in the three variables, x, y and z and the prime p, to m = 1 in two variables described in equation (9), where the variable c must be odd. We establish that $e = 1 \pmod p$, and discuss the standard 'first' and 'second' cases of Fermat's last theorem.

We also prove that z is not prime for x, y and z in (1), provided $(x - y) \neq 1$.

Additional results we have used are that p need not be prime because $x^{tp} = (x^t)^p$, p = 2 does not hold because of Pythagoras's theorem, and the case p = 4, accommodating $x^{4u} = (x^u)^4$, which was proved by Fermat.

Theorem 1. There is no solution with $xyz \neq 0$ of

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

where x, y and z are integers in lowest terms, z does not consist entirely of prime factors to a single power 1, and p is prime > 2. The m = 1 case is detailed later.

Proof. Let us choose $x = \frac{m+n}{2}$ and $y = \frac{m-n}{2}$, with m and n odd integers. On putting $m = 4k \pm 1$ and independently $n = 4k' \pm 1$, we see that one of x and y is even, the other odd. This implies z is odd. We will consider the case firstly when x and y are positive. Then

$$(m + n)^p + (m - n)^p = 2^p z^p, \tag{2}$$

or

$$m^p + \frac{p(p-1)}{2}m^{p-2}n^2 + \frac{p(p-1)(p-2)(p-3)}{4!}m^{p-4}n^4 + \ldots + pmn^{p-1} = 2^{p-1}z^p, \tag{3}$$

so that z^p contains m as a factor.

If $m = fg$, $f = 1$ or f is a product of distinct primes to powers with each power less than p, and $g = 1$ or $\prod_i g_i^{q_i p}$, where each distinct prime g_i is to a power multiple $q_i p$, then for $1 \leq r_i \leq p$, since p is prime

$$z^p = e^p f^p (\prod_i g_i^{q_i p r_i}), \tag{4}$$

where e has no common factor with other terms on the right of (4), in particular with m.

Thus when $f \neq 1$, dividing (3) by m gives

$$m^{p-1} + \frac{p(p-1)}{2}m^{p-3}n^2 + \frac{p(p-1)(p-2)(p-3)}{4!}m^{p-5}n^4 + \ldots + pn^{p-1} = 2^{p-1}e^p f^{p-1}\prod_i g_i^{p(q_i r_i - 1)}. \tag{5}$$

We now introduce until further notice the case e = 1, so considering the f factor and the pn^{p-1} term, we must have p = f or n = hf. But if n = hf then (1) is not in lowest terms, thus p = f and

$$p^{p-2} + \frac{p(p-1)}{2}p^{p-4}n^2 + \frac{p(p-1)(p-2)(p-3)}{4!}p^{p-6}n^4 + \ldots + n^{p-1} = 2^{p-1}p^{p-2}\prod_i g_i^{p(q_i r_i - 1)},$$

so that n contains f as a factor, and since z contains f as a factor, this again is not in lowest terms.

When f = 1 and $g \neq 1$ a similar argument holds for g rather than f, if at least one $q_i r_i \neq 1$. This is the restriction on z already mentioned. Proof of the remaining case m = 1 is established because the maximum value of n is then 1, and this is the trivial solution y = 0.

The only case of equation (1) we need consider is for x, y and z positive. At this juncture under the limitations deduced on z, we have addressed the case of positive variables in x, where variable x we can regard as even, with y odd and z odd, but we have not yet considered

an equation that is positive under the same parity of x, y and z with

$$x^p = y^p + z^p, \quad xyz \neq 0. \tag{6}$$

In the investigation that follows next we retain the same reasoning on z and m as before, in which x is even, which is the only new possibility, but y is now negative in (1), so that this reduces to equation (6). ■

Theorem 2. The case m = 1 is not present with e = 1.

Proof. We have shown this for x, y, z positive in equation (1). For positive x, y, z and m = 1 in equation (6), on putting 2c = n – 1 in (2), we have

$$(c + 1)^p - c^p = z^p. \tag{7}$$

However m = 1 means fg = 1, so f = 1, g = 1, and consequently $z^p = 1$, which implies z = 1, and there is no such non trivial solution for (7). ■

Theorem 3. Fermat's last theorem holds for e = 1.

Proof. The condition on z amounts to the case that m is a product of prime factors to single powers, giving $z^p = m^p$, in other words, z = m. Writing M = m + n = 2x, equation (2) becomes

$$M^p + (M - 2n)^p = 2^p(M - n)^p,$$

or

$$x^p + (x - n)^p = (2x - n)^p = [x + (x - n)]^p,$$

which is impossible for xyz ≠ 0, since for positive (n – x) = Dx ≠ x, D rational,

$$x^p[1 - D^p] = x^p[1 - D]^p,$$

which does not hold for D < 1 where the left hand side is greater than the right, or for D > 1, where $[1 - D^p]$ approaches $-D^p$ and $[1 - D]^p$ is $-[D - 1]^p$. ■

Remark. On putting the positive y on the right of (5) in the form $4k'' \pm 1$, if then z is of the same form $4k''' \pm 1$, on dividing the whole expression by 2, we obtain the impossibility that an even number equals an odd number. ■

Note 4. This diversion up to note 7 on Fermat's little theorem firstly states for prime p, verifiable directly for p = 2

$$s^p - s = wp. \tag{8}$$

for some unique w dependent on s. This is known as Fermat's little theorem.

Proof. We prove this by induction. For s = 0

$$0^p - 0 = 0p.$$

Assume (8) holds. Then for $s \rightarrow s + 1$, by the binomial theorem and the primality of p, so p does not divide any denominator

$$(s + 1)^p - (s + 1) = s^p - s + ps^{p-1} + [p(p - 1)/2]s^{p-2} + ... + 1^p - 1 = wp + w'p$$

for some unique w′. ■

Note 5. The notation s = t (mod p) means s = t + w″p for some w″. The Fermat little theorem states

$$s(s - 1)(s^{p-2} + s^{p-3} + ... + 1) = 0 \text{ (mod p)},$$

and we can deduce that the last term on the left factorises for odd p, since

$$s(s^{(p-1)/2} - 1)(s^{(p-1)/2} + 1) = 0 \text{ (mod p)},$$

and on factorising the second term above

$$s(s - 1)(s^{(p-3)/2} + s^{(p-5)/2} + ... + 1)(s^{(p-1)/2} + 1) = 0 \text{ (mod p)}. \blacksquare$$

Note 6. If $s^p - s = 0$ (mod p), then so is

$$s^{n(p-1)+1} - s.$$

Proof. Since $s^{2p-1} - s^p = s^{p-1}(s^p - s) = 0 \pmod p$, the sum $(s^{2p-1} - s^p) + (s^p - s) = 0 \pmod p$ also, with the general result following by recursion. ■

Corollary. Putting p = 3, we have for any odd natural number q

$$s^q - s = 0 \pmod 2 \text{ and } \pmod 3,$$

and putting p = 5, so q = 4n + 1, or p = 7, giving q = 6n + 1, etc. implies

$$s^q - s = 0 \pmod{6p}.$$ ■

Note 7. If for some x, y and z $\in \mathbf{Z}$

$$x^p + y^p = z^p,$$

with p odd > 1, then x + y – z = 0 (mod 3) .

Proof. Apply the corollary to note 6. ■

When p divides x, y or z, this instance of Fermat's last theorem is known as the 'first case', and if not, the 'second case'.

Theorem 8. For m = 1, now introducing the case e ≠ 1, on putting 2c = n – 1 in (2), we have

$$(c + 1)^p - c^p = e^p, \tag{9}$$

so that, applying Fermat's little theorem

$$s^p - s = 0 \pmod p$$

to all terms in (9) gives

$$e = 1 \pmod p = 1 + dp, \tag{10}$$

where by theorem 6, d = 6d′ for p > 3 and d = 2d′ for p = 3. Then expanding out (9) by the binomial theorem for this version of e

$$pc(1 + \tfrac{p-1}{2}c + \ldots + c^{p-2}) = p^2d + \ldots , \tag{11}$$

implies that c may contain p as a factor. ■

Corollary. For m = 1, e = 0 (mod p) is impossible. Note that by equation (3), if e = 0 (mod p) then m = 0 (mod p), but this is a contradiction since e contains no factor of m.

Theorem 9. In the 'first case' example just described of Fermat's last theorem we can write

$$c = pb,$$

and rewrite (9) using (10) as

$$p^2b + p\tfrac{(p-1)}{2}b^2p^2 + \ldots + p^pb^{p-1} = p^2d + p\tfrac{(p-1)}{2}d^2p^2 + \ldots + p^pd^{p-1} + p^pd^p, \tag{12}$$

so that on dividing by p^2, (b – d) is divisible by p. So put

$$d = b - pu, \tag{13}$$

then

$$u[1 + p\tfrac{(p-1)}{2}(b + d) + \ldots + p^{p-2}(b^{p-2} + b^{p-3}d + \ldots + d^{p-2})] = p^{p-3}d^p. \tag{14}$$

At this first stage equation (14) entails the statement that p divides u

$$u = pu',$$

and then by the same process, u′ is divisible by p, etc. until at the (p – 3)th stage there is a u″ with

$$u = p^{p-3}u'',$$

so that u″, which is odd, divides d^p, which is even. Thus when u″ ≠ 1, then u″, d and as a consequence b have a common factor. Note that

$$[1 + p\tfrac{(p-1)}{2}(b + d) + \ldots + p^{p-2}(b^{p-2} + b^{p-3}d + \ldots + d^{p-2})]$$

does not divide p, and therefore divides d^p. ■

Theorem 10. If the first case example c = pb does not hold, then we do not have

$$c^{p-1} = 0 \pmod p$$

but by a standard result derived from (8)

$$c^{p-1} = 1 \pmod p,$$

giving from (11)

$$(c + \frac{p-1}{2}c^2 + ... + 1) = 0 \pmod p. \blacksquare$$

5.4 Other methods.

Theorem 11. This theorem and theorem 12 are lifted from my work on Beal's conjecture. Let x and y be positive natural numbers, p > 2 and z be prime. There is no solution to (1).

Proof. We employ the expansion

$$z^p = (x + y)(x^{p-1} - x^{p-2}y + x^{p-3}y^2 - \ ... + y^{p-1}). \qquad (1)$$

Since the situation is symmetrical and x = y does not occur, we can consider x > y. The equation

$$z = (x + y)^{j'},$$

with $j' > 1$ cannot hold for z prime. Allocate by definition

$$z^j = (x + y) \qquad (2)$$

where $j \leq p$. Then since $x + y \neq 1$, $j \neq 0$. Thus using (1) and (2)

$$z^{p-j} = [(z^j - y)^{p-1} - (z^j - y)^{p-2}y + (z^j - y)^{p-3}y^2 + \ ... + y^{p-1}]. \qquad (3)$$

Ignoring signs, the sequence of terms in (3) is decreasing.

When j = 1, on putting y = az where $a \in [0, 1]$,

$(1 - a) > a$ for $0 < a < ½$

$(1 - a) = a$ for $a = ½$

and

$(1 - a) < a$ for $½ < a < 1$.

Then for j = 1 since

$$z^p = (z - y)^p + y^p$$
$$= z^p[(1 - a)^p + a^p] \qquad (4)$$

is at a maximum for a = 0 (when y = 0, disallowed) and a = 1 (y = z, again disallowed), and monotonically decreases to the minimum for a = ½, (4) cannot hold.

For j = 2, $(z^j - az) = z(z - a)$ converges to a minimum approaching a = 1, z > 2 and

$$z^{p-2} = z^{p-1}[(z - a)^{p-1} - (z - a)^{p-2}a + (z - a)^{p-3}a^2 + \ ... + a^{p-1}],$$

where the decreasing alternating series is greater than 1, a contradiction.

The situation for j > 2 is similar, we are dealing with

$$z^{p-j} = z^{p-1}[(z^{j-1} - a)^{p-1} - (z^{j-1} - a)^{p-2}a + (z^{j-1} - a)^{p-3}a^2 + \ ... + a^{p-1}],$$

and so (1) and thus 5.2.(1) cannot hold for z prime. ■

Theorem 12. Let p be prime > 2. There are no solutions to 5.3.(6) with z prime and y, x positive natural numbers, provided $(x - y) \neq 1$.

Proof. We have

$$z^p = (x - y)(x^{p-1} + x^{p-2}y + x^{p-3}y^2 + \ ... + x^{p-1}), \qquad (5)$$

the factorisation being unique up to order of the factors.

By definition of j, $z^j = (x - y)$ where $0 \leq j \leq p$. If we exclude the case $(x - y) = 1$, which always occurs in the case $j = 0$, so $j \neq 0$, then by (5)

$$z^{p-j} = [(z^j + y)^{p-1} + (z^j + y)^{p-2}y + (z^j + y)^{p-3}y^2 + \ ... + y^{p-1}],$$

which is impossible for positive terms. ■

Theorem 13. In equation 5.3.(1) for odd $p > 2$, $2q < p < 4q$, the integers x, y and z, $xyz \neq 0$, satisfy

$$x^p = z^p - y^p = (z^{p-2q} - y^{p-2q})(z^{2q} + z^{4q-p}y^{p-2q} + z^{6q-2p}y^{2p-4q} + ... + y^{2q}).$$

Here, for example, y may be negative. Then there are at least $\frac{(p-1)}{2}$ distinct factorisations of $(z^{p-2q} - y^{p-2q})$ and therefore of its accompanying term to the right, at least one of these alternate sets of which $\neq 1$ for all q. Moreover $(z^{p-2q} - y^{p-2q})$ may be subfactorised by the same techniques. Further, $(z^{p-2q} - y^{p-2q}) \neq (z^{p-2q'} - y^{p-2q'})^r$ for $q \neq q'$. Indeed, we have common factors which cancel, so that if, say, $q' > q$ then

$$(z^{p-2q} - y^{p-2q})/(z^{p-2q'} - y^{p-2q'}) = (z^{p-2q'} - y^{p-2q'})^{r-1},$$

is a contradiction for any r. Thus x rather than x^p has $\frac{(p-1)}{2}$ distinct factorisations, and this extends to y and z, with no factorisation $\neq 1$ in common between x, y and z. ■

Theorem 14. For positive x, y and z, $p > 1$, let

$$\frac{1}{x^p} + \frac{1}{y^p} = \frac{1}{z^p}. \tag{6}$$

Multiply (6) by $(xy)^p$. Since the left hand side is then a whole number, there exists a natural number v so that

$$xy = vz. \tag{7}$$

Likewise

$$xz = v'y \tag{8}$$

and

$$yz = v''x \tag{9}$$

for some v', v''. Then multiply (7) and (8) together to give

$$x^2 = vv', \ x = \sqrt{vv'} \tag{10}$$

and similarly

$$y^2 = vv'', \ y = \sqrt{vv''}, \tag{11}$$

$$z^2 = v'v'', \ z = \sqrt{v'v''}. \tag{12}$$

Equation (6) may be written as

$$(yz)^p + (xz)^p = (xy)^p \tag{13}$$

or using (9)

$$(v''x)^p + (xz)^p = (xy)^p$$

– not in lowest terms, but equivalent to an instance of Fermat's last theorem

$$v''^p + z^p = y^p. \tag{14}$$

Equation (13) implies on using equations (7) to (12)

$$(v''\sqrt{vv'})^p + (v'\sqrt{vv''})^p = (v\sqrt{v'v''})^p, \tag{15}$$

and irrespective of whether these are whole numbers

$$\sqrt{v''}^p + \sqrt{v'}^p = \sqrt{v}^p. \blacksquare \tag{16}$$

If x, y and z are in lowest terms in (6) then (13) cannot hold, since there are common factors of x, y and z. Then (6) is a contradiction, and therefore so is (16). ■

Theorem 15. A natural number = 0, 1 or 2 (mod 3). Thus equation 5.3.(1) is of the form

$$(x^m)^3 + (y^m)^3 = (z^m)^3,$$

for which we know xyz = 0, otherwise (1) is an equation of the following type

$$x(x^m)^3 + y(y^m)^3 = z(z^m)^3,$$
$$x^2(x^m)^3 + y^2(y^m)^3 = z^2(z^m)^3. \blacksquare$$

5.5. Fermat's last theorem and Pythagorean triples.

We 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 16. *An integer Pythagoras theorem*

$$x^2 + y^2 = z^2 \quad (1)$$

is satisfied only under the constraints

$$x = n^2 - m^2 \quad (2)$$
$$y = 2nm \quad (3)$$
$$z = n^2 + m^2. \quad (4)$$

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 does not happen 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 $xyw \neq 0$ for Pythagorean triples. 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.

Let L be the least natural number such that an integer K exists with

$$w = Kn + Lm. \qquad (7)$$

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

$$w^p = (Kn + Lm)^p$$
$$= (Qn^2 + Rn + Tm^2 + Um)^p. \quad (8)$$

Then

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

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

$$x^p + y^p = (n^2 - m^2)^p + (2nm)^p$$
$$= n^{2p} - pt^2n^{2p} + [p(p - 1)/2]t^4n^{2p} - ... + pt^{2p-2}n^{2p} - t^{2p}n^{2p} + 2pt^pn^{2p}. \quad (10)$$

Equation (7) becomes for the natural number w

$$w = (K + Lt)n. \quad (11)$$

Thus since n is a square root

$$(K + Lt) = un, \quad (12)$$

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. ■

We could investigate extended Pythagorean triples, for example

Definition. In the notation already used except with B an integer, an *extended Pythagorean triple* satisfies

$$x = n^2 - m^2 + Bn$$
$$y = 2nm$$
$$z = n^2 + m^2.$$

We can now carry out a similar argument to that already discussed for Pythagorean triples. ■

5.6. Another variation on Fermat's last theorem.

Consider

$$u^p - v^p = w^p, \quad (1)$$

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

$$(b - a)^p - (b + a)^p = 2^p c^p \qquad (2)$$

where a, b and c are integers, c is nonzero, and

$$u = b - a \qquad (3)$$

$$v = b + a, \qquad (4)$$

which implies

$$v = u + 2a. \qquad (5)$$

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

$$b^p - pab^{p-1} + p[(p - 1)/2]a^2b^{p-2} + ... + pa^{p-1}b - a^p$$
$$- b^p - pab^{p-1} - p[(p - 1)/2]a^2b^{p-2} - ... - pa^{p-1}b - a^p = 2^p c^p,$$

giving

$$- pab^{p-1} - p[(p - 1)(p - 2)/3!]a^3b^{p-3} - ... - p[(p - 1)/2]a^{p-2}b^2 - a^p = 2^{p-1}c^p. \qquad (6)$$

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

$$- pmb^{p-1} - p[(p - 1)(p - 2)/3!]a'^2m^3b^{p-2} - ... - a'^{p-1}m^p = 2^{p-1}a'^{p-1}k^p. \qquad (7)$$

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

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