Beal's conjecture

11th July, revised 24th October 2013

Abstract. *We investigate aspects of Beal's conjecture by elementary methods.*

We mention two methods for Fermat's last theorem that are not effective on their own. Fermat's little theorem states for prime p

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

so that applied to

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

$$x + y = z \pmod p. \square \quad (1)$$

The condition on quadratic residues, derived from Fermat's little theorem, states that for x a number $\neq 0$ (mod p), for x a square

$$x^{(p-1)/2} = 1 \pmod p,$$

and for a non-square

$$x^{(p-1)/2} = -1 \pmod p,$$

so that if $q = (p - 1)/2$ is prime and $x^q + y^q = z^q$,

$$\pm 1 \pm 1 = \pm 1 \pmod p,$$

a contradiction, so that $xyz = 0$ (mod p). $\square$

We can, however, employ the following argument for

$$x^3 + y^3 = z^3,$$

which we can write as

$$(x + y)(x^2 - xy + y^2) = z^3,$$

where Fermat's little theorem gives

$$x + y = z + 3n,$$

so that using

$$(x + y)^2 = (z + 3n)^2$$

or

$$(x^2 - xy + y^2) = (z + 3n)^2 - 3xy$$

we obtain

$$(z + 3n)[(z + 3n)^2 - 3xy] = z^3,$$

giving on cancelling and dividing by 3

$$3nz^2 + 9n^2z + 9n^2 = xy(z + 3n),$$

and xyz is thus divisible by 3n. $\square$

The Fermat little theorem states

$$x(x - 1)(x^{p-2} + x^{p-3} + ... + 1) = 0 \pmod p,$$

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

$$x(x^{(p-1)/2} - 1)(x^{(p-1)/2} + 1) = 0 \pmod p,$$

and on factorising the second term above

$$x(x - 1)(x^{(p-3)/2} + x^{(p-5)/2} + ... + 1)(x^{(p-1)/2} + 1) = 0 \pmod p. \square$$

Fermat's last theorem can be written

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

where

$$(x + y)(x^{p-1} – x^{p-2}y + ... + y^{p-1})$$

factorises with roots multiplied by their complex conjugates in $(p + 1)/2$ ways, where the integer values of these pairs can possibly be obtained by ruler and compass constructions, but we would have to prove this method of integer factorisation is the only one derivable. We have $x + y > z$ so $(x^{p-1} – x^{p-2}y + ... + y^{p-1}) < z^{p-1}$.

We also obtain

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

the similar integer factorisation being unique up to order of the factors. □

Since $x + y – z = np$ is even in Fermat's last theorem, n is even for prime $p > 2$ and

$$(x + y) > 2p,$$

so that when $(x + y) \approx 2p$ is the minimum under this constraint, the maximum value of $z = \sqrt[p]{x^p + y^p}$ satisfies

$$\sqrt[p]{(2p - 1)^p + 1} < z$$

giving

$$z > 2p – 1$$

and the minimum value of z for the same constraint satisfies

$$\sqrt[p]{2p^p} < z$$

giving

$$z > \sqrt[p]{2}\, p.$$ □

Let x be a Gaussian integer of the form $a + ib$, and x^* be its complex conjugate. Then for prime $p = 4k – 1$

$$x^p – x^* \equiv 0 \pmod p,$$

but if $p = 4k + 1$, the standard Fermat's little theorem holds [Ad12, Chapter V]. With that caveat – the example for Gaussian x we shall take is $p = 4k + 1$,

$$x\prod_{n=1}^{p-1}(x – \omega_{p-1}{}^n) = 0, \pmod p$$

where ω_{p-1} is a $(p – 1)$th root of unity.

For $p = 5$, $(x^{(p-1)/2} + 1) \pmod p$ factorises as

$$(x^{(p-1)/4} + (-i))(x^{(p-1)/2} + (-i)^3) \pmod p,$$

where this is in a unique factorisation domain (UFD).

For general odd p, $(x^{(p-1)/2} + 1) \pmod p$ factorises as

$$\prod_{n=1}^{\frac{p-1}{2}}(x + \omega_{p-1}{}^{2n-1}) \pmod p,$$

where there may exist other factorisations, but not if this expression is zero.

A corresponding possible factorisation for $(x^{(p-3)/2} + x^{(p-5)/2} + ... + 1) \pmod p$ is

$$\prod_{n=1}^{\frac{p-3}{2}}(x + \omega_{p-1}{}^{2n}) \pmod p.$$ □

The equation

$$x^p = z^p – y^p,$$

implies in this UFD

$$x^p = (z – y)v,$$

and combining this with the result (1)

$$x^p – vx + vnp = 0,$$

where v is odd and n is even. There is no general solution by radicals for this equation when p > 4 [Ad12, Chapter VIII]. □

Let p, q and r be natural numbers greater than one and f, g and h be positive natural numbers, all of these being powers, and t, u and v be odd integers.

An even integer can be represented in the form $2^h v$, and any odd integer except 1 in the form $(2^f t + 1)$.

For our purposes, the equation

$$(2^f t)^p + (2^g u)^q = (2^h v)^r$$

is not in lowest terms and so is discarded, together with all solutions divisible by a factor, for instance

$$[a(a^s + b^s)]^s + [b(a^s + b^s)]^s = (a^s + b^s)^{s+1},$$

for which after division by $[(a^s + b^s)]^s$, the right hand side is to the power r = 1. □

There is no equation satisfying

$$(2^f t + 1)^p + (2^g u)^q = (2^h v)^r,$$

since the left hand side is odd and the right hand side is even. □

Remark 1. If there is a solution to

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

then, on multiplying by n^{pqr}, there exist solutions not in lowest terms. □

Theorem 1.2. There is no solution

$$(2^f t + 1)^p + (2^g u + 1)^q = (2^h v)^r \qquad (2)$$

if

f > 1, or f = 1 and p is even,

and

g > 1, or g = 1 and q is even,

otherwise if not the above stipulations

f = g = 1 and neither p nor q is even.

Proof. By the binomial theorem

$$2^{fp}t^p + p2^{f(p-1)}t^{p-1} + \frac{p(p-1)}{2}2^{f(p-2)}t^{p-2} + \ldots + p2^f t + 1$$
$$+ 2^{gq}u^q + q2^{g(q-1)}u^{q-1} + \frac{q(q-1)}{2}2^{g(q-2)}u^{q-2} + \ldots + q2^g u + 1 = 2^{hr}v^r. \qquad (3)$$

Using '1 + 1 = 2', and dividing by 2, gives an odd number on the left of (3) and an even number on the right, a contradiction. □

Corollary 1.3. For (2) to have a solution, it must be one of these types

f > 1, g = 1 and q odd,

g > 1, f = 1 and p odd,

f = g = 1 and only one of p and q is even. □

For instance, with f = 2, p = 2, g = 1 and q odd

$$13^2 + 7^3 = 2^9.$$

Lemma. Let f′ be a positive natural number and t′ an odd integer. If $2^f t + 1 = -2^{f'}t' - 1$, then f = 1 if and only if $f' \neq 1$.

Proof. If f = 1 then

$$-2^{f'-1}t' = 1 + t.$$

and since both t′ and t are odd, when f′ = 1 this is a contradiction. If f ≠ 1 then if f′ ≠ 1

$$-2^{f-1}t = 1 + 2^{f'-1}t,$$

again a contradiction. □

Theorem 2. When p is odd, there can be only solutions to

$$(2^g u + 1)^q = (2^h v)^r + (2^f t + 1)^p \tag{4}$$

when

f = 1, g = 1 and q is odd,

g > 1, f > 1 (and p is odd),

or

f > 1, g = 1 and q is even.

Proof. Put

$$(2^f t + 1)^p = -(2^{f'} t' + 1)^p.$$

The result then follows from the corollary to theorem 1.2. □

Theorem 3. Suppose there is a solution in natural numbers of $x^p + y^q = z^r$, with x and y odd, and p, q and r odd. Let us also to assume to begin with that r is the lowest power. Then applying Fermat's little theorem to z, and similarly for x and y

$$z^r - z = mr$$

and we obtain since z is even

$$z = x^{p-r+1} + y^{q-r+1} - 2nr,$$

so that substituting in the original equation gives

$$x^p + y^q = (x^{p-r+1} + y^{q-r+1} - 2nr)^r,$$
$$= (x^{p-r+1} + y^{q-r+1})^r + r(-2nr)(x^{p-r+1} + y^{q-r+1})^{r-1} + \ldots + (-2nr)^r.$$

Then since $(x^{p-r+1} + y^{q-r+1})$ is even

$$\frac{(x^{p-r+1} + y^{q-r+1})^r - x^p - y^q}{2^r r^2} \tag{5}$$

is a whole number.

If instead, say, q was the lowest power, then

$$z^{r-q+1} = x^{p-q+1} + y - 2nq,$$

and a similar argument carries over. □

Theorem 4. The equation

$$(x - 2n)^p + (x + 2n)^p = (2z)^r,$$

where the variable x must be odd, otherwise the equation is not in lowest terms, has no solution.

Proof. The case for p even is similar.

$$2x^p + p(p - 1)4n^2x^{p-2} + \ldots = (2z)^r$$

and on dividing by 2 the left hand side is odd and the right hand side is even. □

Corollary 4.1. There is no solution to

$$(4k \pm 1)^p + (4m \pm 1)^p = (2z)^r,$$

for r > 1. The sign in ± 1 is the same for the first and second terms.

Proof. Put $n = (m - k)$ and $x = 2(m + k) \pm 1$ in theorem 4. □

Corollary 4.2. For p odd, the equation

$$(2n + x)^p = (2z)^r + (2n - x)^p,$$

where the variable x must be odd, otherwise the equation is not in lowest terms, has no solution. □

Corollary 4.3. For p odd, there is no solution to

$$(4k \pm 1)^p = (2z)^r + (4m - (\pm 1))^p$$

for $r > 1$. If the sign (± 1) is + 1 for the first term, the third term is $-(+1) = -1$, etc.

Proof. Put $n = (k + m)$ and $x = 2(k - m) \pm 1$ in corollary 4.2. □

Theorem 5. If

$$x^p + (x + 2n)^p = (2z)^r,$$

then n is odd and p is odd.

Proof. The variable x must be odd, otherwise the equation is not in lowest terms. On dividing by 2,

$$x^p + pnx^{p-1} + p(p - 1)n^2x^{p-2} + \ ... = 2^{r-1}z^r,$$

again a parity mismatch if n or p are even. □

Remark 5.1. If we combine the circumstances of the corollary to theorem 1, and theorem 5, in particular we have n odd, $f > 1$, $g = 1$ and $p = q$ odd, then

$$x = 2^f t + 1$$
$$x + 2n = 2u + 1$$

so that

$$n = u - 2^{f-1}t, \tag{6}$$

or

$$x + 2n = 2^f t + 1$$
$$x = 2u + 1$$

with

$$n = 2^{f-1}t - u, \tag{7}$$

where the end terms in equation (3) are

$$... + p2^f t + 1 + q2u + 1 = 2^{hr}v^r.$$ □

Remark 5.2. If the condition of theorem 5 holds

$$x^p + (x + 2n)^p = (2z)^r,$$

then we can put this as

$$(y - n)^p + (y + n)^p = (2z)^r,$$

where $y = x + n$. Then if y is odd, n is even – and we have dealt with this already in theorem 3, or y is even and n is odd, which we may put in the form

$$(2u - n)^p + (2u + n)^p = (2z)^r, \tag{8}$$

where $y = 2u$.

Then expanding out by the binomial theorem and dividing by 4

$$2^{p-1}u^p + ... + upn^{p-1} = 2^{r-2}z^r,$$

and u must contain a factor 2^{r-2}, otherwise there is a parity mismatch. For $u = 2^{r-2}f$ in (8) and on dividing out 2^r,

$$2^{p(r-1)-r+1}f^p + \ldots + fpn^{p-1} = z^r$$

and f divides z, z is odd, so f is odd, say vf = z, v odd. Then

$$2^{p(r-1)-r+1}f^{p-1} + \ldots + pn^{p-1} = v^r f^{r-1}.$$

Transferring the term on the right to the left, and the pn^{p-1} term on the left to the right, we see that f divides pn^{p-1}, so that if f does not contain p as a factor or equals 1, f divides n, a contradiction since equation (8) is not now in lowest terms. □

Theorem 6. Let p and q be odd > 2, r > 1, and x be odd, otherwise the equation is not in lowest terms. Then

$$(x - 2n)^p + (x + 2n)^q = (2z)^r,$$

has no solution.

Proof. $[(x^p + x^q)/2] + n(qx^{q-1} - px^{p-1}) + 2n^2[q(q-1)x^{q-2} + p(p-1)x^{p-2}] + \ldots = (2z)^r$ and $(x^p + x^q)/2$ is odd, a parity mismatch. □

Corollary 6.1. Under the same conditions, there is no solution to

$$(4k \pm 1)^p + (4m \pm 1)^q = (2z)^r.$$

The sign in ± 1 is the same for the first and second terms.

Proof. Put n = (m – k) and x = 2(m + k) ± 1 in theorem 6. □

Corollary 6.2. Under these conditions, the equation

$$(2n + x)^q = (2z)^r + (2n - x)^p,$$

has no solution. □

Corollary 6.3. There is thus no solution to

$$(4k \pm 1)^q = (2z)^r + (4m - (\pm 1))^p.$$

If the sign (±1) is + 1 for the first term, the third term is – (+1) = -1, etc.

Proof. Put n = (k + m) and x = 2(k – m) ± 1 in corollary 6.2. □

Remark 7.1. If

$$(4m \pm 1)^p + (2z)^p = (4k \pm 1)^p, \tag{9}$$

where the sign in ± 1 is the same for the first and third terms, this reduces to

$$4^{p-1}m^p \pm p4^{p-2}m^{p-1} + \ldots + m + 2^{p-2}z^p = 4^{p-1}k^p \pm p4^{p-2}k^{p-1} + \ldots + k. \tag{10}$$

Then for a suitable variable u, provided p > 2

$$2^{p-2}z^p = (k - m)(1 \pm 4pu),$$

and since 1 ± 4pu is odd, (k – m) is divisible by 2^{p-2}, which implies k and m are both even or both odd. □

Remark 7.2. We have seen that for some n, the condition on Fermat's last theorem is

$$x + y = z + np,$$

where, say, x is odd, y is even and z is odd, so that n is even. Thus on taking the pth power

$$x^p + y^p + pxy(x^{p-2} + \tfrac{p(p-1)}{2}x^{p-3}y + \ldots + \tfrac{p(p-1)}{2}xy^{p-3} + y^{p-2})$$
$$= z^p + np^2(z^{p-1} + [(p-1)/2]z^{p-2}np + \ldots + (np)^{p-2}n),$$

and subtracting the Fermat equation, the even part of y must be the same as the even part of n, because the long terms in parentheses are odd. So put $y = 2^m v$ and $n = 2^m u$, with u and v odd.

Then the Fermat's equation is expressed as

$$x^p + (2^m v)^p = [x + 2^m v - 2^m up]^p = x^p + (2^m v)^p + p2^m vx^{p-1} + \frac{p(p-1)}{2}x^{p-2}2^{2m}v^2 + ... + 2^{mp}v^p - 2^{mp}(up)^p + (x + 2^m v)p(-2^m up)^{p-1} + ... + (x + 2^m v)^{p-1}(-2^m up),$$

and on cancelling and dividing by 2^m

$$0 = pvx^{p-1} + p(p-1)x^{p-2}2^{m-1}v^2 + ... + 2^{m(p-1)}v^p - 2^{m(p-1)}(up)^p + (x + 2^m v)p(-2^{m(p-2)}(up)^{p-1} + ... + (x + 2^m v)^{p-1}(-up),$$

so we have a term

$$p(x^{p-1}(v - u)),$$

which is divisible by the precise power of 2, 2^m, hence $(v - u)$ is divisible by 2^m. □

Theorem 8. Let p, q and $r > 2$ with q an odd prime. We will make the assumption that $p \geq q$, although the proof carries through under the reverse assumption with p odd prime. Provided the power of 2 part of $[(s - t)^{p-q} + 1]t$ or $[(s - t)^{p-q} - 1]s$ does not exactly divide 2^r, for u odd there are no solutions to

$$(s - t)^p \pm 2^r u = (s + t)^q. \quad (11)$$

Proof. The stipulation that q is prime may be removed in the standard FLT manner. The cases we need to consider are s odd and t even, or s even and t odd. Expanding out by the binomial theorem

$$(s - t)^{p-q}\{s^q - qts^{q-1} + \frac{q(q-1)}{2}t^2s^{q-2} + ... - \frac{q(q-1)}{2}t^{q-2}s^2 + qt^{q-1}s - t^q\} \pm 2^r u = s^q + qts^{q-1} + \frac{q(q-1)}{2}t^2s^{q-2} + ... + \frac{q(q-1)}{2}t^{q-2}s^2 + qt^{q-1}s + t^q\}.$$

Then $[(s - t)^{p-q} - 1]$ and $[(s - t)^{p-q} + 1]$ have a common factor of a power of 2 = 2 and

$$[(s - t)^{p-q} - 1]\{s^q + \frac{q(q-1)}{2}t^2s^{q-2} + \frac{q(q-1)(q-2)(q-3)}{4!}t^4s^{q-4} + ... + qt^{q-1}s\} \pm 2^r u = [(s - t)^{p-q} + 1]\{qts^{q-1} + \frac{q(q-1)(q-2)}{3!}t^2s^{q-2} + ... + t^q\}, \quad (12)$$

so that if s is even and t is odd, or if s is odd and t is even, on dividing by 2, equation (12) cannot hold under the conditions of the theorem. □

Corollary 8.1. Under the same conditions and p odd, there is no solution to

$$2^r u = (t + s)^q + (t - s)^p. \quad (13)$$

□

Example 8.2. We will choose $p = q = 3$, $s = 595$, $t = 324 = 81 \times 4$, so the power of 2 part of $[(s - t)^{p-q} + 1]t$ is 2^3, which exactly divides 2^r for

$$271^3 + 2^3.3^5.73^3 = 919^3 = 776{,}151{,}559.$$ □

Remark 9.1. Define a Mersenne number (see [Ad09] section 2.2 for a generalisation of this idea) by the recursion

$$M_n = (2M_{n-1} + 1)$$

and

$$M_0 = 1.$$

Then multiplying M_n by $(2 - 1)$ gives

$$M_n = (2^{n+1} - 1).$$ □

Remark 9.2. Starting from an odd t = 3, 3 is a Mersenne number. If $t \neq 3$ then 5 is the next odd number along and $t = (2^2.1 + 1)$ which is not a Mersenne number at level m = 1. If we want to generate 7, then (2.3 + 1) satisfies the criterions and this is the Mersenne number M_2. If we generate 9, this is $(2^3.1 + 1)$, not a Mersenne number at level m = 1, 11 is $[2.(2^2.1 + 1)]$, which is not a Mersenne number at level m = 2, 13 = $[2^2.3 + 1]$, which again is not a Mersenne number at iteration level m = 1, and so on.

Theorem 10. Let p′, q′, x′, z′ and u be odd, where p′, q′ and r > 1. For s even and t odd given below, the generalised Beal's conjecture holds; there is no

$$\pm x'^{p'} \pm 2^r u = z'^{q'}. \tag{14}$$

Proof. Let c_m, c'_m and $c''_m = 0$ or 1. We set the binary expansions

$$\begin{aligned} s &= \textstyle\sum_{m=1}^{n} 2^m c_m, \\ t &= \textstyle\sum_{m=0}^{n'} 2^m c'_m, \\ u &= \textstyle\sum_{m=0}^{n''} 2^m c''_m. \end{aligned} \tag{15}$$

We will reduce (14) to a form in which $p = \frac{p'}{a}$ and $q = \frac{q'}{b}$ are prime

$$\pm x^p \pm 2^r u = z^q, \tag{16}$$

under the substitution $x = x'^a$ and $z = z'^b$, and then rewrite (16) as the absence of a solution to

$$(s - t)^p \pm 2^r u = (s + t)^q. \tag{17}$$

It is clear that if (17) is absent then corollary 8.1 holds, and there is no (14).

For the sake of argument, which we could invert, we put n > n′, padding out c'_m for values > n′ with zero, and will express (17) using conditions (15) as

$$\begin{aligned} &[2^n + \textstyle\sum_{m=1}^{n-1}(c_m - c'_m)2^m - 1]^p \pm 2^r \sum_{m=0}^{n''}(c''_m 2^m) \\ &\quad = [2^n + \textstyle\sum_{m=1}^{n-1}(c_m + c'_m)2^m + 1]^q. \end{aligned} \tag{18}$$

Take the two lowest power terms of all factors. Then for p odd so that $(-1)^p = -1$,

$$\begin{aligned} &\ldots + p[\textstyle\sum_{m=1}^{n-1}(c_m - c'_m)2^m] - 1 \pm 2^r[\sum_{m=1}^{n''}(c''_m 2^m) + 1] \\ &\quad = \ldots + q[\textstyle\sum_{m=1}^{n-1}(c_m + c'_m)2^m] + 1, \end{aligned}$$

and on taking the -1 on the left, transposing to the right hand side and dividing by 2

$$\begin{aligned} &\ldots + p[\textstyle\sum_{m=1}^{n-1}(c_m - c'_m)2^{m-1}] \pm 2^{r-1}[\sum_{m=1}^{n''}(c''_m 2^m) + 1] \\ &\quad = \ldots + q[\textstyle\sum_{m=1}^{n-1}(c_m + c'_m)2^{m-1}] + 1. \end{aligned} \tag{19}$$

We have stipulated that r > 1. If $c_1 \neq c'_1$ then $p[c_m - c'_m] - q[c_m + c'_m]$ is even. Then also when $c_1 = c'_1$ this is a contradiction. □

Corollary 10.1. There is no equation (11) restriction for theorem 8 when s is even. □

Remark 10.2. Apart from a possible sign in $\pm 2^r u$ and there being no rth power of u, theorem 10 is identical to corollary 6.2. □

Remark 10.3. To summarise some of these results, provided the power of 2 factor of $[(s - t)^{p-q} + 1]t$ or $[(s - t)^{p-q} - 1]s$ exactly divides 2^{hr}, for u odd there may be solutions to

$$(s - t)^p \pm (2^h u)^r = (s + t)^q, \tag{20}$$

where s is odd, t is even, and p and q are odd.

When this holds and (20) is of the form

$$(2^g j + 1)^q = (2^h u)^r + (2^f k + 1)^p \quad (21)$$

from theorem 2, there can only be solutions when

$$f = 1, g = 1$$

or

$$g > 1, f > 1,$$

and when (20) is of the form

$$(2^f j + 1)^p + (2^g k + 1)^q = (2^h u)^r, \quad (22)$$

then from corollary 1.1

$$f > 1, g = 1$$

or

$$g > 1, f = 1.$$

For Fermat's last theorem, remark 7.2 with (20) implies for some w

$$t = 2^{h-1}(u - wp). \square$$

Theorem 11. Let

$$(s - t)^p \pm 2^r u = (s + t)^q,$$

then $[(s - t)^{p-q} - 1]$ is divisible by 4 and $[(s - t)^{p-q} + 1]/2$ is odd.

Proof. Since s is odd and t is even, for a violation of Beal's conjecture, theorem 8 becomes

$$[(s - t)^{p-q} - 1]\{\text{odd}\} \pm 2^r u = [(s - t)^{p-q} + 1]\{\text{even}\},$$

and since $r > 2$ this is divisible by 4, so $[(s - t)^{p-q} - 1]$ is divisible by 4.
But since $[(s - t)^{p-q} - 1]$ and $[(s - t)^{p-q} + 1]$ have a common power of two factor of precisely 2, $[(s - t)^{p-q} + 1]/2$ is odd. $\square$

Lemma 12. If $y^p - y \equiv 0 \pmod p$, then so is

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

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

Corollary 12.1. Putting p = 3, we have for any odd natural number q

$$y^q - y \equiv 0 \pmod 2 \text{ and } \pmod 3,$$

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

$$y^q - y \equiv 0 \pmod{6p}. \square$$

Theorem 12.2. If for some x, y and $z \in \mathbf{Z}$

$$x^p + y^q = z^r \quad (23)$$

with p, q, r odd > 1, then $x + y - z \equiv 0 \pmod 3$.

Proof. In characteristic 0, if p = q = r, then by the Fermat-Taylor-Wiles theorem xyz = 0, implying x + y = z, but by equation (1) x + y = z + np, so this implies n = 0.

If

$$x^3 - x = 3w_x$$

then by the lemma

$$x^{2h+1} - x = 3[x^{2(h-1)} + x^{2(h-2)} + \ldots + 1]w_x.$$

Thus with w_y as the formula for y, and similarly for w_z, putting $w_x + w_y - w_z = 0$, then

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

implies

$$x + y - z = 3\{[x^{2(h-1)} + x^{2(h-2)} + \ldots + x]w_x + [y^{2(h-1)} + y^{2(h-2)} + \ldots + y]w_y - [z^{2(h-1)} + z^{2(h-2)} + \ldots + z]w_z\},$$

that is

$$x + y - z \equiv 0 \pmod 3. \square$$

Corollary 12.3. Let

$$(s - t)^p \pm (2^r u)^k = (s + t)^q$$

and $t = 2^w v$ with v odd, then from theorem 12.2

$$2^{r-1}u = t + 3m,$$

so that m contains the highest common factor of 2^{r-1} and 2^w. $\square$

Theorem 13.1. Let p be prime ≥ 3. There are no solutions to

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

with x prime and y, z positive natural numbers, provided $(z - y) \neq 1$.

Proof. We have

$$x^p = (z - y)(z^{p-1} + z^{p-2}y + z^{p-3}y^2 + \ldots + y^{p-1}), \quad (24)$$

the factorisation being unique up to order of the factors.

By definition of m, $x^m = (z - y)$, where $0 \leq m \leq p$. If we exclude the case $m = 0$, so that $(z - y) \neq 1$, then by (24)

$$x^{p-m} = [(x^m + y)^{(p-1)} + (x^m + y)^{p-2}y + (x^m + y)^{p-3}y^2 + \ldots + y^{p-1}],$$

which is impossible for positive terms. $\square$

If we try to eliminate all occurrences of $z = y + 1$ irrespective of the primality of x we can obtain the following limited result.

Remark 13.2. Let p be prime ≥ 3 and

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

with x, y, z positive natural numbers, and

$$z = y + a,$$

then $x^p - a^p = mp^2$ for some m when $a = 1$.

Proof. We put

$$x^p + y^p = (y + a)^p$$

$$x^p = (py^{p-1}a + \frac{p(p-1)}{2}y^{p-2}a^2 + \ldots + a^p),$$

so that

$$(x - a)(x^{p-1} + x^{p-2}a + \ldots + a^{p-1}) = p(y^{p-2} + \frac{(p-1)}{2}y^{p-2}a + \ldots + a^{p-2})ya. \quad (25)$$

By Fermat's little theorem

$$x + y = z + np = y + a + np$$

giving

$$x - a = np \quad (26)$$

$$x = np + a,$$

so we infer by (26) in (25)

$$n((np + a)^{p-1} + (np + a)^{p-2}a + ... + a^{p-1})$$
$$= (y^{p-2} + \frac{(p-1)}{2}y^{p-2}a + ... + a^{p-2})ya, \quad (27)$$

where the left hand side under binomial expansions contains p terms with + 1.

To summarise

$(x – a)$ is divisible by p

$(x^{p-1} + x^{p-2}a + ... + a^{p-1})$ is divisible by p when a = 1.

This means

$$x^p – 1 = mp^2,$$

for some m. □

Theorem 13.3. Let q and r be natural numbers > 1 with r odd. There are no solutions

$$x^q + y^r = z^r$$

with x prime, y and z positive natural numbers and $(z – y) \neq 1$.

Proof. If r is composite, denote it by uv, where v is an odd prime. We are now looking at the formula

$$x^q + (y^u)^v = (z^u)^v. \quad (28)$$

By the techniques of theorem 13.1, this has no solution for $q \leq v$ when $(z – y) \neq 1$.

Now multiply (28) by x^{qv}. Then

$$(x^{2q})^{½(v+1)} + (x^q y^u)^v = (x^q z^u)^v,$$

and

$$½(v + 1) \leq v. \square$$

Theorem 13.4. Let p be prime ≥ 3 with $0 \leq k_n \leq p$ and y, z positive natural numbers. There are no solutions to

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

with x a composite $\prod_n t_n$, provided $\prod_n t_n \uparrow k_n = (z – y)$ satisfies all $k_n \neq 0$.

Proof. We still have (24), but now

$$\prod_n t\uparrow(p – k_n) = [(\prod_n t\uparrow k_n + y)^{(p-1)} + (\prod_n t\uparrow k_n + y)^{p-2}y + ... + y^{p-1}], \quad (29)$$

which is impossible if all $k_n \neq 0$. □

Theorem 14.1. Let x and y be positive natural numbers, and p > 2 and z be prime. There is no solution

$$x^p + y^p = z^p. \quad (30)$$

Proof. We employ the alternative expansion

$$z^p = (x + y)(x^{p-1} – x^{p-2}y + x^{p-3}y^2 – ... + y^{p-1}). \quad (31)$$

Allocate by definition

$$z^n = (x + y) \quad (32)$$

where $n \leq p$. Then since $x + y \neq 1$, $n \neq 0$.

Thus using (32) and (31)

$$z^{p-n} = [(z^n – y)^{p-1} – (z^n – y)^{p-2}y + (z^n – y)^{p-3}y^2 + ... + y^{p-1}]. \quad (33)$$

Ignoring signs, the sequence of terms in (30) is decreasing.

When n = 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 n = 1 since

$$z^p = (z - y)^p + y^p$$
$$= z^p[(1 - a)^p + a^p] \quad (34)$$

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, and thus (34) cannot hold.

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

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

where the decreasing sequence of terms before the final 1 is positive.

The situation for n > 2 is similar, and so (33) and thus (30) cannot hold for z prime. □

Theorem 14.2. Let the conditions of theorem 14.1 hold except

$$x^p + y^p = z^q \quad (35)$$

where q is a natural number greater than 1, with z prime. There is no solution to (35).

Proof. Equation (33) pertains for z^{p-n} on the left replaced by z^{q-n}, when q < p. The argument given in theorem 13.3 now applies, so that on multiplying by z^{qp}, (35) also cannot hold when $q \geq p$. □

Remark 15. It is the case simultaneously that we do not have z = y + 1 and z = x + 1, and therefore if $x^p + y^p = z^p$, both z is not prime and one of x and y is not prime, in which if say x is prime then z = y + 1.

Theorem 16.1. Let p be an odd prime, x, z and r be odd and $\in$ **N**, and k $\in$ $\mathbf{N}_{\neq 0}$. If

$$x^p + (2^k r)^p = z^p$$

then

$$z - x = 2^p$$

and

$$x + 2r = z + 2mp,$$

where m is odd.

Proof. The first term on the right below is even, and the second term is odd

$$2^{kp}r^p = (z - x)(z^{p-1} + z^{p-2}x + ... + x^{p-1}),$$

so put

$$2^{kp}r^n = z - x, \quad (36)$$

which means

$$r^{p-n} = (z^{p-1} + z^{p-2}x + ... + x^{p-1}), \quad (37)$$

and inserting (36) for z in (37) gives the result n = 0 and k = 1.

Then Fermat's little theorem gives

$$x + 2r = z + hp.$$ □

Remark 16.2. If x is prime and

$$x^p + (2r)^p = z^p$$

then x – 1 contains only one factor of 2.

Proof. From remark 15, since 2r is composite arising from $r \neq 1$, the only possible situation of a prime variable is x, when z = 2r + 1, but then by theorem 16.1

$$r = 2^{p-1} + mp$$

with m odd, giving

$$x^p + [2(2^{p-1} + mp)]^p = [2(2^{p-1} + mp) + 1]^p,$$

whereas

$$x^p – 1 = (x – 1)(x^{p-1} + ... + 1),$$

with the first term on the right even, and the last term odd, so x – 1 contains only one factor of 2. □

References

Ad09 J.H. Adams, *Exponentiation* (2^{nd} edn), 2009.

Ad12 J.H. Adams, *Hyperintricate matrices*, *Foundations*, 2012.

CS97 G. Cornell, J.H. Silverman and G. Stevens (*editors*), *Modular forms and Fermat's last theorem*, Springer, 1997.

Ed77 H.M. Edwards, *Fermat's last theorem*, Springer (1977).

Eu1770 L.Euler, *Vollständige Anleitung zur Algebra*, St Petersburg, 1770; Opera (1) vol.1.

Fe1891 P. de Fermat, *Observations on Diophantus*; Oeuvres, vol.1. Gauthier-Villars, Paris, 1891.

Ku75a E.E. Kummer, *Collected papers*, ed. André Weil, vol. 1, *Contributions to number theory*, Springer-Verlag, (1975).

Ku75b E.E. Kummer, *De numeris complexis, qui radicibus unitatis et numeris Integris redibus constant*, ibid. 165-192.

Ku75c E.E. Kummer, *Beweis des Fermat'schen Satzes der Unmöglichkeit von* $x^\lambda + y^\lambda = z^\lambda$, *fur eine unendliche Anzahl Primzahlen* λ, ibid. 274-297.

MP07 Yu.I. Manin and A.A. Panchiskin, *Introduction to modern number theory*, Springer, (2005, 2007).

Ma77 B. Mazur, *Modular curves and the Eisenstein ideal*, IHES Publ. Math **47**, 33- 186, (1977).

Ma78 B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44**, 129-162, (1978).

Me03 T. Metsänkylä, *Catalan's conjecture: another old Diophantine problem solved*, Bull. Amer. Math Soc. **41**, 43–57, (2003).

Mi04 P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. reine angew. Math **572**, 167–195, (2004).

Sc08 R. Schoof, *Catalan's conjecture*, Springer-Verlag, (2008).

TW95 R. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Math. **141**, No. 3, 1995, 553-572.

W95 A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of Math. **141**, No. 3, 1995, 443-551.