An alternative way to write Fermat's equation and notes on an elementary proof of FLT

C. Sloane

Victoria University, NZ

(chrissloane70@gmail.com)

(Feb 2018)

Abstract

We discovered a way to write the equation $x^n+y^n-z^n=0$ first studied by Fermat, in powers of 3 other variables defined as; the sum $t = x+y-z$, the product (xyz) and another term $r = x^2+yz-xt-t^2$. Once $x^n+y^n-z^n$ is written in powers of t, r and (xyz) we found that 3 cases of a prime factor q of x^2+yz divided t. We realized that from this alternative form of Fermat's equation if all cases of q divided t that this would lead to a contradiction and solve Fermat's Last Theorem. Intrigued by this, we then discovered that the fourth case, $q=3sp+1$ also divides t when using a lemma that uniquely defines an aspect of Fermat's equation resulting in the following theorem:

If $x^p + y^p - z^p = 0$ *and suppose* x, y, z *are pairwise co-prime then any prime factor* q *of* $(x^2 + yz)$ *will divide* t *, where* $t = x + y - z$

.

Introduction

There have been thousands of attempts to solve Fermat's Last Theorem (FLT) using Elementary Number Theory (ENT) over the centuries. Naturally when considering a problem that can be easily stated and understood one would assume a relatively easy proof in ENT would exist. However, none were found with the equation as it is written, with the exception of Andrew Wile's proof using modern number theory techniques.

When in 1993 Andrew Beal conjectured that there were only common factor solutions to the general case of FLT namely $x^a+y^b-z^c=0$ when $a,b,c>2$ one then assumed that there were common factor solutions to FLT but obviously these solutions would cancel out and be non-existent in the special case. We therefore wondered what would be a good way of showing common factors or more specifically what term's prime composition would give common factors if they shared a prime? We found 3 good candidates x^2+yz, y^2+xz, and z^2-xy because if they shared a prime factor (q) with powers of x, y, z or xy, xz, yz or xyz then we get common factor solutions q.

We can't see how to use this with Fermat's equation as it is written but when we were trying to factor x^2+yz into the n=3,5,7 equation we initially found a separation of the terms $(x+y-z)$ and (xyz). We then wondered whether this was possible for all n. What we wanted to do was see if we can put this equation in terms of($x+y-z$) and (xyz), or more specifically powers of ($x+y-z$) and powers of (xyz) and indeed we could if we introduce a new term we call the symmetric $r= x^2+yz-xt-t^2$ which happens to have a x^2+yz component.

For example we have Fermat's equation for n=7,

$$x^7+y^7-z^7=0$$

and in the new representation we have for n=7,

$$29t^7+56t^5r-35(xyz)t^4+35r^2t^3-35(xyz)t^2r+7tr^3+7(xyz)^2t-7r^2(xyz)=0$$

One can see this is written in powers of the 3 terms t, r,(xyz) and these terms completely replace the powers of x, y and z to become the arguments or variables in the problem.

We then studied this new equation and realised that if we showed all the prime factors of x^2+yz or y^2+xz, or z^2-xy divided t we could solve Fermat's Last theorem because this leads to a contradiction $x^2+yz\leq t$ but $x^2+yz>t$ in FLT as the case in point.

We first show that $t\equiv 0 mod 3$ and recognized that if we take a prime factor (q) of x^2+yz we can easily show that for one case of q and two sub-cases of q namely,

$$q\neq 3sp+1$$
$$q=sp+1,\ s\neq M3$$
$$q=3s+1,\ s\neq Mp$$

when n is prime (p) we get $t\equiv 0 mod q$ or we get common factor solutions for these cases.

The 4th case $q=3sp^k+1$ is more difficult but we develop methods to deal with it. We use a lemma (lemma 5) that defines a particular property of Fermat's equation namely; $x+y=c^p$, $z-y=a^p$, $z-x=b^p$. Then, along with the possible solutions when $q=3sp+1$, we show that these q's must also divide t. We further generalize to all k using an exponentiation method that combined with lemma 5 shows all $q(k)$ divide t.

We therefore end up with $t\equiv 0 mod q$ for all possible cases of q. When we look at our new representation of Fermat's equation, we can show that with the decomposition of ,

$x^2+yz=q_1^{\boldsymbol{q}(q_1)}q_2^{\boldsymbol{q}(q_2)}q_3^{\boldsymbol{q}(q_3)}\ldots q_n^{\boldsymbol{q}(q_n)}$ where q_i is prime and $\boldsymbol{q}(q_i)$ the highest power dividing x^2+yz, that these higher power terms must also divide t but we have that $x^2+yz>t$ which obviously eliminates integer solutions.

Remark: The premise behind solving this problem is quite simple - all we are showing is all the prime factors of a particular term divide t or we get common factor solutions, resulting in the theorem;

If $x^p+y^p-z^p=0$ and suppose x, y, z are pairwise co-prime then any prime factor q of (x^2+yz) will divide t where $t=x+y-z$

Historical Note: Although, FLT is an ancient problem it is only relatively recently (30 years) that we have found the generalized version of the problem almost certainly has only common factor solutions. If ancient mathematicians had known this, they would have realised that common factor solutions to the special case would not exist and would be a good way of solving FLT. It is difficult to find common factor methods working with three independent variables. However changing the form of Fermat's equation to incorporate specific terms like x^2+yz creates an environment friendly to common factor approaches. With this alternative version of Fermat's equation also unknown to mathematicians until now, then the problem may not be outside the realms of elementary number theory after all.
.

Definitions

We define the dependent variable t as,

$$t= x+y-z \tag{1.01}$$

Another way of writing $2t$ is to let, $x+y=C,\ z-y=A,\ z-x=B.$

$$2t=-A-B+C \tag{1.02}$$

$$x = A+t \tag{1.03}$$

$$y = B+t \tag{1.04}$$

$$z = C - t \tag{1.05}$$

We define the symmetric r in general as,

$$r(v) = x^2 + yz - xt + vt^2 = y^2 + xz - yt + vt^2 = z^2 - xy + zt + vt^2 \tag{1.06}$$

We can also write this as,

$$r(v) = xz + yz - xy + vt^2 \tag{1.07}$$

In this work we will only be using v= -1,

$$r(-1) \text{ or } r = xz + yz - xy - t^2 \tag{1.08}$$

The symmetric parts are defined as,

$$r(x/t) = x^2 + yz,\ r(y/t) = y^2 + xz,\ r(-z/t) = z^2 - xy,\ r(0) = xz + yz - xy \tag{1.09}$$

We can use any of $r(x/t)= x^2+yz,\ r(y/t)=y^2+xz,\ r(-z/t)=z^2-xy,$ to contain our prime factors q
In this work we will use,

$$r(x/t) \text{ or } r' = x^2 + yz \tag{1.10}$$

We use capitalization when refering to these definitions in x^p, y^p, z^p *i.e* $x \to x^p,\ y \to y^p,\ z \to z^p$
Hence,

$$T = x^p + y^p - z^p \tag{1.11}$$

$$R = x^p z^p + y^p z^p - x^p y^p - T^2 \tag{1.12}$$

$$R' = x^{2p} + y^p z^p \tag{1.13}$$

Remark: '*M'* stands for 'multiple of' at some places in this work.

We derive the new form of Fermat's equation using combinatorial arguments. This proof is quite long and as one knows combinatorial proofs take a long time to work through (over 14 pages in this instance). Hence not to distract the reader with this cumbersome proof we will state the results Theorem 1.1 and Corollary 1,2 for brevity. One can use a calculator or computer to check the validity of these equations for any input. If one requires the rigorous proof please see extract 2

Proposition 1 *We can write* $x^n + y^n + (-z)^n$ *in terms of* $(xyz)^m$, r^{ϖ} *and* t^{ℓ}

Starting with,

$$x^n + y^n - z^n = (A+t)^n + (B+t)^n - (C-t)^n$$

We initially factor $A^2+BC\text{-}At\text{-}t^2$ in this derivation and convert back to $x^2+yz\text{-}xt\text{-}t^2$. In general we end up getting for n *and* ℓ;

$n = odd\ \ell = even$

$\# n = even\ \ell = odd \rightarrow -1$

$$-((n\frac{\frac{n+(\ell-3)}{2}\frac{n+(\ell-5)}{2}\cdots\frac{n-(\ell+1)}{2}}{\ell!1!0!}+n\frac{\frac{n+(\ell-5)}{2}\cdots\frac{n-(\ell+1)}{2}}{(\ell-2)!1!1!}+\ldots n\frac{\frac{n-(3\#)}{2}\frac{n-(5\#)}{2}\cdots\frac{n-(\ell+1)}{2}}{1!1!(\frac{\ell\#}{2})!})t^{\ell}xyzr^{\frac{n-\ell-3}{2}}$$

$$-(n\frac{\frac{n+(\ell-5)}{2}\frac{n+(\ell-7)}{2}\cdots\frac{n-(\ell+7)}{2}}{\ell!3!0!}+n\frac{\frac{n+(\ell-7)}{2}\cdots\frac{n-(\ell+7)}{2}}{(\ell-2)!3!1!}+\ldots n\frac{\frac{n-(5\#)}{2}\frac{n-(7\#)}{2}\cdots\frac{n-(\ell+7)}{2}}{1!3!(\frac{\ell\#}{2})!})t^{\ell}(xyz)^3r^{\frac{n-\ell-9}{2}}$$

$$-(\frac{n(\frac{n+(\ell-m-2)}{2})(\frac{n+(\ell-m-4)}{2})\ldots(\frac{(n-(\ell+3m-2)}{2})}{\ell!m!0!}+\frac{n(\frac{n+(\ell-m-4)}{2})(\frac{(n+(\ell-m-6)}{2})\ldots(\frac{(n-(\ell+3m-2)}{2})}{(\ell-2)!m!1!}+\ldots$$

$$\frac{n(\frac{n-(m+2\#)}{2})(\frac{(n-(m+4\#)}{2})\ldots(\frac{(n-(\ell+3m-2)}{2})}{1!m!\frac{(\ell\#)}{2}!}))t^{\ell}(xyz)^m r^{\frac{n-\ell-3m}{2}} \qquad (1.14)$$

$n = odd\ \ell = odd$

$*n = even, \ell = even \rightarrow +1$

$$((n\frac{\frac{n+(\ell-2)}{2}\frac{n+(\ell-4)}{2}\cdots\frac{n-(\ell-2)}{2}}{\ell!0!0!}+n\frac{\frac{n+(\ell-4)}{2}\cdots\frac{n-(\ell-2)}{2}}{(\ell-2)!0!1!}+\ldots n\frac{\frac{n-(1*)}{2}\frac{n-(3*)}{2}\cdots\frac{n-(\ell-2)}{2}}{1!0!(\frac{\ell*-1}{2})!})t^{\ell}{}_{-1}r^{\frac{n-\ell}{2}}+$$

$$(n\frac{\frac{n+(\ell-4)}{2}\frac{n+(\ell-6)}{2}\cdots\frac{n-(\ell+4)}{2}}{\ell!2!0!}+n\frac{\frac{n+(\ell-6)}{2}\cdots\frac{n-(\ell+4)}{2}}{(\ell-2)!2!1!}+\ldots n\frac{\frac{n-(3*)}{2}\frac{n-(5*)}{2}\cdots\frac{n-(\ell+4)}{2}}{1!2!(\frac{\ell*-1}{2})!})t^{\ell}(xyz)^2{}_{-1}r^{\frac{n-\ell-6}{2}}\ldots$$

$$+(\frac{n(\frac{n+(\ell-m-2)}{2})(\frac{n+(\ell-m-4)}{2})\ldots(\frac{(n-(\ell+3m-2)}{2})}{\ell!m!0!}+\frac{n(\frac{n+(\ell-m-4)}{2})(\frac{(n+(\ell-m-6)}{2})\ldots(\frac{(n-(\ell+3m-2)}{2})}{(\ell-2)!m!1!}+\ldots$$

$$\frac{n(\frac{n-(m+1*)}{2})(\frac{(n-(m+3*)}{2})\ldots(\frac{(n-(\ell+3m-2)}{2})}{1!m!\frac{(\ell*-1)}{2}!}))t^{\ell}(xyz)^m{}_{-1}r^{\frac{n-\ell-3m}{2}} \qquad (1.15)$$

This gives,

$$t^{\ell}\ \text{terms for}\ x^n + y^n + (-z)^n = \pm\sum_{s=0}^{\lfloor \ell/2 \rfloor}\ \sum_{\substack{m=0 \\ m+n+\ell \equiv 1\, mod\ 2}}^{\lfloor (n-\ell)/3 \rfloor} n(\frac{(\frac{n+(\ell-2s-m-2)}{2})!}{(\ell-2s)!m!s!(\frac{n-3m-\ell}{2})!})t^{\ell}(xyz)^m r^{\frac{n-3m-\ell}{2}} \qquad (1.16)$$

Therefore we can write,

Theorem 1.1 *t* dependent equation *v* = -1, (*n* > 0)

$$x^n + y^n + (-z)^n = \sum_{\ell=0}^{n} \sum_{s=0}^{\lfloor \ell/2 \rfloor} \sum_{\substack{m=0 \\ m+n+\ell \equiv 1 \bmod 2}}^{\lfloor (n-\ell)/3 \rfloor} (-1)^n (-1)^\ell n \left(\frac{\left(\frac{n+(\ell-2s-m-2)}{2}\right)!}{(\ell-2s)!\, m!\, s!\left(\frac{n-3m-\ell}{2}\right)!} \right) t^\ell (xyz)^m r^{\frac{n-3m-\ell}{2}} \quad (1.17)$$

Where r is the v= -1 symmetric $x^2+yz-xt-t^2$

Making $\omega = \frac{n-3m-\ell}{2}$

$$x^n + y^n + (-z)^n = \sum_{\ell=0}^{n} \sum_{s=0}^{\lfloor \ell/2 \rfloor} \sum_{\substack{m=0 \\ m+n+\ell \equiv 1 \bmod 2}}^{\lfloor (n-\ell)/3 \rfloor} (-1)^n (-1)^\ell n \left(\frac{(\omega+\ell-s+m-1)!}{(\ell-2s)!\, m!\, s!(\omega)!} \right) t^\ell (xyz)^m r^\omega \quad (1.18)$$

Corollary 1

$$z^n - x^n = (z-x)^n + n(z-x)^{n-2} zx + \frac{n(n-3)}{2!}(z-x)^{n-4} z^2x^2 + \frac{n(n-4)(n-5)}{3!}(z-x)^{n-6} z^3x^3 +$$

$$\ldots + \frac{n\left(\frac{n-2}{2}\right)\left(\frac{n-4}{2}\right)\ldots 1}{\frac{n}{2}!} (z^{n/2} - x^{n/2}) z^{n/2} x^{n/2} \qquad (n\text{=even})$$

$$\ldots + \frac{n\left(\frac{n-1}{2}\right)\left(\frac{n-3}{2}\right)\ldots 2}{\frac{(n-1)}{2}!} (z-x) z^{(n-1)/2} x^{(n-1)/2} \qquad (n\text{=odd}) \qquad (1.19)$$

Corollary 2

$$x^n + y^n = (x+y)^n - \frac{n!}{(n-1)!} x^{n-1} y - \frac{n!}{1!(n-1)!} xy^{n-1} - \frac{n!}{(n-2)!\,2!} x^{n-2} y^2 - \frac{n!}{2!(n-2)!} x^2 y^{n-2} \ldots$$

$$- \frac{n!}{m!(n-m)!} x^m y^{n-m} - \frac{n!}{(n-m)!\,m!} x^{n-m} y^m \ldots - \frac{n!}{\frac{n}{2}!\,\frac{n}{2}!} x^{n/2} y^{n/2} \qquad (n = \text{even})$$

$$\ldots - \frac{n!}{\frac{(n-1)}{2}!\,\frac{(n+1)}{2}!} x^{(n-1)/2} y^{(n-1)/2} \qquad (n = \text{odd}) \qquad (1.20)$$

First Examples *v* = -1

...

$$x^{-6}+y^{-6}+z^{-6}=(t^{12}+6t^{10}r+6xyzt^{9}+15t^{8}r^{2}+24xyzt^{7}r+20t^{6}r^{3}+3(xyz)^{2}t^{6}+36xyzt^{5}r^{2}+15r^{4}t^{4}+0(xyz)^{2}t^{4}r+24xyzt^{3}r^{3}$$
$$-10(xyz)^{3}t^{3}+6t^{2}r^{5}-9t^{2}(xyz)^{2}r^{2}+6txyzr^{4}-12t(xyz)^{3}r+r^{6}-6(xyz)^{2}r^{3}+3(xyz)^{4})(xyz)^{-6}$$
$$x^{-5}+y^{-5}-z^{-5}=(t^{10}+5t^{8}r+5xyzt^{7}+10t^{6}r^{2}+15xyzt^{5}r+10t^{4}r^{3}+0(xyz)^{2}t^{4}+15xyzt^{3}r^{2}+5r^{4}t^{2}-5(xyz)^{2}t^{2}r+5xyztr^{3}$$
$$-5(xyz)^{3}t+r^{5}-5(xyz)^{2}r^{2})(xyz)^{-5}$$
$$x^{-4}+y^{-4}+z^{-4}=(t^{8}+4t^{6}r+4xyzt^{5}+6r^{2}t^{4}+8xyzrt^{3}+4r^{3}t^{2}-2(xyz)^{2}t^{2}+4xyztr^{2}+r^{4}-4(xyz)^{2}r)(xyz)^{-4}$$
$$x^{-3}+y^{-3}-z^{-3}=(t^{6}+3t^{4}r+3xyzt^{3}+3t^{2}r^{2}+3xyztr+r^{3}-3(xyz)^{2})(xyz)^{-3}$$
$$x^{-2}+y^{-2}+z^{-2}=(t^{4}+2t^{2}r+2xyzt+r^{2})(xyz)^{-2}$$
$$x^{-1}+y^{-1}-z^{-1}=(t^{2}+r)(xyz)^{-1}$$
$$x^{0}+y^{0}+z^{0}=3$$
$$x^{1}+y^{1}-z^{1}=t$$
$$x^{2}+y^{2}+z^{2}=3t^{2}+2r$$
$$x^{3}+y^{3}-z^{3}=4t^{3}+3tr-3xyz$$
$$x^{4}+y^{4}+z^{4}=7t^{4}+8t^{2}r-4xyzt+2r^{2}$$
$$x^{5}+y^{5}-z^{5}=11t^{5}+15t^{3}r-10xyzt^{2}+5r^{2}t-5xyzr$$
$$x^{6}+y^{6}+z^{6}=18t^{6}+30t^{4}r-18xyzt^{3}+15r^{2}t^{2}-12xyztr+2r^{3}+3(xyz)^{2}$$
$$x^{7}+y^{7}-z^{7}=29t^{7}+56t^{5}r-35xyzt^{4}+35r^{2}t^{3}-35xyzt^{2}r+7tr^{3}+7(xyz)^{2}t-7r^{2}xyz$$
$$x^{8}+y^{8}+z^{8}=47t^{8}+104t^{6}r-64xyzt^{5}+80r^{2}t^{4}-80xyzt^{3}r+24t^{2}r^{3}+20(xyz)^{2}t^{2}-24xyztr^{2}+2r^{4}+8(xyz)^{2}r$$
$$x^{9}+y^{9}-z^{9}=76t^{9}+189t^{7}r-117xyzt^{6}+171r^{2}t^{5}-180xyzt^{4}r+66t^{3}r^{3}+45(xyz)^{2}t^{3}-81xyzt^{2}r^{2}+9tr^{4}+27(xyz)^{2}rt-9xyzr^{3}-3(xyz)^{3}$$
$$x^{10}+y^{10}+z^{10}=123t^{10}+340t^{8}r-210xyzt^{7}+355r^{2}t^{6}-380xyzt^{5}r+170t^{4}r^{3}+100(xyz)^{2}t^{4}-220xyzt^{3}r^{2}+35t^{2}r^{4}+90(xyz)^{2}rt^{2}-40xyztr^{3}$$
$$-10(xyz)^{3}t+2r^{5}+15r^{2}(xyz)^{2}$$
$$x^{11}+y^{11}-z^{11}=199t^{11}+605t^{9}r-374xyzt^{8}+715r^{2}t^{7}-781xyzt^{6}r+407t^{5}r^{3}+209(xyz)^{2}t^{5}-561xyzt^{4}r^{2}+110t^{3}r^{4}+242(xyz)^{2}rt^{3}$$
$$-154xyzt^{2}r^{3}-33(xyz)^{3}t^{2}+11r^{5}t+66r^{2}(xyz)^{2}t-11xyzr^{4}-11(xyz)^{3}r$$

....

Computer Verification. One may care to verify these results by computer where $t = x+y-z$ and $r = x^2+yz-xt-t^2=y^2+xz-yt-t^2=z^2-xy+zt-t^2$

There are many corollaries but notable corollaries required for FLT are as follows:

Corollary 3 *When n is a multiple of 3 then the equation ends with* $\pm 3(xyz)^{n/3}$

Proof

From (1.17) with $\ell = 0$, we have $\frac{n-3m}{2}=0$ then $n=3m$ hence,

$$\pm n\frac{(\frac{n-(m+2)}{2})!}{0!m!(\frac{n-3m}{2})!}(xyz)^{m}=\pm n\frac{(m-1)!}{m!}=\pm\frac{3m}{m}=\pm 3(xyz)^{m}$$

Corollary 4 *For n=M3-1 or n=M3+1 and ℓ=0 then the coefficients of $(xyz)^m r$ or $(xyz)^m r^2$ respectively is ±n*

Proof

From (1.17) with $\ell = 0$, we have $\frac{n-3m}{2} = 1$ then $n-3m = 2$ hence,

$$\pm n \frac{(\frac{n-(m+2)}{2})!}{0!m!(\frac{n-3m}{2})!}(xyz)^m r = \pm n \frac{(m)!}{m!}(xyz)^n r = \pm n(xyz)^n r = \pm n(xyz)^m r$$

$\frac{n-3m}{2} = 2$ then $n-3m = 4$

$$\pm n \frac{(\frac{n-(m+2)}{2})!}{0!m!(\frac{n-3m}{2})!}(xyz)^m r = \pm n \frac{(2m)!}{m!2!}(xyz)^n r^2 = \pm n(xyz)^n r^2 = \pm n(xyz)^m r^2$$

Corollary 5 *For n=M3+1 and ℓ=1 then the coefficient of $(xyz)^m t$ is ±n and for n=M3-1 and ℓ=2 then the coefficient of $(xyz)^m t^2$ is ±n(m+3)/2*

Proof

The t sequence for $x^n + y^n + (-z)^n =$

$$\sum_{\substack{m=0 \ even(n\, odd) \\ m=1 \ odd(n\, even)}}^{\lfloor (n-1)/3 \rfloor} \mp n \frac{(\frac{n-(m+1)}{2})!}{1!m!(\frac{n-3m-1}{2})!} t(xyz)^m r^{\frac{n-(3m+1)}{2}} \quad (1.21)$$

for $\frac{n-(3m+1)}{2} = 0$ we get,

$$\mp n \frac{(\frac{n-(m+1)}{2})!}{1!m!(\frac{n-3m-1}{2})!} = \pm n \frac{m!}{m!} t(xyz)^m = \pm nt(xyz)^m$$

The t^2 sequence for $x^n + y^n + (-z)^n$

$$= \pm \sum_{\substack{m=0 \ even(n\, even) \\ m=1 \ odd(n\, odd)}}^{\lfloor (n-2)/3 \rfloor} (n(\frac{(\frac{n-(m)}{2})!}{2!m!(\frac{n-3m-2}{2})!}) + n(\frac{(\frac{n-(m+2)}{2})!}{0!m!(\frac{n-3m-2}{2})!}))t^2(xyz)^m r^{\frac{n-(3m+2)}{2}} \quad (1.22)$$

for $\frac{n-(3m+2)}{2} = 0$ we get,

$$\pm(n(\frac{(\frac{n-(m)}{2})!}{2!m!(\frac{n-3m-2}{2})!}) + n(\frac{(\frac{n-(m+2)}{2})!}{0!m!(\frac{n-3m-2}{2})!}))t^2(xyz)^m = \pm(n\frac{m+1}{2!} + n\frac{m!}{m!})t^2(xyz)^m = \pm n(\frac{m+3}{2})t^2(xyz)^m$$

Corollary 6 *The total sum of the exponents in each term add to n* (*n* > 0) *and 2n (n < 0) if we include the x,y,z degree (xyz) = 3, r = 2 and t = 1 as a weighting factor.*

Proof

Equation (1.17) the total sum is $\ell + m + \frac{n-3m-\ell}{2} \to \ell + 3m + n - 3m - \ell = n$

We therefore have for $n = M3$, lone $(xyz)^{n/3}$ terms (Corollary 3)

For $n=M3$-1we have $(xyz)^{\frac{n-2}{3}} t^2$ and $(xyz)^{\frac{n-2}{3}}{}_{-1}r$ terms in $n > 0$ and vice versa in $n < 0$. For $n=M3+1$ we have $(xyz)^{\frac{n-4}{3}} t$ and $(xyz)^{\frac{n-4}{3}}{}_{-1}r^2$ terms in $n > 0$ (Corollaries 4,5)

Corollary 7 *The first term coefficient is given by the Lucas sequence over n and for n= p(prime) is congruent to 1modp, all the other terms are congruent to 0modp. The first term coefficient is generated from the Lucas function and hence L_n is congruent to 1modn if n is prime* [2]

Proof

We have when $\ell = n$ and $m = 0$ from thm 1.1

$$\sum_{s=0}^{\lfloor n/2 \rfloor} n\frac{(n-s-1)!}{s!((n-2s)!}t^n$$

This is a formula for the Lucas sequence hence and for $n = p$, L_n is congruent to $1 \, mod n$ *if* n is prime [2]

We can see from 1.1 that if $\ell \neq n$ then the denominator factorials are always less than n so if $n = p$ then there is a p term in the numerator hence all terms when $\ell \neq n$ are congrurent to $0 \bmod p$

Corollary 8 *We can apply the t, r, (xyz) representation to any three variable equation of the form $Ax^a+By^b-Cz^c = D$ if we make T equal the equation in question T=D and $X=Ax^a$, $Y=By^b$, $Z=Cz^c$*

T dependent equation,

$$X^n + Y^n + (-Z)^n = \sum_{\ell=0}^{n} \sum_{s=0}^{\lfloor \ell/2 \rfloor} \sum_{\substack{m=0 \\ m+n+\ell \equiv 1 \bmod 2}}^{\lfloor (n-\ell)/3 \rfloor} (-1)^n (-1)^\ell n \left(\frac{\left(\frac{n+(\ell-2s-m-2)}{2}\right)!}{(\ell-2s)!\,m!\,s!\left(\frac{n-3m-\ell}{2}\right)!} \right) T^\ell (XYZ)^m R^{\frac{n-3m-\ell}{2}} \tag{1.23}$$

Where X, Y, Z represents the terms in the equation and $R = X^2 + YZ - XT - T^2 = Y^2 + XZ - YT - T^2 = Z^2 - XY + ZT - T^2$

For example in FLT we have that T= $x^p + y^p - z^p = 0$

so T *is* 0 *and* $R = x^{2p} + y^p z^p - x^p T - T^2 = x^{2p} + y^p z^p$

Hence,

$$(x^p)^n + (y^p)^n + (-z^p)^n = \sum_{\ell=0}^{n} \sum_{s=0}^{\lfloor \ell/2 \rfloor} \sum_{\substack{m=0 \\ m+n+\ell \equiv 1 \bmod 2}}^{\lfloor (n-\ell)/3 \rfloor} (-1)^n (-1)^\ell n \left(\frac{\left(\frac{n+(\ell-2s-m-2)}{2}\right)!}{(\ell-2s)!\,m!\,s!\left(\frac{n-3m-\ell}{2}\right)!} \right) T^\ell (x^p y^p z^p)^m R^{\frac{n-3m-\ell}{2}} \tag{1.24}$$

Hence if $T = 0$ *then we necessarily have* $\ell = 0$ *and we get the* T independent equation

$$(x^p)^n + (y^p)^n + (-z^p)^n = \sum_{\substack{m=0(n,m\ even) \\ m=1(n,m\ odd)}}^{\lfloor n/3 \rfloor} (-1)^n n \frac{\left(\frac{n-(m+2)}{2}\right)!}{0!\,m!\left(\frac{n-3m}{2}\right)!} (x^p y^p z^p)^m (R)^{\frac{n-3m}{2}} \tag{1.25}$$

Where $R = x^{2p} + y^p z^p$

Lemma 1 *If* $x^2 + yz \equiv 0 \bmod q$ *and* $x^p + y^p - z^p = 0$ *then* $x^{2p} + y^p z^p \equiv 0 \bmod q$, $y^{2p} + x^p z^p \equiv 0 \bmod q$, $z^{2p} - x^p y^p \equiv 0 \bmod q$

Proof $x^{2p} + y^p z^p$ can be factored into $x^2 + yz$ since p is odd hence $x^{2p} + y^p z^p \equiv 0 \bmod q$

With $x^p + y^p - z^p = 0$ then $x^{2p} + y^p z^p = x^p(z^p - y^p) + y^p z^p = x^p z^p + y^p(z^p - x^p) = y^{2p} + x^p z^p$

hence if $x^{2p} + y^p z^p \equiv 0 \bmod q$ so must $y^{2p} + x^p z^p \equiv 0 \bmod q$

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

hence if $x^{2p} + y^p z^p \equiv 0 \bmod q$ so must $z^{2p} - x^p y^p \equiv 0 \bmod q$

Lemma 2 *If* $x, y, z \neq 0 \, mod \, q$ *and* $x^p + y^p - z^p = 0$ *, and where* $q > 0$ *is a prime factor of any of the symmetric parts* $R = x^{2p} + y^p z^p \equiv 0 \, mod \, q$ *or* $R = y^{2p} + x^p z^p \equiv 0 \, mod \, q$ *or* $R = z^{2p} - x^p y^p \equiv 0 \, mod \, q$ *we can write;*

$$g^m x^p \equiv 1 \, mod \, q$$
$$g^{3m} y^{3p} \equiv 1 \, mod \, q$$
$$g^{3m} z^{3p} \equiv -1 \, mod \, q$$

Where g^m *is define d as the multiplicative primitive root set generator*

Proof

q has a primitive root g and we use the primitive root as the generator of the multiplicative set of integers *mod ulo* q or g^m generates all residues $mod \, q$, for $0 < m < q$

Lets choose a g^m acting on x^a such that the residue is $1 \, mod \, q$ hence,

$$g^m x^p \equiv 1 \, mod \, q$$

With $x^{2p} + y^p z^p \equiv y^{2p} + x^p z^p \equiv z^{2p} - x^p y^p \equiv 0 \, mod \, q$ from *lemma* 1 *we have*

$g^m x^{2p} + g^m y^p z^p \equiv 0 \, mod \, q$

$x^p + g^m y^p z^p \equiv 0 \, mod \, q$

and with $g^m y^{2p} + z^p \equiv 0 \, mod \, q$

hence, $x^p - g^{2m} y^{3p} \equiv 0 \, mod \, q$

$1 - g^{3m} y^{3p} \equiv 0 \, mod \, q$

and with, $g^m z^{2p} - y^p \equiv 0 \, mod \, q$

$x^p + g^{2m} z^{3p} \equiv 0 \, mod \, q$

$1 + g^{3m} z^{3p} \equiv 0 \, mod \, q$

Therefore,

$$g^m x^p \equiv 1 \, mod \, q \tag{1.26}$$
$$g^{3m} y^{3p} \equiv 1 \, mod \, q \tag{1.27}$$
$$g^{3m} z^{3p} \equiv -1 \, mod \, q \tag{1.28}$$

$\therefore$ we have $$x^{3p} \equiv y^{3p} \mathrm{modq}, \ z^{3p} \equiv -y^{3p} \, mod \, q, \ z^{3p} \equiv -x^{3p} \, mod \, q \tag{1.29}$$

Lemma 3 *If* $g^m x^p \equiv 1 \, mod \, q$ *then*, $g^m y^p \neq 1 \, mod \, q$ *and* $g^m z^p \neq -1 \, mod \, q$ *therefore* $g^{2m} y^{2p}, \, g^{2m} z^{2p} \neq 1 \, mod \, q$

Proof

When $g^m x^p \equiv 1 \, mod \, q$, $g^{3m} y^{3p} \equiv 1 \, mod \, q$, $g^{3m} z^{3p} \equiv -1 \, mod \, q$ then,

$(g^m y^p - 1)(g^{2m} y^{2p} + g^m y^p + 1) \equiv 0 \, mod \, q$, $(g^m z^p + 1)(g^{2m} z^{2p} - g^m z^p + 1) \equiv 0 \, mod \, q$.

If $g^m y^p \equiv 1 \, mod \, q$ or $g^m z^P \equiv -1 \, mod \, q$, then $g^m z^p \equiv 2 \, mod \, q$ or $y^p \equiv -2 \, mod \, q$ respectively

from $\mathrm{g}^m x^p + g^m y^p - g^m z^p = 0$

Then from $g^{2m} x^{2p} + g^{2m} y^p z^p \equiv 0 \, mod \, q$ we get $3 \equiv 0 \, mod \, q$ which it is not

hence $g^m y^p \neq 1 \, mod \, q, g^m z^p \neq -1 \, mod \, q$,

Lemma 4 *We have* 2 *quadratic congruences in* y^p *and* z^p *with* 2 *unique solutions for* y^p, z^p

Proof

We can write $y^{3p} + z^{3p} \equiv 0 \, mod \, q, \ (y^p + z^p)(y^{2p} - y^p z^p + z^{2p}) \equiv 0 \, mod \, q$

If $y^p \equiv -z^p \, mod \, q$ then $2g^m y^p \equiv -1 \, mod \, q, 2g^m z^p \equiv 1 \, mod \, q$ from $g^m \mathrm{x}^p + \mathrm{g}^m \mathrm{y}^p - \mathrm{g}^m \mathrm{z}^p = 0$,

$\therefore 4g^{2m} y^{2p} + 4g^{2m} x^p z^p \equiv 0 \, mod \, q$, and $1 + 2g^m x^p \equiv 0 \, mod \, q$,

which is a contradiction $3 \neq 0 \, mod \, q$ hence $y^p \neq z^p \, mod \, q$ *so* $y^{2p} - y^p z^p + z^{2p} \equiv 0 \, mod \, q$.

So we have 2 quadratic congruences in y^p and z^p with 2 unique solutions for y^p, z^p

Fermat's Last Theorem

$x^n+y^n-z^n = 0$ *has no non zero integer (and hence rational) solutions when* $n > 2$.

Proof

Make n prime (p). We assume that x,y,z have no common divisors for if they did we could factor them out and find a new solution to the equation.

If one of $x,y,z = M3$ then the other 2 variables must be $\pm 1 \bmod 3$ to satisfy $x^p + y^p - z^p = 0$

i.e. $(M3)^p + (M3\pm1)^p - (M3\pm1)^p = 0$

$$\therefore x + y - z = t \equiv 0 \, mod\, 3 \tag{5.01}$$

If $x,y,z \neq M3$ then only $(M3\pm1)^p + (M3\pm1)^p - (M3\mp1)^p = 0$ is allowed, hence $t = M3\pm1 + M3\pm1 - M3\mp1 = M3$

$$\therefore t \equiv 0 \, mod\, 3 \tag{5.02}$$

$x,y,z > 0$ and $t = x+y-z$ so if $x+y<z$ then $z = x+y+d$ and $x^p + y^p - (x+y+d)^p < 0$ an inequality, hence $t > 0$

With $z > x,y$ and $r' = x^2 + yz$ $\therefore r' > 0$ and r' is odd as one of x,y,z must be even and t is even. Furthermore, $x^2 + yz > t$ i.e $(z-y+t)^2 + yz > t$. We can also show this for $r(y/t),\ r(-z/t)$. (5.03)

Using $r' = x^2 + yz$, lets make q a prime decomposition factor of r' which is odd > 3

Proposition 5 For all the cases of q we show that $t \equiv 0 \, mod\, q$ or x,y,z share common factor q or we get a contradiction modulo q.

If $q = 3$ then $t \equiv 0 \, mod\, q$ as above, otherwise We need to define 2 cases (plus 2 sub-cases) when $q \neq 3$:

1) $q \neq 3sp+1$ (5.05)

1b) $q = sp+1,\ s \neq M3$ (5.06)

1c) $q = 3s+1,\ s \neq Mp$ (5.07)

2) $q = 3sp+1$ (5.08)

Case 1. Write $lp = uq - v$ and make $u - v = 1$. This is an extention of Bezoult's lemma where q,p are co-prime or if $q = p$ then GCD is $p\ (v = Mp)$. Hence,

$$lp = (v+1)q - v = v(q-1) + q \tag{5.09}$$

Choose v such that $v(q-1)+q = lp$ where $l \neq M3$ and from our (T independent) representation (Corollary 8) with $T = 0$

$$(x^p)^l + (y^p)^l - (z^p)^l = 0 - l(xyz)^p((R)^{\frac{(l-3)}{2}} + \frac{(\frac{l-5}{2})(\frac{l-7}{2})}{3!}(xyz)^{2p}(R)^{\frac{(l-9)}{2}} + \frac{(\frac{l-7}{2})(\frac{l-9}{2})(\frac{l-11}{2})(\frac{l-13}{2})}{5!}(xyz)^{4p}(R)^{\frac{l-15}{2}}$$

$$... + \frac{(\frac{(l-(n+2))}{2})(\frac{(l-(n+4))}{2})...(\frac{(l-(3n-2))}{2})}{m!}(xyz)^{(m-1)p}(R)^{\frac{l-3m}{2}}) \tag{5.10}$$

$LHS \equiv t \, mod\, q$ i.e. $(x+y-z) + Mq = t + Mq = t \, mod\, q$ if $x,y,z \neq Mq$ (from Fermat's little theorem)

$RHS \equiv 0 \, mod\, q$. $(R = x^{2p} + y^p z^p - 0x^p - 0 = Mr)$

$$\therefore t \equiv 0 \, mod\, q \tag{5.11}$$

Remark: If one of x,y,z contain q then so do the other 2 variables and we have a common factor solution which must factor out.

Case 1b) Write $lp = uq - v$ and make $u - v = 3p$,

$$lp = \left(v + 3p\right)q - v = v\left(q - 1\right) + 3pq \tag{5.12}$$

$l = vs + 3q$ where s is even $\neq 3 \therefore$ l is odd $\neq M3$ hence from (C.29), $T = 0$.

$$(x^p)^l + (y^p)^l - (z^p)^l = 0 - l(xyz)^p((R)^{\frac{(l-3)}{2}} + \frac{(\frac{l-5}{2})(\frac{l-7}{2})}{3!}(xyz)^{2p}(R)^{\frac{(l-9)}{2}} + \frac{(\frac{l-7}{2})(\frac{l-9}{2})(\frac{l-11}{2})(\frac{l-13}{2})}{5!}(xyz)^{4p}(R)^{\frac{l-15}{2}}$$

$$... + \frac{(\frac{(l-(n+2))}{2})(\frac{(l-(n+4))}{2})...(\frac{(l-(3n-2))}{2})}{m!}(xyz)^{(m-1)p}(R)^{\frac{l-3m}{2}}) \tag{5.13}$$

$LHS = x^{3p} + y^{3p} - z^{3p} \bmod q$ if $x, y, z \neq Mq$

$RHS \equiv 0 \bmod q$

$$\therefore -3(xyz)^p \equiv 0 \bmod q \tag{5.14}$$

Hence we get common factor solutions in this case.

Case 1c) Write $lp = uq - v$ and make $u - v = 1$,

$$lp = \left(v + 1\right)q - v = v\left(q - 1\right) + q \tag{5.15}$$

$lp = v3s + q$ where s is even $q \neq M3 \therefore$ l is odd $\neq M3$.

$$(x^p)^l + (y^p)^l - (z^p)^l = 0 - l(xyz)^p((R)^{\frac{(l-3)}{2}} + \frac{(\frac{l-5}{2})(\frac{l-7}{2})}{3!}(xyz)^{2p}(R)^{\frac{(l-9)}{2}} + \frac{(\frac{l-7}{2})(\frac{l-9}{2})(\frac{l-11}{2})(\frac{l-13}{2})}{5!}(xyz)^{4p}(R)^{\frac{l-15}{2}}$$

$$... + \frac{(\frac{(l-(n+2))}{2})(\frac{(l-(n+4))}{2})...(\frac{(l-(3n-2))}{2})}{m!}(xyz)^{(m-1)p}(R)^{\frac{l-3m}{2}}) \tag{5.16}$$

$LHS \equiv t \bmod q$ if $x, y, z \neq Mq$

$RHS \equiv 0 \bmod q$

$$\therefore t \equiv 0 \bmod q \tag{5.17}$$

Case 2) With $q = 3sp + 1$, we can factor r' from $R = x^{2p} + (yz)^p$ *by* Lemma1

For case 2 we need to uniquely define $x^p+y^p-z^p=0$ as opposed to $x^p+y^p-z^p\equiv 0 \bmod q$. This is done via this lemma 5

Lemma 5, *If $x^p+y^p-z^p=0$ then Case 1) We can write $x+y=c^p$, $z-y=a^p$, $z-x=b^p$ if $x^p+y^p-z^p=0$ if p does not divide x,y,z*

Case 2) If one of x,y,z=Mp then we can write $z-y=p^{p-1}a^p$, $z-x=p^{p-1}b^p$, $x+y=p^{p-1}c^p$ respectively

Proof

Case 1) With $n = p$ factor out $x + y = C$ therefore C must divide z

Make $z = cw$ where c is any common divisor of $(x + y)$ and z

From Corollory 2 (see extract 2) we have,

$$x^p + y^p - z^p = (x+y)\{(x+y)^{p-1} - p(x+y)^{p-3}xy + \frac{p(p-3)}{2!}(x+y)^{p-5}x^2y^2....$$

$$... + p(x^{(p-1)/2}y^{(p-1)/2})\} - z^p \tag{5.22}$$

Hence, $(x + y) = c^p$ otherwise xy would share all common factors with z (excluding p) which is not possible in the special case.

Therefore, if p does not divide C then $x + y = C = c^p$ and $z = cw$

and z^p is divisable by all of $x + y$

Similarly, $z - y = A$ must divide x^p and from Corollory 1(see extract 2) $z - y = A = a^p$ and $x = au$

and $z - x = B = b^p$ and $y = bv$ for $a, b, c > 0$

Furthermore, if none of A, B, C contain p then we have,

$$x = au = A + t \quad = a^{p} + t \quad \text{and}\, a / t \tag{5.23}$$

$$y = bv = B + t \quad = b^{p} + t \quad \text{and}\, b / t \tag{5.24}$$

$$z = cw = C - t \quad = c^{p} + t \quad \text{and}\, c / t \tag{5.25}$$

Furthermore, $(x+y)^{p} - z^{p} = Mp$ hence $C - z = Mp$ but $C - z = t \therefore \; p / t$

Moreover we now can write , $A + B - C = -2t$

Hence ,

$$a^{p} + b^{p} - c^{p} = -2t = -2mpabc \tag{5.26}$$

Case 2) If p divides, say C, and hence z then we have $C = p^{p-1}c^{p}$

However, the other terms A, B will not contain p otherwise we have a common factor p.

Because we have a p coefficient in the last term of corollary 2 the shared common factor p between $x + y$ and z does not need to be to the power p but one less p -1.

So lets say $p = 5$ and $x + y = p^{5}$ and $z^{5} = p^{5}w^{5}$ So from corollary 2

$\mathrm{p}^{p}w^{p} = p^{p}\{(p^{5})^{4} - p(p^{5})^{2}xy + px^{2}y^{2}\}$

$w^{p} = \{(p^{5})^{4} - p(p^{5})^{2}xy + px^{2}y^{2}\}$

hence $w = Mp$ and in turn $xy = Mp$ giving common factor solutions p

Therefore, $x + y = p^{p\text{-}1}c^{p}$ where c is the other shared factors as above.

If $g^{m}x^{p} \equiv 1 \bmod q, g^{3m}y^{3p} \equiv 1 \bmod q,\; g^{3m}z^{3p} \equiv -1 \bmod q$ and $q = 3sp + 1$ then from lemma 3, 4 either:

$$g^{sp}z^{p} \equiv -y^{p} \bmod q \;\text{ and }\; \mathrm{g}^{sp}x^{p} \equiv -z^{p} \bmod q \;\textit{ and }\; g^{sp}y^{p} \equiv x^{p} \bmod q \tag{5.27}$$

or

$$g^{2sp}z^{p} \equiv -y^{p} \bmod q \;\text{ and }\; g^{2sp}x^{p} \equiv -z^{p} \bmod q \;\text{ and }\; g^{2sp}y^{p} \equiv x^{p} \bmod q \tag{5.28}$$

Lemma 6 *We can also write* $g^{(3l+1)sp}z^{p} \equiv -y^{p} \bmod q$ for $l = 0, 1, 2 \ldots (p-1)$ *etc. for each of these congruences. There must exist one* $\ell = 3l + 1$ *such that* $g^{\ell s}z \equiv -y \bmod q$

Proof Write,

$g^{sp}z^{p} \equiv -y^{p} \bmod q$

$g^{s(4)p}z^{p} \equiv -y^{p} \bmod q$

$g^{s(7)p}z^{p} \equiv -y^{p} \bmod q$

$\vdots$

$g^{s(\ell)p}z^{p} \equiv -y^{p} \bmod q$

$\vdots$

$g^{s(3(p-1)+1)p}z^{p} \equiv -y^{p} \bmod q$

Factoring we get,

$(g^{s}z + y)(g^{s(p-1)}z^{p-1} - g^{s(p-2)}z^{p-2}y \ldots + y^{p-1})$

$(g^{4s}z + y)(g^{4s(p-1)}z^{p-1} - g^{4s(p-2)}z^{p-2}y \ldots + y^{p-1})$

$\vdots$

$(g^{s(3p-2)}z + y)(g^{s(3p-2)(p-1)}z^{p-1} - g^{s(3p-2)(p-2)}z^{p-2}y \ldots y^{p-1})$

We have p rows with each one having a unique solution otherwise we get common factor solutions if they share the same solution. Since there are at most $p-1$ unique solutions in the second brackets there must be one solution in the first braket on any particular row.

Likewise for the other relations so we can write a table as follows;

Table 1 g^{sp}

$g^{s}z \equiv -y \bmod q$	$g^{s}x \equiv -z \bmod q$	$g^{s}y \equiv x \bmod q$
$g^{4s}z \equiv -y \bmod q$	$g^{4s}x \equiv -z \bmod q$	$g^{4s}y \equiv x \bmod q$
$g^{7s}z \equiv -y \bmod q$	$g^{7s}x \equiv -z \bmod q$	$g^{7s}y \equiv x \bmod q$
$\vdots$	$\vdots$	$\vdots$
$g^{\ell_1 s}z \equiv -y \bmod q$	$g^{\ell_2 s}x \equiv -z \bmod q$	$g^{\ell_3 s}y \equiv x \bmod q$
$\vdots$	$\vdots$	$\vdots$
$g^{(3p-2)s}z \equiv -y \bmod q$	$g^{(3p-2)s}x \equiv -z \bmod q$	$g^{(3p-2)s}y \equiv x \bmod q$

or g^{2sp}

$g^{2s}z \equiv -y \bmod q$	$g^{2s}x \equiv -z \bmod q$	$g^{2s}y \equiv x \bmod q$
$g^{5s}z \equiv -y \bmod q$	$g^{5s}x \equiv -z \bmod q$	$g^{5s}y \equiv x \bmod q$
$g^{8s}z \equiv -y \bmod q$	$g^{8s}x \equiv -z \bmod q$	$g^{8s}y \equiv x \bmod q$
$\vdots$	$\vdots$	$\vdots$
$g^{\ell_4 s}z \equiv -y \bmod q$	$g^{\ell_5 s}x \equiv -z \bmod q$	$g^{\ell_6 s}y \equiv x \bmod q$
$\vdots$	$\vdots$	$\vdots$
$g^{(3p-1)s}z \equiv -y \bmod q$	$g^{(3p-1)s}x \equiv -z \bmod q$	$g^{(3p-1)s}y \equiv x \bmod q$

Lemma 7: *When one of $x^2+yz\equiv 0 \bmod q$, $y^2+xz\equiv 0 \bmod q$, $z^2-xy\equiv 0 \bmod q$ then two of the solutions to lemma 6 must fall on the same row.*

Proof

There are a number of ways to show this. We have $x^2+yz \equiv 0 \bmod q$ hence we have,

$g^{n}x \equiv y \bmod q$ for some g^{n} if $x, y, z \neq Mq$

$g^{n}x^2 + g^{n}yz \equiv 0 \bmod q$

$y(x+g^{n}z) \equiv 0 \bmod q$

so we have $g^{-n}y \equiv x \bmod q$ and $g^{-n}x \equiv -z \bmod q$ (so $\ell_2 = \ell_3$ in the top table)

For $y^2+xz \equiv 0 \bmod q$, $\ell_1 = \ell_3$

For $z^2-xy \equiv 0 \bmod q$, $\ell_1 = \ell_2$

For x^2+yz and our two lemma 7 solutions being on the same row, they must be on the *ps* or 2ps row. because by lemma5 taken together we have $g^{\ell s}(x+y)\equiv(x-z) \bmod q \rightarrow g^{\ell s}c^p\equiv -b^p \bmod q$ But we must have a $g^{n}c\equiv -b \bmod q$ if $a,b,c\neq Mq$ hence raising both sides to p means $\ell=Mp$

There is only one p exponent on each of the tables if $s\neq Mp$ and this occurs 1/3 partition points; *2ps* and *ps*.

For Case 2 of lemma 5 depending on which x,y,z is divisible by p we choose a decomposition term such that we have two of a^p,b^p,c^p giving the 1/3, 2/3 partition points;

If $x=Mp$ then choose x^2+yz

If $y=Mp$ then choose y^2+xz

If $z=Mp$ then choose z^2-xy

These 1/3, 2/3 points mean $t\equiv 0 \bmod q$ as follows.

We work out what a^p is in terms of b^p and c^p for example. This is independent on what the first column solution is and is only dependent on the *ps* or *2ps* solution given by lemma 5 and 7

Write $g^{\ell_1 s} z - g^{2ps} x \equiv a^p \bmod q$

$g^{sp}(g^{\ell_1 s-2sp}-1)z + g^{2sp}(z-x) \equiv a^p \bmod q$

and write $-g^{\ell_1 s} z - g^{2sp} y \equiv c^p \bmod q$

$-g^{sp}(g^{\ell_1 s-2sp}-1)z - g^{2sp}(z-y) \equiv c^p \bmod q$

$$\therefore g^{2sp} b^p - g^{2sp} a^p \equiv a^p + c^p \bmod q \tag{5.29}$$

(Hence it is independent of ℓ_1) but $g^{2sp} c^p \equiv -b^p \bmod q$

$$\therefore -(g^{2sp}+1)a^p \equiv (g^{4sp}+1)c^p \bmod q \tag{5.30}$$

Now $(g^{2sp}+1)(g^{sp}+1)^{-1} \equiv g^{2sp} \bmod q$ since $g^{3sp} \equiv 1 \bmod q$

$$\therefore g^{2sp} a^p \equiv -c^p \bmod q \tag{5.31}$$

Next we have from (5.29)

$g^{4sp} b^p - g^{4sp} a^p \equiv g^{2sp} a^p - b^p \bmod q$

$$\therefore (g^{4sp}+1)b^p \equiv g^{2sp}(g^{2sp}+1)a^p \bmod q \tag{5.32}$$

$b^p \equiv g^{sp} a^p \bmod q$ or $g^{2sp} b^p \equiv a^p \bmod q$

Hence we can write; $g^{2sp} a^p + g^{2sp} b^p - g^{2sp} c^p \equiv -c^p + a^p + b^p \bmod q$

$g^{2sp}(-2t) \equiv -2t \bmod q$

$(g^{2sp}-1)2t \equiv 0 \bmod q$ and since $(g^{2sp}-1) \neq 0 \bmod q$

$$\therefore t \equiv 0 \bmod q \tag{5.33}$$

Therefore, t must also be divisible by $q=3sp+1$, $s\neq Mp$. However, this is not necessarily true when $q=3sp^n+1$ for $n>1$. To generalize to all n we do the following.

Lemma 8 *If* $q = 3sp^n + 1$ *and* $x^p + y^p - z^p = 0$ *then we also have* $x^{p^n} + y^{p^n} - z^{p^n} = 0$

Proof

Starting with $q = 3sp^2 + 1$ we can write from the lemma 6 **Table 1**

$$\begin{array}{lll}
g^{sp} z \equiv -y \bmod q & g^{sp} x \equiv -z \bmod q & g^{sp} y \equiv x \bmod q \\
g^{4sp} z \equiv -y \bmod q & g^{4sp} x \equiv -z \bmod q & g^{4sp} y \equiv x \bmod q \\
g^{7sp} z \equiv -y \bmod q & g^{7sp} x \equiv -z \bmod q & g^{7sp} y \equiv x \bmod q \\
\vdots & \vdots & \vdots \\
g^{\ell_1 sp} z \equiv -y \bmod q & g^{\ell_2 sp} x \equiv -z \bmod q & g^{\ell_3 sp} y \equiv x \bmod q \\
\vdots & \vdots & \vdots \\
g^{(3p-2)sp} z \equiv -y \bmod q & g^{(3p-2)sp} x \equiv -z \bmod q & g^{(3p-2)sp} y \equiv x \bmod q
\end{array}$$

Assume the g^{sp} solution and ℓ_1, ℓ_2, ℓ_3 are solutions respectively.

One can see if $q = 3sp^2 + 1$ we have the exponents of g being multiples of p

From lemma 5 we have $x = au,\ y = bv,\ z = cw$

There is no loss of generality if we write $g^{\ell_2 sp} x = -z + dq$ where $d \neq 0 \bmod a$ or $d \neq 0 \bmod u$, since $x = au$ and if $z = M(a,u)$ they would share common factors a, u.

Moreover, there must exist an α such that $g^{\ell_2 s}\alpha \equiv \delta \bmod q$ for some $\alpha, \delta \neq 0 \bmod q$ where δ is the residue $\bmod q$ whereby rising it to p we have $\delta^p \equiv -z \bmod q$

Example, if $-z \equiv 2 \bmod 151$ then $\delta = 22$ if $p = 5$

Also without loss of generality we can write, $g^{\ell_2 s}\alpha \equiv \delta + hq$ ($h \neq 0 \bmod a$ or $h \neq 0 \bmod q$)

We can add $g^{\ell_2 s} h_i$ to both sides for $h_1 = 0,1,2 \ldots i$, $0 \le i < a$ or $0 \le i < u-1$ thereby giving us,

$$g^{\ell_2 s}(\alpha + h_i) = \delta + (h + g^{\ell_2 s} h_i) q \tag{5.34}$$

Hence,

$$g^{\ell_2 sp}(\alpha')^p = (\delta + (h + g^{\ell_2 s} h_i) q)^p = -z + f' q \tag{5.35}$$

where $\alpha' = \alpha + h_i$

We can get all residues $\bmod a$ or $\bmod u$ on the RHS by adjusting h_i such that $f' \equiv d \bmod a$ or $f' \equiv d \bmod u$ because $z, g, q \neq 0 \bmod a$ or $\neq 0 \bmod u$

(Note: if $a = g$ or $u = g$ then choose another primitive root as q is now large $3sp^2 + 1$ and has many primitive roots)

Therefore, if we make the residue $d \bmod a$ or $d \bmod u$ we have

$$g^{\ell_2 sp} x - g^{\ell_2 sp}\alpha'^p = Maq, \text{ or } = Muq \tag{5.36}$$

Moreover, since $x = au$ then $\alpha^p = Ma^p$ or Mu^p

Example: Let $p = 5,\ q = 151,\ a = 7,\ -z \equiv 2 \bmod 151,\ d \equiv 5 \bmod q,\ f = h + g^{\ell_2 s}(0,1,2,3,4,5,6) = 0,1,2,3,4,5,6 \bmod a$
$\rightarrow (22+0q)^p - 2 \equiv (5 \bmod 7)q, (22+1q)^p - 2 \equiv (2 \bmod 7)q,\ (22+2q)^p - 2 \equiv (4 \bmod 7)q,\ (22+3q)^p - 2 \equiv (1 \bmod 7)q,$
$(22+4q)^p - 2 \equiv (6 \bmod 7)q,\ (22+5q)^a - 2 \equiv (3 \bmod 7)q,\ (22+6q)^a - 2 \equiv (0 \bmod 7)q$

Hence if $d = d'a + 5$ then we choose $(22+0q)^p \equiv 5 \bmod a,$

Furthermore, we can get all residues in the coeficients of the $a, a^2, a^3 \ldots a^p$ terms $\bmod a$ (that being $d', d'' \ldots$ etc.) or $u, u^2, u^3 \ldots u^p \bmod u$ by adding multiples of $a,\ u$ respectively and since $d' \equiv (0,1 \ldots a-1) \bmod a$ we can make $M = m'a$ *or* $m'a^2 \ldots\ m'a^{p-1}$ giving $g^{\ell_2 sp} x - g^{\ell_2 sp}\alpha'^p = m'a^2 \ldots m'a^p$ hence we can make $x = Ma^p$. Likewise $x = Mu^p$

Example: as above if we add $n7q, (0 \le n < 7)$ to both sides of [5.29] for $(22+0q)^p - 2 \equiv 5 \bmod a$, we get
$\rightarrow ((3 \bmod 7)7 + 5 \bmod 7)q, ((1 \bmod 7)7 + 5 \bmod 7)q, ((6 \bmod 7)7 + 5 \bmod 7)q,\ ((4 \bmod 7)7 + 5 \bmod 7)q,$
$((2 \bmod 7)7 + 5 \bmod 7)q,\ ((0 \bmod 7)7 + 5 \bmod 7)q$

So we can add multiples of $aq, a^2q...a^{p-1}q$ and $uq, u^2q...u^{p-1}q$ to both sides of (5.34) to get the exponentiation of $x=(au)^p=(x')^p$ where x' is obviously less than x or we could view it as x is a power.

Remark, we can do this because we have $g^{\ell_2 p}$ in our table1 which can be eliminated in (5.36). If we did not have p in the exponent then we could not eliminate it leaving g^n terms meaning a^p, u^p would not necessarily divide x.

Likewise, we can do this for the other columns of table 1 to get $y=(bv)^p=(y')^p$, $z=(cw)^p=(z')^p$
Hence, we can write

$$x'^{p^2}+y'^{p^2}-z'^{p^2}=0 \tag{5.37}$$

One can see from Lemma 5 $x'+y'=c'^{p^2}, z'-y'=a'^{p^2}, z'-x'=b'^{p^2}$ and a', b', c' do not necessarily equal a, b, c

Now we have from Lemma 1 that $x^{2p}+y^pz^p=y^{2p}+x^pz^p=z^{2p}-x^py^p$ which is the same as
$x'^{2p^2}+y'^{p^2}z'^{p^2}=y'^{2p^2}+x'^{p^2}z'^{p^2}=z'^{2p^2}-x'^{p^2}y'^{p^2}$

Therefore, we get $x'^{3p^2}\equiv y'^{3p^2}\equiv z'^{3p^2} \bmod q$

We have from table 1 and lemma 6
$g^{\ell_2 sp}x'^p\equiv -z'^p \bmod q,\ g^{\ell_2 sp}y'^p\equiv x'^p \bmod q$

However, now $\ell_2=Mp$ for we have $z'-x'=b'^{p^2}$, $x'+y'=c'^{p^2}$ so if we have $g^{\ell_2 s}x'\equiv -z' \bmod q$ then $\ell_2=Mp^2$ and this is the $1/3, 2/3$ solution points. Therefore $t'=x'+y'-z'\equiv 0 \bmod q$ and $t=x+y-z\equiv 0 \bmod q$.

We can repeat this for $q=3sp^3+1$ to give $x''^{p^3}+y''^{p^3}-z''^{p^3}=0$ etc. ...$q=3sp^n+1$
$\rightarrow x'''^{...p^n}+y'''^{...p^n}-z'''^{...p^n}=0$ and we get smaller triples $x'''<x''<x'<x$ etc. as n increases.
The above arguments hold for all n therefore all $q's$ divide t

Theorem 2.1

If $x^p+y^p-z^p=0$ and suppose x,y,z are pairwise co–prime then any prime factor q of (x^2+yz) will divide t where $t=x+y-z$

Corollary 39

Theorem 2.1 is valid for any prime factor q of (y^2+xz) or (z^2-xy)

This follows from the symmetry of the problem and methods above

Closing Argument

If we have common factors, the special case $x^n+y^n-z^n=0$ loses no generality in assuming that the greatest common divisor of *x; y* and *z* is 1. Hence *t* must contain all the prime decompositions q of (x^2+yz).

We can now use 3 inequality arguments for exponent p in $x^p+y^p-z^p$ congruent to 1 modulo 3, congruent to 2 modulo 3, and exponent $p=q$. We need our equation 1.1 in primes p and Corollaries 9,15,18.
We will write ${}_{x/t}r=x^2+yz=q_1^{\boldsymbol{q}(q_1)}q_2^{\boldsymbol{q}(q_2)}q_3^{\boldsymbol{q}(q_3)}...q_n^{\boldsymbol{q}(q_n)}$ where q_i is prime and $\boldsymbol{q}(q_i)$ is defined to be the highest power of q_i dividing x^2+yz.

Lemma 9: *For exponent $p>3$ congruent to 1 modulo 3 and $q_i \neq$ exponent p then $t = M\ {}_{x/t}r$*

Proof. If $\boldsymbol{q}(q_1), \boldsymbol{q}(q_2), \boldsymbol{q}(q_3)...\boldsymbol{q}(q_n)$ are all equal to 1 then $t = M\ {}_{x/t}r$ but $x^2+yz>t$ from [5.03].
Hence, we have an inequality and contradiction. Therefore one or more of $\boldsymbol{q}(q_1), \boldsymbol{q}(q_2), \boldsymbol{q}(q_3)...\boldsymbol{q}(q_n) > 1$
Lets firstly assume $\boldsymbol{q}(q_1) = 2$

From corollaries 9,15,18 we have $x^p + y^p - z^p = Mq_1^3 + p(xyz)^{m+1}t - p(x^2+yz-xt-t^2)^2(xyz)^m = 0$ (5.38)

One can see $p(xyz)^{m+1}t = Mq_1^2$ because the last term $p(x^2+yz-xt-t^2)^2(xyz)^m = Mq_1^2$

hence $t = Mq_1^2$ because (xyz) gives us common factors q in $x; y$ and z

then $t = M\ {}_{x/t}r$ but $x^2+yz>t$ hence we have an inequality and contradiction as before.

Lets make $\boldsymbol{q}(q_1) = 3$ we still get $t = Mq_1^2$ so then the higher terms in $t^2{}_{-1}r$ or $t_{-1}r^3 = Mq_1^6$ we write,

$x^p + y^p - z^p = Mq_1^6 + p(xyz)^{m+1}t - p(x^2+yz-xt-t^2)^2(xyz)^m = 0$ (5.39)

Hence, $p(xyz)^{m+1}t = Mq_1^4$ and $t > x^2+yz$ but $x^2+yz>t$ hence we have an inequality and contradiction as before.

Next make $\boldsymbol{q}(q_1) = 4$ we still get $t = Mq_1^4$ and our higher terms become Mq_1^8 hence,

$x^p + y^p - z^p = Mq_1^8 + p(xyz)^{m+1}t - p(x^2+yz-xt-t^2)^2(xyz)^m$ and $t = Mq_1^8$ and we get our contradiction again.

Therefore, for any $\boldsymbol{q}(q_1)$ we get $t = Mq_1^{2\boldsymbol{q}(q_1)}$. As q_1 in x^2+yz increases in powers $\boldsymbol{q}(q_1)\ \therefore\ t$ increases in powers $2\boldsymbol{q}(q_1)$ so then must the higher terms containing higher $t,_{-1}r$ combinations which in turn increases t and we continue to get the contradiction as $\boldsymbol{q}(q_1) \to \infty$.
One can see this is true for all $\boldsymbol{q}(q_1), \boldsymbol{q}(q_2), \boldsymbol{q}(q_3)...\boldsymbol{q}(q_n) \geq 1$ so we can conclude $t = M\ {}_{x/t}r$ which is a contradiction ${}_{x/t}r > t$.

Lemma 10: *For exponent $p>3$ congruent to 2 modulo 3 and $q_i \neq$ exponent p then $t = M\ {}_{x/t}r$*

Proof. If $\boldsymbol{q}(q_1), \boldsymbol{q}(q_2), \boldsymbol{q}(q_3)...\boldsymbol{q}(q_n)$ are all equal to 1 then $t = M\ {}_{x/t}r$ but $x^2+yz>t$ from [5.03].
Hence we have an inequality and contradiction. Therefore one or more of $\boldsymbol{q}(q_1), \boldsymbol{q}(q_2), \boldsymbol{q}(q_3)...\boldsymbol{q}(q_n) > 1$
Lets firstly assume $\boldsymbol{q}(q_1) = 2$

From corollaries 9,15,18 we have $x^p + y^p - z^p = Mq_1^3 - p\dfrac{m+3}{2}(xyz)^m t^2 - p(xyz)^m(x^2+yz-xt-t^2) = 0$ (5.40)

hence, $xt = Mq_1^2$ in the last term ${}_{-1}r$ but x gives us common factor q_1 in $x; y$ and z so $t = Mq_1^2$

then $t = M\ {}_{x/t}r$ but $x^2+yz>t$ hence we have an inequality and contradiction as before.

Lets make $\boldsymbol{q}(q_1) = 3$ we still get $t = Mq_1^2$ and higher terms in $t_{-1}r^2$ and $t^3{}_{-1}r = Mq_1^6$ we write,

$x^p + y^p - z^p = Mq_1^6 - p\dfrac{m+3}{2}(xyz)^m t^2 - p(xyz)^m(x^2+yz-xt-t^2) = 0$ (5.41)

$\therefore xt = Mq_1^3$ hence $t = Mq_1^3$ and we get a contradiction as before

Next make $\boldsymbol{q}(q_1) = 4$ we still get $t = Mq_1^3$ and hence $xt = Mq_1^4$ and $t = Mq_1^4$ and we get a contradiction again

Therefore, for any $\boldsymbol{q}(q_1)$, we get $t = Mq_1^{\boldsymbol{q}(q_1)}$ and we get a contradiction as $\boldsymbol{q}(q_1) \to \infty$.

One can see this is true for all $\boldsymbol{q}(q_1), \boldsymbol{q}(q_2), \boldsymbol{q}(q_3)...\boldsymbol{q}(q_n) \geq 1$ so we can conclude $t = M\ {}_{x/t}r$ which is a contradiction ${}_{x/t}r > t$.

From Corollary 20, in that the coefficients of all terms are congruent to $0 \bmod p$ except the first we need to make sure the contradiction still works for $q_i = p$ or ${}_{x/t}r$ contains a power of p

Lemma 11 *For exponent* $p>3$ *and* $q_i = p$ *then lemma* $11{,}12$ *are unchanged;* $t = M_{x/t}r$
From corollary 20 the coefficients of all terms are congrurent to $0 \, mod \; p$ except the first which is congrurent to $1 \, mod \; p$ so if $t = Mp$ then we divide out p leaving the relavent end terms coefficents equal to 1 so we have the same form of the equation but with the first term t^p deminished by p so that term is Mp^{n-1} however this term is irrelevant in the above arguments so our contradiction holds in this case too.

For $p=3$ we get directly $3xyz \equiv 0 \, mod \; q$ if $q>3$ hence common factor solutions again.
If $q=3$, and since $t = M3$ then $3xyz = M3^2$ therefore, one of $x, y, z = M3$ and then so must the other 2 variables hence share a common factor 3. (5.42)

Remark $t \neq 0$ even if x or y is negative for we would just rearranged the equation for odd exponents
i.e if y is a negative integer $x^n - y^n = z^n$ becomes $y^n + z^n = x^n$ and x becomes the higher term but in that case we would just write $x \leftrightarrow z$

With $n=4$ solved by Fermat we can conclude there are no discrete solutions to Fermat's equation for $n>2$.