ON FERMAT'S EQUATION AND THE GENERAL CASE

C. Sloane

(Feb 2017)

Abstract

We discovered a beautiful symmetry to the equation $x^n+y^n\pm z^n$, first studied by Fermat, in a dependent variable $t = x+y-z$ and the product (xyz) if we introduce a term we call the symmetric $r = x^2+yz-xt-t^2$. Once $x^n+y^n\pm z^n$ is written in terms of powers of t, r and (xyz) we looked at the coefficient vs. exponent abstract space and found Lucas, Fibonacci and Convoluted Fibonacci sequences among other corollaries. We also found that 3 cases of a prime decomposition factor q of x^2+yz gave certain results for Fermat's Last Theorem which could be eliminated if a forth case could also be solved. Intrigued by this, we then introduce partial congruence representations modulo a prime for this much harder forth case to find the 'form' of the solutions *modulo q*. The form of the solutions leads us to a cubic congruence method that solves the special and general cases. There are several pages and stages of the proofs where computer verification of the results is possible.

Introduction

When studying the equation $x^n+y^n\pm z^n$ we found that a particular approach to Fermat's Last Theorem (FLT) was giving back our original starting point. We analyzed why this was so and found that a certain term $x^2+yz-xt-t^2$ was the cause, thereby making that approach to FLT intractable. So what we did, was try and put the equation in terms of this new term, which we called the symmetric *r*. What we initially found with small *n* was a separation of *t* and (*xyz*) and so we 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 with this new term $x^2+yz-xt-t^2$. Once we had done this, we looked at the structure of this equation and found many corollaries including Lucas, Fibonacci and convoluted Fibonacci sequences over the exponents *n*. We next recognized that if we take a prime decomposition factor (*q*) of x^2+yz for example, we can show that with this new transformation or representation of Fermat's equation for $n=p$ gives us $t\equiv 0 mod q$ or we get common factor solutions for 3 cases of *q*. The forth case however, proved a lot more difficult and had us introducing partial congruence's and primitive roots to build a picture of the form of the solutions *modulo q* for this case. Once we discovered the 'form' of the congruence solutions we then use a cubic congruence method that eliminates solutions (congruence contradictions), gives common factor solutions or makes $t\equiv 0 mod q$. In the general case (Beal's conjecture) this method also puts constraints on the exponents. Lastly we show that if $t\equiv 0 mod q$ then $t\to\infty$ using this new representation of Fermat's equation.

Definitions

We define the dependent variable *t* as $t= x+y-z$ to reflect Fermat's equation. However, the definition of *t* depends on the plus/minus form of the fundamental equation $\pm x^n\pm y^n \pm z^n$ including the odd/even exponents.

Example. $x^n + y^n - z^n$ for *n* odd and $x^n + y^n + z^n$ for *n* even, we use $t = x + y - z$. For $x^n - y^n + z^n$ with *n* odd we use $t = x - y + z$. For $x^n + y^n - z^n$ for *n* even then we use a complex definition, $t = x + y - iz$.

Lemma 1 Another way of writing *t* is that, if we have three variables *x,y,z* then there exists a '*t*' $\epsilon\ \Re$ that has the only other plus/minus combinations as *x,y,z*.

Let, $x + y = C,\ z - y = A,\ z - x = B.$ Furthermore let, $t = x + y - z \therefore z = C \pm t, x = A \mp t \quad y = B \mp t$

When $z = C - t$ then $z < C, z < x + y,\ z - y < x \therefore x = A + t.$ When $z = C + t$ then $z > C,\ z - y > x \ \therefore x = A - t$

likewise when $z = C - t,$ then $z > C, z - x < y \ \therefore y = B + t.$ When $z = C + t,$ then $y = B - t,$ therefore,

$$\pm 2z = \pm A \pm B \pm C \tag{1.01}$$

$$\pm 2x = \pm A \mp B \pm C \tag{1.02}$$

$$\pm 2y = \mp A \pm B \pm C \tag{1.03}$$

Moreover, $\mp t = \pm z \mp y \mp x = \pm C \mp t \mp B \mp t \mp A \mp t,$ therefore,

$$\pm 2t = \mp A \mp B \pm C \tag{1.04}$$

Therefore, *t* has the only other plus/minus combinations as *x*, *y*, *z* and can be written as (1.04)

We define the symmetric ***r*** in general as,

$$_V\boldsymbol{r} = \boldsymbol{x^2 + yz - xt + Vt^2 = y^2 + xz - yt + Vt^2 = z^2 - xy + zt + Vt^2} \tag{1.05}$$

We can also write this as,

$$_V\boldsymbol{r} = \boldsymbol{xz + yz - xy + Vt^2} \tag{1.06}$$

When we transform to the *t, r, xyz* space we use *V*= -1 and we call this the convoluted Fibonacci abstract space which is simply an exponent vs. coefficient function space. The abstract function spaces are taken over the exponents *n* and each are given by linear recurrence relations. Other *V*'s give other abstract spaces with different properties.

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

The symmetric parts are defined as,

$$ {}_{x/t}\boldsymbol{r} = \boldsymbol{x^2 + yz},\quad {}_{y/t}\boldsymbol{r} = \boldsymbol{y^2 + xz},\quad {}_{-z/t}\boldsymbol{r} = \boldsymbol{z^2 - xy},\quad {}_{0}\boldsymbol{r} = \boldsymbol{xz + yz - xy} \tag{1.07} $$

$$ {}_{\forall}\boldsymbol{r} = \text{any of } {}_{x/t}\boldsymbol{r},\ {}_{y/t}\boldsymbol{r},\ {}_{-z/t}\boldsymbol{r} \tag{1.08} $$

Proposition 1: *We can write* $x^n + y^n \pm z^n$ *in terms of* $(xyz)^m$ *and* $({}_{\forall}r)^{\frac{n-3m}{2}}$ *modulo t (or t independent, t = 0).*

We derive the *t* independent equation (*t* = 0) by factoring A^2+BC or B^2+AC or C^2-AB with,

$$ x^n + y^n - z^n = (A+t)^n + (B+t)^n - (C-t)^n $$
$$ \equiv (-C^n + A^n + B^n) \bmod t $$
$$ \equiv (-C^n + A^n + (C-A)^n) \bmod t $$
$$ \equiv -nCA(C-A)((C-A)^{n-3} + \frac{(n-3)}{2!}CA(C-A)^{n-5} + \frac{(n-4)(n-5)}{3!}C^2A^2(C-A)^{n-7} \ldots $$
$$ \frac{(n-N)(n-(N+1))(n-(N+2))\ldots 4}{(N-1)!}C^{\frac{n-5}{2}}A^{\frac{n-5}{2}}(C-A)^2 + \frac{(n-(N+1))(n-(N+2))\ldots 2}{N!}C^{\frac{n-3}{2}}A^{\frac{n-3}{2}}) \bmod t \tag{1.09} $$

Where *N* is the number of terms, *n* is odd.

We are using B^2+AC in this derivation. We get when *n*=odd, [1]

$$ x^n + y^n - z^n \equiv -nABC((B^2+AC)^{\frac{(n-3)}{2}} + \frac{(\frac{n-5}{2})(\frac{n-7}{2})}{3!}(ABC)^2(B^2+AC)^{\frac{(n-9)}{2}} $$
$$ + \frac{(\frac{n-7}{2})(\frac{n-9}{2})(\frac{n-11}{2})(\frac{n-13}{2})}{5!}(ABC)^4(B^2+AC)^{\frac{n-15}{2}} + $$
$$ \frac{(\frac{n-9}{2})(\frac{n-11}{2})(\frac{n-13}{2})(\frac{n-15}{2})(\frac{n-17}{2})(\frac{n-19}{2})}{7!}(ABC)^6(B^2+AC)^{\frac{n-21}{2}} + \ldots $$
$$ + \frac{(\frac{(n-(m+2))}{2})(\frac{(n-(m+4))}{2})\ldots(\frac{(n-(3m-2))}{2})}{m!}(ABC)^{m-1}(B^2+AC)^{\frac{n-3m}{2}}) \bmod t \tag{1.10} $$

***t*-independent (*t* = 0) equation *n* = odd >1**

(With $(B^2+AC) \equiv {}_{x/t}r \bmod t \equiv {}_{y/t}r \bmod t \equiv {}_{-z/t}r \bmod t \equiv {}_{\forall}r \bmod t$ **)**

$$ x^n + y^n - z^n \equiv \sum_{\substack{m=1(odd) \\ m=n/3 \\ m=(n-2)/3 \\ m=(n-4)/3}} -n\frac{(\frac{(n-(m+2))}{2})!}{m!\,\frac{n-3m}{2}!}(xyz)^m({}_{\forall}r)^{\frac{n-3m}{2}} \bmod t \tag{1.11} $$

***t*-independent (*t* = 0) equation *n* = even >1**

$$ x^n + y^n + z^n \equiv (2(B^2+AC)^{\frac{n}{2}} + \frac{n(\frac{n-4}{2})}{2!}(ABC)^2(B^2+AC)^{\frac{n-6}{2}} + \frac{n(\frac{n-6}{2})(\frac{n-8}{2})(\frac{n-10}{2})}{4!}(ABC)^4(B^2+AC)^{\frac{n-12}{2}} + $$
$$ \frac{n(\frac{n-8}{2})(\frac{n-10}{2})(\frac{n-12}{2})(\frac{n-14}{2})(\frac{n-16}{2})}{6!}(ABC)^6(B^2+AC)^{\frac{n-18}{2}} + \ldots $$
$$ \frac{n(\frac{n-(m+2)}{2})(\frac{(n-(m+4))}{2})\ldots(\frac{n-(3m-2)}{2})}{m!}(ABC)^m(B^2+AC)^{\frac{n-3m}{2}}) \bmod t \tag{1.12} $$

$$x^n + y^n + z^n \equiv \sum_{\substack{m=0(even)\\ m=(n-4)/3\\ m=(n-2)/3\\ m=n/3}} n\frac{(\frac{n-(m+2)}{2})!}{0!m!(\frac{n-3m}{2})!}(xyz)^m({}_{\forall}r)^{\frac{n-3m}{2}} \quad modt \tag{1.13}$$

We can write both *n* odd and *n* even as,

$$x^n + y^n \pm z^n \equiv \sum_{\substack{m=0(n,m\ even)\\ m=1(n,m\ odd)\\ m=(n-4)/3\\ m=(n-2)/3\\ m=n/3}} (-1)^n n\frac{(\frac{n-(m+2)}{2})!}{0!m!(\frac{n-3m}{2})!}(xyz)^m({}_{\forall}r)^{\frac{n-3m}{2}} modt \tag{1.14}$$

Proposition 2 *We can write* $x^n + y^n \pm z^n$ *in terms of* $(xyz)^m$, ${}_{-1}r^{\omega}$ *and* t^{ℓ} *(or t dependent).*

What's remarkable is that we can do this for each power of *t* by 'factoring' the symmetric into the equation (*r* is factored into parts of the expanded equation) which separates t^{ℓ} and $(xyz)^m$ to get a t^{ℓ} dependent representation or transformation. The rigorous proof is available in Extract 2 if one wishes to see this.
In general, we get for *n* and ℓ,

$n = odd\ \ell = even$

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

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

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

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

$$\frac{n(\frac{n-(m+2\#)}{2})(\frac{(n-(m+4\#)}{2})\ldots(\frac{(n-(\ell+3m-2)}{2})}{1!m!\frac{(\ell\#)}{2}!})t^{\ell}(xyz)^m\,{}_{-1}r^{\frac{n-\ell-3m}{2}} \tag{1.15}$$

$n = odd\ \ell = odd$

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

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

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

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

$$\frac{n(\frac{n-(m+1^*)}{2})(\frac{(n-(m+3^*)}{2})\ldots(\frac{(n-(\ell+3m-2)}{2})}{1!m!\frac{(\ell^*-1)}{2}!})t^{\ell}(xyz)^m\,{}_{-1}r^{\frac{n-\ell-3m}{2}} \tag{1.16}$$

This gives,

$$t^{\ell} \text{ terms for } x^n + y^n \pm z^n = \pm \sum_{s=0}^{s=\ell/2} \sum_{\substack{m=1\,odd(n\,even,\ell\,odd,\#) \\ m=0\,even(n\,odd,\ell\,odd,*)}}^{\substack{m=(n-\ell-4)/3 \\ m=(n-\ell-2)/3 \\ m=(n-\ell)/3}} n\left(\frac{\left(\frac{n+(\ell-2s-m-2)}{2}\right)!}{(\ell-2s)!\,m!\,s!\left(\frac{n-3m-\ell}{2}\right)!}\right) t^{\ell}(xyz)^m \,{}_{-1}r^{\frac{n-3m-\ell}{2}} \qquad (1.17)$$

Therefore we can write,

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

$$x^n + y^n \pm z^n = \sum_{\ell=0}^{n} \sum_{s=0}^{s=\ell/2} \sum_{\substack{m=1\,odd(\#) \\ m=0\,even(*)}}^{\substack{m=(n-\ell-4)/3 \\ s=(\ell-1)/2\; m=(n-\ell-2)/3 \\ m=(n-\ell)/3}} (-1)^n (1)^s (-1)^{\ell} n\left(\frac{\left(\frac{n+(\ell-2s-m-2)}{2}\right)!}{(\ell-2s)!\,m!\,s!\left(\frac{n-3m-\ell}{2}\right)!}\right) t^{\ell}(xyz)^m \,{}_{-1}r^{\frac{n-3m-\ell}{2}} \qquad (1.18)$$

$*n = odd, \ell = odd, n = even, \ell = even$

$\# n = odd, \ell = even, n = even, \ell = odd$

Where ${}_{-1}r$ is the V= -1 symmetric $x^2+yz-xt-t^2$

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

$$x^n + y^n \pm z^n = \sum_{\ell=0}^{n} \sum_{s=0}^{s=\ell/2} \sum_{\substack{m=1\,odd(\#) \\ m=0\,even(*)}}^{\substack{m=(n-\ell-4)/3 \\ s=(\ell-1)/2\; m=(n-\ell-2)/3 \\ m=(n-\ell)/3}} (-1)^n (1)^s (-1)^{\ell} n\left(\frac{(\omega+\ell-s+m-1)!}{(\ell-2s)!\,m!\,s!(\omega)!}\right) t^{\ell}(xyz)^m \,{}_{-1}r^{\omega} \qquad (1.19)$$

$*n = odd, \ell = odd, n = even, \ell = even$

$\# n = odd, \ell = even, n = even, \ell = odd$

Proposition 3 *We can write the negative n equation or $xz^n+yz^n\pm xy^n$ in terms of $(xyz)^m$ and $({}_{\forall}r)^{n-3m}$ modulo t. (t independent or t=0)*

$$(xyz)^n(x^{-n}+y^{-n}\pm z^{-n}) = (zy)^n + (zx)^n \pm (xy)^n = (-x^2 + {}_{-1}r)^n + (-y^2 + {}_{-1}r)^n \pm (z^2 - {}_{-1}r)^n$$

$$= 3\,{}_{-1}r^n \pm (x^{2n}+y^{2n}+z^{2n}) \mp \frac{n!}{1!(n-1)!}\,{}_{-1}r(x^{2n-2}+y^{2n-2}+z^{2n-2}) \pm \frac{n!}{2!(n-2)!}\,{}_{-1}r^2(x^{2n-4}+y^{2n-4}+z^{2n-4})\ldots$$

$$\pm \frac{n!}{(n-1)!1!}\,{}_{-1}r^{n-1}(x^2+y^2+z^2)$$

$$= 3\,{}_{-1}r^n \pm (2r^n + \frac{2n(n-2)}{2!}(xyz)^2({}_{-1}r)^{n-3} + \frac{2n(n-3)(n-4)(n-5)}{4!}(xyz)^4({}_{-1}r)^{n-6} +$$

$$\frac{2n(n-4)(n-5)(n-6)(n-7)(n-8)}{6!}(xyz)^6({}_{-1}r)^{n-9} + \ldots((2.72)\to 2n))$$

$$\mp \frac{n!}{1!(n-1)!}\,{}_{-1}r(2r^{n-1} + \frac{(2n-2)(n-3)}{2!}(xyz)^2({}_{-1}r)^{n-4} + \frac{(2n-2)(n-4)(n-5)(n-6)}{4!}(xyz)^4({}_{-1}r)^{n-7} +$$

$$\frac{(2n-2)(n-5)(n-6)(n-7)(n-8)(n-9)}{6!}(xyz)^6({}_{-1}r)^{n-10} + \ldots((2.72)\to 2n-2))$$

$$\pm \frac{n!}{2!(n-2)!}\,{}_{-1}r^2(2r^{n-2} + \frac{(2n-4)(n-4)}{2!}(xyz)^2({}_{-1}r)^{n-5} + \frac{(2n-4)(n-5)(n-6)(n-7)}{4!}(xyz)^4({}_{-1}r)^{n-9} +$$

$$\frac{(2n-4)(n-6)(n-7)(n-8)(n-9)(n-10)}{6!}(xyz)^6({}_{-1}r)^{n-11} + \ldots((2.72)\to 2n-4)).. \pm \frac{n!}{(n-1)!1!}\,{}_{-1}r^{n-1}$$

Hence we have,

$$x^{-n}+y^{-n}\pm z^{-n}\equiv({}_{-1}r^{n}(xyz)^{-n}-n\,{}_{-1}r^{n-3}(xyz)^{-n+2}+\frac{n(n-5)}{0!\,2!}\,{}_{-1}r^{n-6}(xyz)^{-n+4}-\frac{n(n-7)(n-8)}{0!\,3!}\,{}_{-1}r^{n-9}(xyz)^{-n+6}$$
$$+\frac{n(n-9)(n-10)(n-11)}{0!\,4!}\,{}_{-1}r^{n-12}(xyz)^{-n+8}\ldots\frac{n(n-(2m+1))(n-(2m+2))\ldots(n.-(3m-1))}{m!}\,{}_{-1}r^{n-3m}(xyz)^{-n+2m})\bmod t$$

The *t* independent (*t* = 0), *n* < 1

$$(xyz)^{n}(x^{-n}+y^{-n}\pm z^{-n})$$
$$=(xz)^{n}+(yz)^{n}\pm(xy)^{n}\equiv\sum_{m=0}^{m=n/3\;\;m=(n-1)/3\;\;m=(n-2)/3}(-1)^{m}n\frac{(n-(2m+1))!}{0!\,m!(n-3m)!}\,{}_{\forall}r^{(n-3m)}(xyz)^{2m}\bmod t$$

Proposition 4 *We can write the negative n equation or* $(xz)^{n}+(yz)^{n}\pm(xy)^{n}$ *in terms of* $(xyz)^{2m}$, ${}_{-1}r^{\omega}$ *and* t^{ℓ}.

This is written in 2 forms when ℓ is even and odd respectively. Hence, both forms are required to generate the *t* dependent equation for negative *n*.

Theorem 1.2 *t* dependent equation *V* = -1, (*n* < 0).

ℓ *even*

$$(xyz)^{n}(x^{-n}+y^{-n}\pm z^{-n})=(xz)^{n}+(yz)^{n}\pm(xy)^{n}$$
$$=\sum_{\ell=0(\ell\,even)}^{2n}\;\sum_{s=0(s\,even)}^{s=\ell}\;\sum_{m=0}^{m=(n-\frac{(\ell+4)}{2})/3\;\;m=(n-\frac{(\ell+2)}{2})/3\;\;m=(n-\frac{(\ell)}{2})/3}(-1)^{m}(-1)^{\frac{s}{2}}n\frac{(n-(2m+1)!}{s!(\frac{\ell-s}{2})!(m-\frac{s}{2})!(n-3m-\frac{\ell}{2})!}t^{\ell}(xyz)^{2m}\,{}_{-1}r^{n-3m-\frac{\ell}{2}}\quad(1.20)$$

Note: if we are using the $s=\ell$ summation then make $\frac{(n-(2m+1)!}{(m-s/2)!}=0$ when $s/2>m$ as we can't have negative factorials. We could also use $s=2m$ summation that does the same thing.

ℓ *odd*

$$(xyz)^{n}(x^{-n}+y^{-n}\pm z^{-n})=(xz)^{n}+(yz)^{n}\pm(xy)^{n}$$
$$=\sum_{\ell=1(odd)}^{2n}\;\sum_{s=1odd}^{or\;s=\ell}\;\sum_{m=0}^{m=(n-\frac{(\ell+7)}{2})/3\;\;m=(n-\frac{(\ell+5)}{2})/3\;\;m=(n-\frac{(\ell+3)}{2})/3}(-1)^{m}(-1)^{\frac{s-1}{2}}n\frac{(n-(2m+2))!}{s!(\frac{\ell-s}{2})!(m-\frac{s-1}{2})!(n-3m-\frac{(\ell+3)}{2})!}t^{\ell}(xyz)^{2m+1}\,{}_{-1}r^{n-3m-\frac{\ell+3}{2}}\quad(1.21)$$

Note: if using $s=\ell$ summation then make $\frac{(n-(2m+2))!}{(m-s/2)!}=0$ when $s/2>m$.

Otherwise we can use $s=2m+1$ summation.

Result. Hence by making $\omega=\frac{n-3m-\ell}{2}$ or $n-3m-\frac{\ell}{2}$ or $n-3m-\frac{\ell-3}{2}$ we can conclude we can write all these equations in terms $(xyz)^{m^{*}}$, ${}_{-1}r^{\omega}$ and t^{ℓ}

First Examples V = -1, $_{-1}r \to r$

...

$$x^{-6}+y^{-6}+z^{-6}=(t^{12}+6t^{10}r+6xyzt^{9}+15t^{8}r^{2}+24xyzt^{7}r+20t^{6}r^{3}+3(xyz)^{2}t^{6}+36xyzt^{5}r^{2}+15r^{4}t^{4}+0(xyz)^{2}t^{4}r+24xyzt^{3}r^{3}$$
$$-10(xyz)^{3}t^{3}+6t^{2}r^{5}-9t^{2}(xyz)^{2}r^{2}+6txyzr^{4}-12t(xyz)^{3}r+r^{6}-6(xyz)^{2}r^{3}+3(xyz)^{4})(xyz)^{-6}$$

$$x^{-5}+y^{-5}-z^{-5}=(t^{10}+5t^{8}r+5xyzt^{7}+10t^{6}r^{2}+15xyzt^{5}r+10t^{4}r^{3}+0(xyz)^{2}t^{4}+15xyzt^{3}r^{2}+5r^{4}t^{2}-5(xyz)^{2}t^{2}r+5xyztr^{3}$$
$$-5(xyz)^{3}t+r^{5}-5(xyz)^{2}r^{2})(xyz)^{-5}$$

$$x^{-4}+y^{-4}+z^{-4}=(t^{8}+4t^{6}r+4xyzt^{5}+6r^{2}t^{4}+8xyzrt^{3}+4r^{3}t^{2}-2(xyz)^{2}t^{2}+4xyztr^{2}+r^{4}-4(xyz)^{2}r)(xyz)^{-4}$$

$$x^{-3}+y^{-3}-z^{-3}=(t^{6}+3t^{4}r+3xyzt^{3}+3t^{2}r^{2}+3xyztr+r^{3}-3(xyz)^{2})(xyz)^{-3}$$

$$x^{-2}+y^{-2}+z^{-2}=(t^{4}+2t^{2}r+2xyzt+r^{2})(xyz)^{-2}$$

$$x^{-1}+y^{-1}-z^{-1}=(t^{2}+r)(xyz)^{-1}$$

$$x^{0}+y^{0}+z^{0}=3$$

$$x^{1}+y^{1}-z^{1}=t$$

$$x^{2}+y^{2}+z^{2}=3t^{2}+2r$$

$$x^{3}+y^{3}-z^{3}=4t^{3}+3tr-3xyz$$

$$x^{4}+y^{4}+z^{4}=7t^{4}+8t^{2}r-4xyzt+2r^{2}$$

$$x^{5}+y^{5}-z^{5}=11t^{5}+15t^{3}r-10xyzt^{2}+5r^{2}t-5xyzr$$

$$x^{6}+y^{6}+z^{6}=18t^{6}+30t^{4}r-18xyzt^{3}+15r^{2}t^{2}-12xyztr+2r^{3}+3(xyz)^{2}$$

$$x^{7}+y^{7}-z^{7}=29t^{7}+56t^{5}r-35xyzt^{4}+35r^{2}t^{3}-35xyzt^{2}r+7tr^{3}+7(xyz)^{2}t-7r^{2}xyz$$

$$x^{8}+y^{8}+z^{8}=47t^{8}+104t^{6}r-64xyzt^{5}+80r^{2}t^{4}-80xyzt^{3}r+24t^{2}r^{3}+20(xyz)^{2}t^{2}-24xyztr^{2}+2r^{4}+8(xyz)^{2}r$$

$$x^{9}+y^{9}-z^{9}=76t^{9}+189t^{7}r-117xyzt^{6}+171r^{2}t^{5}-180xyzt^{4}r+66t^{3}r^{3}+45(xyz)^{2}t^{3}-81xyzt^{2}r^{2}+9tr^{4}+27(xyz)^{2}rt-9xyzr^{3}-3(xyz)^{3}$$

$$x^{10}+y^{10}+z^{10}=123t^{10}+340t^{8}r-210xyzt^{7}+355r^{2}t^{6}-380xyzt^{5}r+170t^{4}r^{3}+100(xyz)^{2}t^{4}-220xyzt^{3}r^{2}+35t^{2}r^{4}+90(xyz)^{2}rt^{2}-40xyztr^{3}$$
$$-10(xyz)^{3}t+2r^{5}+15r^{2}(xyz)^{2}$$

$$x^{11}+y^{11}-z^{11}=199t^{11}+605t^{9}r-374xyzt^{8}+715r^{2}t^{7}-781xyzt^{6}r+407t^{5}r^{3}+209(xyz)^{2}t^{5}-561xyzt^{4}r^{2}+110t^{3}r^{4}+242(xyz)^{2}rt^{3}$$
$$-154xyzt^{2}r^{3}-33(xyz)^{3}t^{2}+11r^{5}t+66r^{2}(xyz)^{2}t-11xyzr^{4}-11(xyz)^{3}r$$

....

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 are as follows:

Corollary16

$$x^{n}+y^{n}\pm z^{n}=(x^{n-1}+y^{n-1}\mp z^{n-1})t+(x^{-1}+y^{-1}-z^{-1})(x^{n-2}+y^{n-2}\pm z^{n-2})xyz-(x^{n-3}+y^{n-3}\mp z^{n-3})xyz \quad (1.22)$$

Corollary17

$$x^{-n}+y^{-n}\mp z^{-n}=(x^{-(n-2)}+y^{-(n-2)}\mp z^{-(n-2)})(xyz)^{-1}t+(x^{-1}+y^{-1}-z^{-1})(x^{-(n-1)}+y^{-(n-1)}\pm z^{-(n-1)})$$
$$-(x^{-(n-3)}+y^{-(n-3)}+z^{-(n-3)})(xyz)^{-1} \quad (1.23)$$

Corollary18

The sum of the exponents in each term add to n ($n > 0$) and $2n$ ($n < 0$) so with exponent factor $(xyz) = 3$, $r = 2$ and $t = 1$ we therefore have for $n = M3$, lone $(xyz)^{n/3}$ terms. 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 $n > 0$ and vice versa in $n < 0$.

(1.24)

Corollary 20 First term coefficient for $n= p$ (prime) is 1$modp$, all the rest are 0$modp$. Column 1 is a Lucas sequence and L_n is congruent to 1$modn$ if n is prime. [2] (1.25)

Corollary 24.

One can see the positive columns are binomial variations of the convolved Fibonacci sequence and column 1 is Lucas. Write;

$F_n^{(0)} = F_n = 1,1,2,3,5,8,13,21....$

$F_n^{(1)} = 1,2,5,10,20,38,71,130...$

$F_n^{(2)} = 1,3,9,22,51,111,233,474...$

$F_n^{(3)} = 1,4,14,40,105,256,594,1324...$

etc. such that,

$F_n^{(k)} = F_n^{(k-1)} + F_{n-1}^{(k)} + F_{n-2}^{(k)}$

hence we get, $F_n^{(k)} = F_1^{(k-1)} F_n^{(0)} + F_2^{(k-1)} F_{n-1}^{(0)} + F_3^{(k-1)} F_{n-2}^{(0)} ... F_m^{(k-1)} F_{n-(m-1)}^{(0)} .... F_n^{(k-1)} F_1^{(0)} = \sum_{m=1}^{n} F_m F_{n-m}^{(k-1)}$

and $F_n^{(k)} = \sum_{m=1}^{m=n} \sum_{d=1}^{d=m} \sum_{e=1}^{e=d} ...... \sum_{w=1}^{w=v} F_{n-(m-1)} F_{m-(d-1)} F_{d-(e-1)} .....F_{v-(w-1)} F_w$

Where the number of summations $= k - 1$

We can also see binomial coefficients as follows;

$[1] = L_n t^n$

$[2] = n F_{n-1}^{(0)} t^{n-2} \; {}_{-1}r$

$[3] = -n F_{n-2}^{(0)} t^{n-3} xyz$

$[4] = \frac{n}{2} F_{n-3}^{(1)} t^{n-4} \; {}_{-1}r^2$

$[5] = -n F_{n-4}^{(1)} t^{n-5} xyz \; {}_{-1}r$

$[7] = \frac{n}{2} F_{n-5}^{(1)} t^{n-6} (xyz)^2$

$[6] = \frac{n}{3} F_{n-5}^{(2)} t^{n-6} \; {}_{-1}r^3$

$[8] = -n F_{n-6}^{(2)} t^{n-7} xyz \; {}_{-1}r^2$

$[9] = \frac{n}{4} F_{n-7}^{(3)} t^{n-8} \; {}_{-1}r^4$

$[10] = n F_{n-7}^{(2)} t^{n-8} (xyz)^2 \; {}_{-1}r$

$[11] = -n F_{n-8}^{(3)} t^{n-9} xyz \; {}_{-1}r^3$

$[12] = -\frac{n}{3} F_{n-8}^{(2)} t^{n-9} (xyz)^3$

$[14] = \frac{6n}{4} F_{n-9}^{(3)} t^{n-10} (xyz)^2 \; {}_{-1}r^2$

$[15] = n F_{n-10}^{(3)} t^{n-11} (xyz)^3 \; {}_{-1}r$

$[18] = \frac{n}{4} F_{n-11}^{(3)} t^{n-12} (xyz)^4$

Hence, each column group is given by, $\pm \sum_{h=0}^{k} \frac{k!}{h!(k-h)!} \frac{n}{k} F_{n-2k-h+1}^{(k)} t^{n-2k-h} (xyz)^h \; {}_{-1}r^{k-h}$

$$x^n + y^n \pm z^n = L_n t^n \pm \sum_{k=1}^{\substack{n/2 \\ (n-1)/2}} \sum_{h=0}^{k} \frac{k!}{h!(k-h)!} \frac{n}{k} F_{n-2k-h+1}^{(k)} t^{n-2k-h} (xyz)^h \; {}_{-1}r^{k-h} \qquad (1.26)$$

Therefore we have,

$$\sum_{\ell=0}^{n} \sum_{s=0}^{\substack{s=(\ell-1)/2 \\ s=\ell/2}} \sum_{\substack{m=1\ odd(\#) \\ m=0\ even(*)}}^{\substack{(n-\ell-4)/3 \\ (n-\ell-2)/3 \\ (n-\ell)/3}} (-1)^n (-1)^\ell n \left(\frac{(\omega+\ell-s-m-1)!}{(\ell-2s)!\,m!\,s!(\omega)!}\right) t^\ell (xyz)^m \; {}_{-1}r^\omega = L_n t^n \pm \sum_{k=1}^{\substack{n/2 \\ (n-1)/2}} \sum_{h=0}^{k} \frac{k!}{h!(k-h)!} \frac{n}{k} F_{n-2k-h+1}^{(k)} t^{n-2k-h} (xyz)^h \; {}_{-1}r^{k-h}$$

(1.27)

Hence, one can also view this as a transformation to the convoluted Fibonacci space in as much as it is easier to find high *t* exponent, low *r*, (*xyz*) coefficients using the convoluted Fibonacci sequence.

Corollary 29 The *T, R,* (*XYZ*) equation.
We can apply the *t, r,* (*xyz*) representation or transformation to any three variable equation if we make *T* equal the equation in question.

T dependent equation,

$$X^n+Y^n\pm Z^n=\sum_{\ell=0}^{n}\ \sum_{s=0}^{s=\ell/2}\ \sum_{\substack{m=1\ odd(\#)\\ m=0\ even(*)}}^{\substack{m=(n-\ell-4)/3\\ s=(\ell-1)/2\ m=(n-\ell-2)/3\\ m=(n-\ell)/3}} (-1)^n(-1)^{\ell}n\left(\frac{\left(\frac{n+(\ell-2s-m-2)}{2}\right)!}{(\ell-2s)!\,m!\,s!\left(\frac{n-3m-\ell}{2}\right)!}\right)T^{\ell}(XYZ)^m\ {}_{-1}R^{\frac{n-3m-\ell}{2}} \quad (1.28)$$

$*n=odd,\ell=odd,n=even,\ell=even$

$\#\ n=odd,\ell=even,n=even\ \ell=odd$

Where X,Y,Z represents the terms in the equation and ${}_{-1}R=X^2+YZ-XT-T^2=Y^2+XZ-YT-T^2=Z^2-XY+ZT-T^2$

For example if

$x+3y-z^2=C\quad(C\ \text{constant})$

Make $T=C$

${}_{-1}R=x^2+3yz^2-xT-T^2$

$=(3y)^2+xz^2-3yT-T^2$

$=z^4-3xy+z^2T-T^2$

Choose $n=3$

$x^3+(3y)^3-(z^2)^3=4T^3+3T\ {}_{-1}R-3(x)(3y)(z^2)$

$X=x,Y=3y,Z=z^2$

T independent equation $T=0$,

$$X^n+Y^n\pm Z^n=\sum_{\substack{m=0(n,m\ even)\\ m=1(n,m\ odd)}}^{\substack{m=n/3\\ m=(n-2)/3\\ m=(n-4)/3}} (-1)^n n\frac{\left(\frac{n-(m+2)}{2}\right)!}{0!\,m!\left(\frac{n-3m}{2}\right)!}(XYZ)^m({}_{-1}R)^{\frac{n-3m}{2}} \quad (1.29)$$

Where ${}_{X/T}R=x^2+3yz^2$, ${}_{Y/T}R=(3y)^2+xz^2$, ${}_{-Z/T}R=z^4-3xy$

Partial Congruence and the primitive root multiplier

If $x,y,z \neq 0 \, mod \, q$ where q is a prime decomposition factor of ${}_0r = xz + yz - xy$ or the symmetric parts ${}_{x/t}r = x^2 + yz$ or ${}_{y/t}r = y^2 + xz$ or ${}_{-z/t}r = z^2 - xy$. We define a partial congruence $mod \, {}_0r$ or $mod \, {}_\forall r$ as,

$$\begin{aligned} \boldsymbol{xz} &\equiv \boldsymbol{x' mod q} \\ \boldsymbol{yz} &\equiv \boldsymbol{y' mod q} \\ \boldsymbol{xy} &\equiv \boldsymbol{z' mod q} \end{aligned} \tag{4.01}$$

Where $x' + y' - z' = t'$ and x', y', z' are congruence residues. If $xz \equiv 0 \, mod \, q$, then xz is a multiple of q but q is a prime decomposition factor of $x^2 + yz, y^2 + xz, z^2 - xy$ or $xz + yz - xy$ which would mean x, y, z must share the common factor q if $x, y, z > 0$. Similarly if $yz \equiv 0 \, mod \, q$ and $xy \equiv 0 \, mod \, q$.

One can see that $x' + y' - z' = t' \equiv 0 \, mod \, q$ and if $t = 0$ then $x' + y' - z' = t' \equiv 0 \, mod \, {}_\forall r$ because $xz + yz - xy = x^2 + yz = y^2 + xz = z^2 - xy$ in that case $t = 0$.

Moreover, if we had an equation such as $x^n + y^n - z^n = 0$ where n is odd and we write the partial congruence as,

$$\begin{aligned} \boldsymbol{(xz)^n} &\equiv \boldsymbol{x' mod q} \\ \boldsymbol{(yz)^n} &\equiv \boldsymbol{y' mod q} \\ \boldsymbol{(xy)^n} &\equiv \boldsymbol{z' mod q} \end{aligned} \tag{4.02}$$

One can see $x' + y' - z' = t' \equiv 0 \, mod \, {}_\forall r$ because $(xz)^n + (yz)^n - (xy)^n = x^{2n} + y^n z^n = y^{2n} + (xz)^n = z^{2n} - (xy)^n$ of which $x^2 + yz$, $y^2 + xz$, $z^2 - xy$ are factors respectively if n is odd.

We can multiply the residues to get $x'z' + y'z' - x'y' \equiv xyzt \, mod \, q$ or in the second example partial congruence (4.02) $x'z' + y'z' - x'y' \equiv 0 \, mod \, q$ or we could just square x' and add $y'z'$ to get $xz(xz + y^2)$ so, $x'^2 + y'z' \equiv 0 \, mod \, q$ for q of ${}_{y/t}r$.

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 $0 < m < q$ so we write,

$$\begin{aligned} \boldsymbol{g^m xz} &\equiv \boldsymbol{x' mod q} \\ \boldsymbol{g^m yz} &\equiv \boldsymbol{y' mod q} \\ \boldsymbol{g^m xy} &\equiv \boldsymbol{z' mod q} \end{aligned} \tag{4.03}$$

and in this form g^m just generates the set of residues but we will refer to m as phase number.

The double partial congruence is defined as,

$$\begin{aligned} \boldsymbol{g^m xz} &\equiv \boldsymbol{x' mod q} & \qquad \boldsymbol{g^{n_1} x'z'} &\equiv \boldsymbol{y' mod q} \\ \boldsymbol{g^m yz} &\equiv \boldsymbol{y' mod q} & \qquad \boldsymbol{g^{n_2} y'z'} &\equiv \boldsymbol{x' mod q} \\ \boldsymbol{g^m xy} &\equiv \boldsymbol{z' mod q} & \qquad \boldsymbol{g^{n_3} x'y'} &\equiv \boldsymbol{z' mod q} \end{aligned} \tag{4.04}$$

where n_1, n_2, n_3 are such that we get back our y', x', z' residues respectively.

n_1, n_2, n_3 are not arbitary for $t = 0$ or equations that are equivalent to 0 *mod ulo* q.

We have $y'^2 + x'z' \equiv 0 \, mod \, q$ so, $x'z'(g^{2n_1} x'z' + g^{n_2 + n_3} y'^2) \equiv 0 \, mod \, q$ but $y'^2 \equiv -x'z' \, mod \, q$ hence $g^{2n_1 - n_2 - n_3} \equiv 1 \, mod \, q$. Likewise $g^{2n_2 - n_1 - n_3} \equiv 1 \, mod \, q$, $g^{2n_3 - n_1 - n_2} \equiv 1 \, mod \, q$ and with $n_1, n_2, n_3 < q$ we get two possible solutions:

1) $n_1 = n_2 = n_3 \rightarrow n$ (Note, n is not the other exponent n - but for lack of symbols)

2) $3n_1 = 3n_2 = 3n_3 \equiv 0 \, mod \, q$ where n_1, n_2, n_3 take the 3 values $\boldsymbol{\frac{1}{3}(q-1)}$, $\boldsymbol{\frac{2}{3}(q-1)}$, $\boldsymbol{(q-1)}$.

Remark: $q - 1 \equiv 0 \, mod \, q$ so we can write our 3 values as $0, \frac{1}{3}(q-1), \frac{2}{3}(q-1)$

We can refer to the $n's$ as partition numbers.

Computer Verifications - Take any equation that equals 0 that doesn't have common factors (though one could factor out the common factors) and solve for n_1, n_2, n_3.

Example 1 $5+7=12$ $(t=0)$ and ${}_{x/t}r=109$ which is prime with a primitive root of 6 we find that $n_1=64, n_2=28$ and $n_3=100$ these are shifted $0,1/3,2/3$ partitions of $q-1$ so if we made $m=28$ then we get our $0,1/3,2/3$ partitions.

Example 2 $x+y^3-z^5=0$ and $x=118, y=5$ and $z=3$, ${}_{X/T}R=x^2+y^3z^5=(31)(1429)$ So our first q is 31 and we don't need a g^m since we find $n_1=0$, $n_2=20$, $n_3=10$ with $g=3$. Our second q is 1429 and what we find with $g=6$ is $n_1=24$, $n_2=500, n_3=976$ these are shifted $0,1/3,2/3$ exponents, shifted by 24 but to get $n_1=0, n_2=476, n_3=952$ we need to multiply our first partial congruences by $g^{24}, m=24$. The reason why $q=31$ has $m=0$ is because $q=Mabc+1$ where a,b,c are the exponents.

Applications

Theorem 5 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 $n = p$ (prime).

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

i.e. $(M3)^p + (M3 \pm 1)^p - (M3 \pm 1)^p = 0$

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

If $x,y,z \neq M3$ then only $(M3 \pm 1)^p + (M3 \pm 1)^p - (M3 \mp 1)^p = 0$ is allowed hence $t = M3 \pm 1 + M3 \pm 1 - M3 \mp 1 = M3$

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

$x,y,z > 0$ 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 ${}_{x/t}r = x^2 + yz$ $\therefore {}_{x/t}r > 0$ and ${}_{x/t}r$ is odd as one of x,y,z is even and t is even. Furthermore, $x^2 + yz > t$ *i.e* $(z - y + t)^2 + yz > t$. We can also show this for ${}_{y/t}r$, ${}_{-z/t}r$.

Using ${}_{x/t}r = x^2 + yz$, lets make q a prime decomposition factor of ${}_{x/t}r$ which is odd > 3 (5.03)

If $q = 3$ then $t \equiv 0 \, mod \, q$ as above, otherwise write our first partial congruence,

$$g^m (xz)^p \equiv x' \, mod \, q$$
$$g^m (yz)^p \equiv y' \, mod \, q$$
$$g^m (xy)^p \equiv z' \, mod \, q \tag{5.04}$$

Where g is the primitive root of q or a multiplicative set generator. $x', y', z' \neq 0 \, mod \, q$ otherwise $x,y,z \equiv 0 \, mod \, q$ and we get common factors q. Hence, from the partial congruences we have $x'z' + y'z' - x'y' \equiv 0 \, mod \, q$ and $x'^2 + y'z' \equiv 0 \, mod \, q$ since we can factor ${}_{x/t}r$ from $(yz)^{2p} + (yz)^p x^{2p}$ *Hence* $x^{2p} + (yz)^p \equiv 0 \, mod \, q$ as shown previously. We need to define 4 cases when $q \neq 3$*:*

1a) $q \neq 3sp + 1$ (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 1a. Write $lp = uq - v$ and make $u - v = 1$. 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,R (T independent) representation (C.29) 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)

$RHS \equiv 0 \, mod \, q$. $(R = x^{2p} + y^p z^p = M \, {}_{x/t}r)$

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

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 $u - v = 3p$,

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

$l = vs + 3q$ 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 $u - v = 1$,

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

$lp = v3s + q$ 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 $q = 3sp + 1$, write a double partial congruence,

$$\begin{aligned} g^m(xz)^p &\equiv x' \bmod q & g^{n_1}(x'z') &\equiv y' \bmod q \\ g^m(yz)^p &\equiv y' \bmod q & g^{n_2}(y'z') &\equiv x' \bmod q \\ g^m(xy)^p &\equiv z' \bmod q & g^{n_3}(x'y') &\equiv z' \bmod q \end{aligned} \tag{5.18}$$

Where $g^{n's}$ is the primitive root multiplier such that we can get all residues $mod ulo\ q$ including x', y', z'.

Now we have $x' + y' - z' \equiv 0 \bmod q$ and multiplying entries gives us,

$$g^{2m}(xyz)^p(x^p + y^p - z^p) \equiv x'z' + y'z' - x'z' \bmod q \tag{5.19}$$

hence $x'z' + y'z' - x'z' \equiv 0 \bmod q$ also. This means $x'^2 + y'z' \equiv 0 \bmod q$, $y'^2 + x'z' \equiv 0 \bmod q$, $z'^2 - x'y' \equiv 0 \bmod q$ or we can show it directly as $(xz)^{2p} + (xz)^p y^{2p} \equiv 0 \bmod q$ etc. hence,

$$g^{2n_1}(x'z') + g^{n_2+n_3}(y')^2 \equiv 0 \bmod q \rightarrow g^{2n_1-n_2-n_3} = 1 \bmod q, \tag{5.20}$$

$$g^{2n_2}(y'z') + g^{n_1+n_3}(x')^2 \equiv 0 \bmod q \rightarrow g^{2n_2-n_1-n_3} \equiv 1 \bmod q, \tag{5.21}$$

$$g^{2n_3}(x'y') - g^{n_1+n_2}(z')^2 \equiv 0 \bmod q \rightarrow g^{2n_3-n_1-n_2} \equiv 1 \bmod q \tag{5.22}$$

With $n_1, n_2, n_3 < q$ we get two solutions:

2a) $n_1 = n_2 = n_3 \rightarrow n$ or (5.23)

2b) $3n_1 = 3n_2 = 3n_3 \equiv 0 \bmod q$

Where n_1, n_2, n_3 take the 3 values,

$$\frac{1}{3}(q-1), \frac{2}{3}(q-1), (q-1). \tag{5.24}$$

Case 2a)

$$g^n(x'z') \equiv y' \bmod q$$
$$g^n(y'z') \equiv x' \bmod q$$
$$g^n(x'y') \equiv z' \bmod q \qquad (5.25)$$

Make $g^{n+d}x' \equiv y' \bmod q$, $g^{\nu}z' \equiv 1 \bmod q$ hence $g^{d+\nu} \equiv 1 \bmod q$
and $g^{n+\omega}y' \equiv x' \bmod q$, $g^{\nu}z' \equiv 1 \bmod q$ hence $g^{\omega+\nu} \equiv 1 \bmod q \ \therefore d \equiv \omega \bmod q$ and $\nu \equiv -d \bmod q$.
We have $g^{2n+2d}(x'y') \equiv (x'y') \bmod q$,

$$\therefore g^{(2n+2d)} \equiv 1 \bmod q \qquad (5.26)$$

Next write $g^{n+e}z' \equiv x' \bmod q$, $g^{w}y' \equiv 1 \bmod q$, hence $g^{e+w} \equiv 1 \bmod q$
and $g^{n+m}x' \equiv z' \bmod q$, $g^{w}y' \equiv 1 \bmod q$, hence $g^{m+w} \equiv 1 \bmod q \ \therefore e \equiv m \bmod q$ and $w \equiv -e \bmod q$.
We have, $g^{2n+2e}(x'z') \equiv (z'x') \bmod q$,

$$\therefore g^{2n+2e} \equiv 1 \bmod q \qquad (5.27)$$

and write $g^{n+f}z' \equiv y' \bmod q$, $g^{\mu}x' \equiv 1 \bmod q$, hence $g^{f+\mu} \equiv 1 \bmod q$
and $g^{n+l}y' \equiv z' \bmod q$, $g^{\mu}x' \equiv 1 \bmod q$, hence $g^{l+\mu} \equiv 1 \bmod q \ \therefore l \equiv f \bmod q$ and $\mu \equiv -f \bmod q$.
We have, $g^{2n+2f}(y'z') \equiv (z'y') \bmod q$,

$$\therefore g^{2n+2f} \equiv 1 \bmod q \qquad (5.28)$$

Therefore, we have 3 equations if one of $d, e, f \neq 0$ or $q-1$ or one of $2d, 2e, 2f \neq 0$ or $q-1$:

$$g^{(2n+2d)} \equiv 1 \bmod q$$
$$g^{(2n+2e)} \equiv 1 \bmod q$$
$$g^{(2n+2f)} \equiv 1 \bmod q$$

or,

$$(2n+2d) = 0,(q-1),(2q-2)\ldots$$
$$(2n+2e) = 0,(q-1),(2q-2)\ldots$$
$$(2n+2f) = 0,(q-1),(2q-2)\ldots \qquad (5.29)$$

$\therefore e \equiv d \bmod q$, $e \equiv f \bmod q$, $d \equiv f \bmod q$, $d, e, f < q$.
If $e \equiv d \bmod q$ then $z' \equiv y' \bmod q$, if $e \equiv f \bmod q$ then $x' \equiv y' \bmod q$, if $d \equiv f \bmod q$ then $z' \equiv x' \bmod q$ giving $x', y', z' \equiv 0 \bmod q$ because $x' + y' - z' \equiv 0 \bmod q$ (i.e $2y' \equiv z' \bmod q$ hence, $y' \equiv 0 \bmod q$).
If $x', y', z' \equiv 0 \bmod q$ then $x, y, z \equiv 0 \bmod q$ and we have common factor solutions q. (5.30)
Otherwise:
If one of $e, f = 0$ or $q-1$, say f, then $g^n z' \equiv y' \bmod q$, $g^n y' \equiv z' \bmod q$, $x' \equiv 1 \bmod q$ hence since $x' + y' - z' \equiv 0 \bmod q$ then $1 + y' - z' \equiv 0 \bmod q$ and $g^n \equiv 1 \bmod q$, $n = 0$, $y'z' \equiv 1 \bmod q$, but $x'^2 \equiv 1 \bmod q$ hence $x'^2 + y'z' \equiv 2 \bmod q$ which is false. Similarly for $e = 0$. (5.31)
If $d = 0$ or $q-1$ then $g^n x' \equiv y' \bmod q$, $g^n y' \equiv x' \bmod q$, $z' \equiv 1 \bmod q$ but $x' + y' - 1 \equiv 0 \bmod q$ hence $g^n \equiv 1 \bmod q$, $n = 0$, $x'y' \equiv 1 \bmod q$. Moreover, $x' \equiv y' \bmod q$ hence, $x'^2 \equiv 1 \bmod q$, $x' \equiv \pm 1 \bmod q$ and $y'^2 \equiv 1 \bmod q$, $y' \equiv \pm 1 \bmod q$ which is a contradiction in $x' + y' - 1 \equiv 0 \bmod q$. (5.32)
If $2e$ or $2f = q-1$ say $2e$ then $e = \frac{q-1}{2}$ hence $\omega \equiv -\frac{q-1}{2}$ and $y' \equiv -1 \bmod q$, $g^n z' \equiv -x' \bmod q$, $g^n x' \equiv -z' \bmod q$ but $x' - 1 - z' \equiv 0 \bmod q$ hence $g^n \equiv 1 \bmod q$, $n = 0$, $x'z' \equiv -1 \bmod q$, $y'^2 \equiv 1 \bmod q$ $x^a z^c \equiv -1 \bmod q$, $y^{2b} \equiv 1 \bmod q, y^b \equiv \pm 1 \bmod q$. Moreover, $-z' \equiv x' \bmod q$, $z'^2 \equiv 1 \bmod q$, $z' \equiv \pm 1 \bmod q$, $x' \equiv \pm 1 \bmod q$ which is a contradiction with $x' - 1 - z' \equiv 0 \bmod q$. (5.33)
If $2d = q-1$ then $z' \equiv -1 \bmod q$, $x'y' \equiv -1 \bmod q$ and we get a contradiction $z'^2 - x'y' \equiv 2 \bmod q$
If more than 1 of $d, 2e, 2f, = 0$ or $q-1$ then we get 2 or 3 of $z' - y', z' - x', x' - y' \equiv 0 \bmod q$ and we get common factor solutions. (5.34)
Therefore, there are only common factor solutions for Case 2a.

$m=0$ for case **2b)** We have $q=3sp+1$ or $q-1=3sp$ so $g^{3ms}\equiv y'^{3s}\ mod\ q\equiv x'^{3s}\ mod\ q\equiv z'^{3s}\ mod\ q$ hence, $g^{3n_i s}\equiv y'^{3s}\ \therefore y'^{3s}\equiv 1 mod\ q$ as n_1,n_2,n_3 are 1/3 partitions. Therefore, $g^{3ms}\equiv 1 mod\ q,\ s\neq 0, q-1\ \therefore m=0$ (5.35)

Case 2b) When n_1,n_2,n_3 take the 3 values $\frac{1}{3}(q-1), \frac{2}{3}(q-1), (q-1)$ cube both sides to get,

$$x'^3 z'^3\equiv y'^3\ mod\ q$$
$$y'^3 z'^3\equiv x'^3\ mod\ q$$
$$x'^3 y'^3\equiv z'^3\ mod\ q \qquad (5.36)$$

Make $g^{d'}x'^3\equiv y'^3\ mod\ q$, $g^{\nu'}z'^3\equiv 1 mod\ q$ hence $g^{d'+\nu'}\equiv 1 mod\ q$

and $g^{\omega'}y'^3\equiv x'^3\ mod\ q$, $g^{\nu'}z'^3\equiv 1 mod\ q'$ hence $g^{\omega'+\nu'}\equiv 1\ mod\ q\ \therefore d'\equiv\omega' mod\ q$ and $\nu'\equiv -d' mod\ q$.

We have $g^{2d'}(x'^3 y'^3)\equiv(x'^3 y'^3) mod\ q$.

$$\therefore g^{(2d')}\equiv 1 mod\ q \qquad (5.37)$$

Next write $g^{e'}z'^3\equiv x'^3\ mod\ q$, $g^{w'}y'^3\equiv 1 mod\ q$, hence $g^{e'+w'}\equiv 1 mod\ q$

and $g^{m'}x'^3\equiv z'\ mod\ q$, $g^{w}y'^3\equiv 1 mod\ q$, hence $g^{m'+w'}\equiv 1\ mod\ q\ \therefore e'\equiv m'\ mod\ q$ and $w'\equiv -e'\ mod\ q$.

Hence, $g^{2e'}(x'^3 z'^3)\equiv(z'^3 x'^3) mod\ q$.

$$\therefore g^{2e'}\equiv 1 mod\ q \qquad (5.38)$$

and write $g^{f'}z'^3\equiv y'^3\ mod\ q$, $g^{\mu'}x'^3\equiv 1 mod\ q$, hence $g^{f'+\mu'}\equiv 1 mod\ q$

and $g^{l'}y'^3\equiv z'^3\ mod\ q$, $g^{\mu'}x'^3\equiv 1 mod\ q$, hence $g^{l'+\mu'}\equiv 1\ mod\ q\ \therefore l'\equiv f'\ mod\ q$ and $\mu'\equiv -f'\ mod\ q$.

Hence, $g^{2f'}(y'^3 z'^3)\equiv(z'^3 y'^3) mod\ q$.

$$\therefore g^{2f'}\equiv 1 mod\ q \qquad (5.39)$$

Therefore, $2d', 2e', 2f'=0, q-1, 2q-2$ and we have 8 possibilities:

1.) $d', e', f'=0, q-1\ \rightarrow x'^3\equiv 1 mod\ q, y'^3\equiv 1 mod\ q, z'^3\equiv 1 mod\ q$ and from our $n=3,-3$ transformations we get $1\equiv -3x'y'z' mod\ q$ and $1\equiv -3x'^2 y'^2 z'^2\ mod\ q$ respectively $\therefore x'y'z'\equiv 1 mod\ q$ which is a contradiction $(4\neq q)$.

(Note; $(x'y'z')^3(x'^{-3}+y'^{-3}-z'^{-3})=(y'z')^3+(x'z')^3-(x'y')^3$ so use the $-n$ transformation) (5.40)

2.) $2d', 2e', 2f'=q-1, 2q-2.\ \rightarrow x'^3\equiv -1 mod\ q, y'^3\equiv -1 mod\ q, z'^3\equiv -1 mod\ q$ hence we get

$-1\equiv -3x'y'z' mod\ q$ and $1\equiv -3x'^2 y'^2 z'^2\ \therefore x'y'z'\equiv -1 mod\ q$ again a contradiction $(-4\neq q)$. (5.41)

3.) $e'=0, q-1, 2d', 2f'=q-1, 2q-2\rightarrow y'^3\equiv 1 mod\ q, x'^3\equiv -1 mod\ q, z'^3\equiv -1 mod\ q$ hence we get $1\equiv -3x'y'z' mod\ q$

$1\equiv -3x'^2 y'^2 z'^2\ mod\ q\ \therefore x'y'z'\equiv 1 mod\ q$ again a contradiction $(4\neq q)$. (5.42)

4.) $f'=0, q-1, 2d', 2e'=q-1, 2q-2\rightarrow x'^3\equiv 1 mod\ q, y'^3\equiv -1 mod\ q, z'^3\equiv -1 mod\ q$ hence we get

$-1\equiv -3x'y'z' mod\ q$, $1\equiv -3x'^2 y'^2 z'^2\ mod\ q\ \therefore x'y'z'\equiv -1 mod\ q$ again a contradiction $(-4\neq q)$. (5.43)

5.) $d', e'=0, q-1, 2f'=q-1, 2q-2\rightarrow y'^3\equiv 1 mod\ q, x'^3\equiv -1 mod\ q, z'^3\equiv 1 mod\ q$ hence we get $-1\equiv -3x'y'z' mod\ q$

$1\equiv -3x'^2 y'^2 z'^2\ mod\ q\ \therefore x'y'z'\equiv -1 mod\ q$ again a contradiction $(-4\neq q)$. (5.44)

6.) $d', f'=0, q-1, 2e'=q-1, 2q-2\rightarrow y'^3\equiv -1 mod\ q, x'^3\equiv 1 mod\ q, z'^3\equiv 1 mod\ q$ hence we get $-1\equiv -3x'y'z' mod\ q$

$1\equiv -3x'^2 y'^2 z'^2\ mod\ q\ \therefore x'y'z'\equiv -1 mod\ q$ again a contradiction $(-4\neq q)$. (5.45)

7.) $e', f'=0, q-1, 2d'=q-1, 2q-2\rightarrow y'^3\equiv 1 mod\ q, x'^3\equiv 1 mod\ q, z'^3\equiv -1 mod\ q$ hence we get $-3\equiv -3x'y'z' mod\ q$

$-3\equiv -3x'^2 y'^2 z'^2\ mod\ q\ \therefore x'y'z'\equiv 1 mod\ q$ and no contradiction, but $x'^3 z'^3\equiv -1 mod\ q$ and $y'^3\equiv 1 mod\ q$

which is a contradiction. (5.46)

8.) $d'=0, q-1, 2e', 2f'=q-1, 2q-2\rightarrow z'^3\equiv 1 mod\ q, x'^3\equiv -1 mod\ q, y'^3\equiv -1 mod\ q$ hence we get

$-3\equiv -3x'y'z' mod\ q$, $-3\equiv -3x'^2 y'^2 z'^2\ mod\ q\ \therefore x'y'z'\equiv 1 mod\ q$ and **no contradiction.** (5.47)

Therefore, we only have **Case 8.)** possibility.

(Note: The other cases are applicable to the sum/difference combinations in $\pm x^n \pm y^n \pm z^n$)

Case 2b.8) $x'y'z' \equiv 1 mod\ q$ but one of n_1, n_2, n_3 must be 0 or $q-1$ hence for n_1 we get $y'^2 \equiv 1 mod\ q, y' \equiv \pm 1 mod\ q,$ but $+1$ is ruled out above so $y' \equiv -1 mod\ q$, $x'z' \equiv -1 mod\ q \rightarrow x^p z^p \equiv -1 mod\ q,\ \ y^{2p} \equiv 1 mod\ q,\ y^p \equiv \pm 1 mod\ q.$ (5.48)

If $n_2 = 0$ or $q-1$, $x'^2 \equiv 1 mod\ q,\ x' \equiv \pm 1 mod\ q$ but $+1$ is ruled out above so $x' \equiv -1 mod\ q$, $y'z' \equiv -1 mod\ q \rightarrow y^p z^p \equiv -1 mod\ q$ $x^{2p} \equiv 1 mod\ q,\ x^p \equiv \pm 1 mod\ q.$ (5.49)

If $n_3 = 0$ or $q-1$, $z'^2 \equiv 1 mod\ q,\ z' \equiv \pm 1 mod\ q$ but -1 is ruled out above so $z' \equiv 1 mod\ q$, $y'x' \equiv 1 mod\ q \rightarrow x^p y^p \equiv 1 mod\ q$ $z^{2p} \equiv 1 mod\ q,\ z^p \equiv \pm 1 mod\ q.$ Hence, (5.50)

n_1	n_2	n_3
$\mp y^p \equiv y' mod\ q \equiv -1 mod\ q$	$\pm z^p \equiv y' mod\ q$	$\pm x^p \equiv y' mod\ q$
$\pm z^p \equiv x' mod\ q$	$\mp x^p \equiv x' mod\ q \equiv -1 mod\ q$	$\pm y^p \equiv x' mod\ q$
$\pm x^p \equiv z' mod\ q$	$\pm y^p \equiv z' mod\ q$	$\pm z^p \equiv z' mod\ q \equiv 1 mod\ q$ (5.51)

Choose any of $n's$, for example $n_3 = 0, (z^p \equiv \pm 1 mod\ q)$ we have $x^{3p} \equiv \mp 1 mod\ q$ hence $(x^p \pm 1)(x^{2p} \mp x^p + 1) \equiv 0 mod\ q$ and $y^{3p} \equiv \mp 1 mod\ q, (y^p \pm 1)(y^{2p} \mp y^p + 1) \equiv 0 mod\ q.$ These are called the 'form' of the solutions $(n_3 = 0),$

$$z^p \equiv \pm 1 mod\ q$$
$$x^{3p} \equiv \mp 1 mod\ q$$
$$y^{3p} \equiv \mp 1 mod\ q \quad (5.52)$$

(Remark : We can't computer validate this because we have no discrete solutions to choose from. However, we can for the general case, see later)

When $z^p \equiv 1 mod\ q$ then $x^p, y^p \neq -1 mod\ q,$ for if x^p or $y^p \equiv -1 mod\ q$ then y^p or $x^p \equiv 2 mod\ q$ respectively from $x^p + y^p - z^p = 0$ hence, $3 \equiv 0 mod\ q$ which it is not. Therefore, we have 2 quadratic congruences in x^p and y^p with 2 unique solutions for x^p, y^p because if $x^p \equiv y^p\ mod\ q$ then $2x^p, 2y^p \equiv 1 mod\ q,\ 4x^{2p} \equiv 1 mod\ q,\ -4y^p z^p \equiv 1 mod\ q,$ $\pm 4y^p \equiv 1 mod\ q$ which is a contradiction. (5.53)

When $z^p \equiv -1 mod\ q,\ x^{3p} \equiv 1 mod\ q, y^{3p} \equiv 1 mod\ q$ Then $x^{2p} + x^p + 1 \equiv 0 mod\ q,\ \ y^{2p} + y^p + 1 \equiv 0 mod\ q$ solutions and $x^p, y^p \neq 1 mod\ q,$ as above and $x^p \neq y^p\ mod\ q$ also. Therefore, we know $x, y \neq \mp 1 mod\ q.$ (5.55)

We now develop the following method which uses cubic congruences:

Firstly, lets assume $x^3 \neq \mp 1 mod\ q$ and $y^3 \neq \mp 1 mod\ q.$ We can write, $x^3 \equiv u_1 x^2\ mod\ q$ where $u_1{}^{3p} \equiv \mp 1 mod\ q$ (i.e $u_1 \equiv x mod\ q$)

We next write $u_1 \equiv u_2 x^2\ mod\ q$ hence $u_2{}^{3p} \equiv \mp 1 mod\ q$ also. We repeat until $u_{3p-1} \equiv u_{3p} x^2\ mod\ q$ with each $u_N{}^{3p} \equiv \mp 1 mod\ q.$

We can see none of the u_N's equal as this would give $x^{2h} \equiv \pm 1$ which would give the $x^p,\ x^{2p} \equiv \pm 1$ contradictions.

However, there must be a $(\mp 1) mod\ q$ solution and it can't be u_{3p} because that must equal x^3.

Hence we can write, $x^3 \equiv \mp x^2, \mp x^4, \mp x^6 .... \mp x^{6p-2}\ mod\ q.$ (5.56)

One can see that $\mp x^2, \mp x^8 ...$ and $\mp x^4, \mp x^{10} ...$ congruence sequences give $x^{2p} \equiv 1 mod\ q,\ x^p \equiv -1 mod\ q$ respectively which gives common factor solutions or the $3 \equiv 0 mod\ q$ contradiction. So we can write;

$$x^3 \equiv \mp x^6, \mp x^{12} ... \mp x^{6p-6}\ mod\ q \quad (5.57)$$

We also do this for $x^3 \equiv v_1 y^2\ mod\ q$ etc. and $y^3 \equiv v'_1\ y^2\ mod\ q$ etc. *and* $y^3 \equiv u'_1\ x^2\ mod\ q$ etc. to get,

$$x^3 \equiv \mp y^6, \mp y^{12} ... \mp y^{6p-6}\ mod\ q \quad (5.58)$$
$$y^3 \equiv \mp x^6, \mp x^{12} ... \mp x^{6p-6}\ mod\ q \quad (5.59)$$
$$y^3 \equiv \mp y^6, \mp y^{12} ... \mp y^{6p-6}\ mod\ q \quad (5.60)$$

Next we write $x^6 \equiv w_1 x^2 y^2\ mod\ q$ where $w_1{}^p \equiv 1 mod\ q$ repeating we must get a $(+1) mod\ q$ solution for w_N hence we have,

$$x^6 \equiv (xy)^2, (xy)^4 ... (xy)^{2p-2}\ mod\ q \quad (5.61)$$

likewise, $$y^6 \equiv (xy)^2, (xy)^4 ... (xy)^{2p-2}\ mod\ q \quad (5.62)$$

and $$x^3 y^3 \equiv (xy)^2, (xy)^4 ... (xy)^{2p-2}\ mod\ q \text{ if } xy \neq 1 mod\ q^* \quad (5.63)$$

This means that the x^3, y^3 solutions must have the same exponent otherwise $x, y \equiv \mp 1 \ mod\ q$ or $x^3, y^3 \equiv \mp 1 mod\ q$ which have been ruled out. Hence, $x^3 \equiv y^3 \ mod\ q$. (5.64)

$\therefore x^3 - y^3 \equiv 0 \ mod\ q \rightarrow (x-y)(x^2+xy+y^2) \equiv 0 \ mod\ q$, but $x \neq y \ mod\ q\ (x^p \neq y^p \ mod\ q)$ so $(x^2+xy+y^2) \equiv 0 \ mod\ q$,

$(-yz+xy+y^2) \equiv 0 \ mod\ q \ \ \therefore yt \equiv 0 \ mod\ q$ (y gives common factors q so we are left with $t \equiv 0 \ mod\ q$.) (5.65)

*If $xy \equiv 1 mod\ q$ then with either $z \equiv \pm 1 mod\ q$ or $z \neq \pm 1 mod\ q$ we get: If $z \equiv \pm 1 mod\ q$ then $z^2 - xy \equiv 0 \ mod\ q$ and therefore, $t \equiv 0 \ mod\ q$. (5.66)

(i.e $x^2 + yz - z^2 + xy = (x+z)(x-z+y) = (x+z)t$ and $x \equiv -z \ mod\ q$ gives common factors q or $3 \equiv 0 \ mod\ q$)

If $z \neq 1 mod\ q$ we repeat our analysis above but with $z \neq \pm 1 mod\ q$ and $y^3 \neq \mp 1 mod\ q$ (see below #) to get $y^3 + z^3 \equiv 0 \ mod\ q$, $(z+y)(z^2 - yz + y^2) \equiv 0 \ mod\ q$, $z \neq -y \ mod\ q\ (z^p \neq -y^p \ mod\ q)$ and $(z^2 - yz + y^2) \equiv 0 \ mod\ q$, $(x^2 + y^2 + z^2) \equiv 0 \ mod\ q$

$= (3t^2 + 2_{-1}r) \equiv t^2 \ mod\ q \equiv 0 \ mod\ q \ \therefore t \equiv 0 \ mod\ q$.

or we have $y^3 z^3 \equiv -1 mod\ q$ but if this is the case then we would repeat our analysis again but instead with $z \neq \pm 1 mod\ q$ and $x^3 \neq \mp 1 mod\ q$ giving $(x^3 + z^3) \equiv 0 \ mod\ q \rightarrow zt \equiv 0 \ mod\ q$ or $x^3 z^3 \equiv -1 mod\ q$. But if both $y^3 z^3 \equiv -1 mod\ q$ and $x^3 z^3 \equiv -1 mod\ q$ we have $x^3 - y^3 \equiv 0 \ mod\ q \rightarrow yt \equiv 0 \ mod\ q$ as before. $\therefore t \equiv 0 \ mod\ q$. (5.67)

Next we assume $x^3 \equiv \mp 1 mod\ q$ but $y^3 \neq \mp 1 mod\ q$ and $z \neq \pm 1 mod\ q$ (Note: if p=3 then if $x^3 \equiv \mp 1 mod\ q$ then because $z^3 \equiv \pm 1 mod\ q$, $y^3 \equiv \pm 2 \ mod\ q$ contradiction. Hence, $z^3, z^6 \neq \pm 1 mod\ q$ for $p > 3$.)

Make, $z^3 \equiv w'_1 y^2$ where $w_1{}'^{3p} \equiv \pm 1 mod\ q$ etc. so we get $z^3 \equiv \pm y^2, \pm y^4 ... \pm y^{6p-2} \ mod\ q$ and refining,

$$z^3 \equiv \pm y^6, \pm y^{12} ... \pm y^{6p-6} \ mod\ q \quad (5.68)$$

With $z^3 \equiv w_1{}'' z^2 \ mod\ q$ etc. giving, $z^3 \equiv \pm z^2, \pm z^4 ... z^{2p-2} \ mod\ q$ (5.69)

likewise, $y^3 \equiv \mp y^6, \mp y^{12} ... \mp y^{6p-6} \ mod\ q$ (5.70)

$y^3 \equiv \mp z^2, \mp z^4 ... \mp z^{2p-2} \ mod\ q$ (5.71)

$z^6 \equiv (yz)^6, (yz)^{12} ... (yz)^{6p-6} \ mod\ q$ (Note, $z^6 \neq \mp 1 mod\ q$ as $z^p \equiv \pm 1 mod\ q$) (5.72)

$y^6 \equiv (yz)^6, (yz)^{12} ... (yz)^{6p-6} \ mod\ q$ (Note, $y^6 \neq \pm 1$, as $y^{3p} \equiv \mp 1 mod\ q$) (5.73)

$y^3 z^3 \equiv -(yz)^6, -(yz)^{12} ... -(yz)^{6p-6} \ mod\ q$ if $y^3 z^3 \neq -1 mod\ q$ ◊ (5.74)

Hence $y^3 + z^3 \equiv 0 \ mod\ q$ $(z+y)(z^2 - yz + y^2) \equiv 0 \ mod\ q$, $z \neq -y \ mod\ q\ (z^p \neq -y^p \ mod\ q)$ and $(z^2 - yz + y^2) \equiv 0 \ mod\ q$

$(x^2 + y^2 + z^2) \equiv 0 \ mod\ q = (3t^2 + 2r) \equiv 0 \ mod\ q$, $t^2 \equiv 0 \ mod\ q$ therefore, $t \equiv 0 \ mod\ q$. (5.75)

◊ If $y^3 z^3 \equiv -1 mod\ q$ which it would be for our $_{x/t}r$ choice then with $y^3 \equiv \mp z^2, \mp z^4 ... \mp z^{2p-2} \ mod\ q$ and $y^3 \equiv \mp y^6, \mp y^{12} ... \mp y^{6p-6} \ mod\ q$ write $z \equiv wz^2 \ mod\ q$ etc. to get,

$$z \equiv \pm z^2, \pm z^4 ... \pm z^{2p-2} \ mod\ q \quad (5.76)$$

and with $z \equiv v' y^2 \ mod\ q$... etc. to get $z \equiv \pm y^6, \pm y^{12} ... \pm y^{6p-6} \ mod\ q$ (5.77)

Moreover, write $y^3 z \equiv uzy^2 \ mod\ q$ etc. $y^3 z \equiv \mp z^3 y^6, \mp z^6 y^{12} ... \mp z^{3p-3} y^{6p-6} \ mod\ q$ (5.78)

and $y^6 \equiv u' y^2 zm \ od\ q$ etc. $y^6 \equiv y^6 z^3, y^{12} z^6 .... y^{6p-6} z^{3p-3} \ mod\ q$ (5.79)

and $z^2 \equiv w''' y^2 z \ mod\ q$ etc. $z^2 \equiv y^6 z^3, y^{12} z^6 .... y^{6p-6} z^{3p-3} \ mod\ q$ (5.80)

Therefore, y^3, z must have the same exponents hence $y^3 \equiv -z \ mod\ q$, $z^4 \equiv 1 mod\ q$ and hence $z \equiv \pm 1 mod\ q$ which is a contradiction. (5.81)

If $y^3 \equiv \mp 1 mod\ q$ and $x^3, z \neq \mp 1 \pm 1 mod\ q$ respectively then we repeat analysis # to get $z^3 + x^3 \equiv 0 \ mod\ q \rightarrow z^2 - xz + x^2 \rightarrow$

$$\therefore -zt \equiv 0 \ mod\ q \quad (5.82)$$

or $z^3 x^3 \equiv -1 mod\ q$. In this case we can repeat similarly ◊ above but with x congruence sequences to get $z \equiv \pm 1 mod\ q$ contradiction. (5.83)

If $x^3, y^3 \equiv \mp 1 mod\ q$ then we get $x^3 - y^3 \equiv 0 \ mod\ q \rightarrow (x-y)(x^2+xy+y^2) \equiv 0 \ mod\ q \rightarrow \therefore yt \equiv 0 \ mod\ q$ as above. (5.84)

If $x^3, z \equiv \mp 1, \pm 1$ then we get $x^3 + z^3 \equiv 0 \ mod\ q \rightarrow z^2 - xz + x^2 \rightarrow \therefore -zt \equiv 0 \ mod\ q$ as above. (5.85)

If $y^3, z \equiv \mp 1, \pm 1$ then we get $y^3 + z^3 \equiv 0 \ mod\ q \rightarrow (z+y)(z^2 - yz + y^2) \equiv 0 \ mod\ q \rightarrow t \equiv 0 \ mod\ q$ as above. (5.86)

Therefore, for all cases we either have common factor solutions q or $t \equiv 0 \, mod \, q$.
For $t \equiv 0 \, mod \, q$, the special case allows us to factor out the common factors, hence t must contain all the prime decompositions of $x^2 + yz$. So we can now use an inequality argument for primes p (exponent p) of the form $M3 + 1$ and $M3$ -1. So looking at our transformation equation examples and corollary18.

$x^5 + y^5 - z^5 = 11t^5 + 15t^3 r - 10xyzt^2 + 5r^2 t - 5xyzr$

$x^7 + y^7 - z^7 = 29t^7 + 56t^5 r - 35xyzt^4 + 35r^2 t^3 - 35xyzt^2 r + 7tr^3 + 7(xyz)^2 t - 7r^2 xyz$ Where r is ${}_{-1}r$

We have, $t = M_{x/t} r$ but ${}_{x/t}r = x^2 + yz > t \;\; \therefore \; {}_{x/t}r$ must contain a power of $q's = q_1, q_2, q_3 ...$ (say q_1 is a power) but for $p = M3 + 1$ we have from our $t, {}_{-1}r$ equation $t = Mq_1^{\,2}$ so if q_1 is a power then,

$$x^2 + yz = Mq_1^{\,2} \rightarrow t = Mq_1^{\,2} \rightarrow {}_{-1}r \rightarrow Mq_1^{\,2}, t \rightarrow Mq_1^{\,4} \tag{5.87}$$

but then $x^2 + yz > t > q^2{}_1 q_2 q_3$ which is an inequality so q_1 must be a higher power q_1^4 hence,

$$x^2 + yz = Mq_1^{\,4} \rightarrow t = Mq_1^{\,4} \rightarrow {}_{-1}r \rightarrow Mq_1^{\,4}, t \rightarrow Mq_1^{\,8} \tag{5.88}$$

but then $x^2 + yz > t > q^4{}_1 q_2 q_3$ and so on ad infinitum hence $t \rightarrow \infty$. (5.89)

For primes of the form $M3$-1 we get from our transformation ${}_{-1}r = Mq_1^{\,2}$ but ${}_{-1}r = x^2 + yz - xt - t^2$ and ${}_{x/t}r = q_1^{\,2} q_2 ...$ Therefore, $xt = Mq_1^{\,2}$ so either common factors or $t = Mq_1^{\,2}$ but $x^2 + yz > t > q^2{}_1 q_2 q_3$ which is an inequality so q_1 must be a higher power, say q_1^3 hence, $x^2 + yz = Mq_1^3$, ${}_{-1}r = Mq_1^{\,4}$ from our transformation and then $xt = Mq_1^{\,3} \rightarrow t = Mq_1^{\,3}$ and so on ad infinitum $t \rightarrow \infty$. (5.90)

For $p = 3$ we get directly $3xyz \equiv 0 \, mod \, q$ for $q > 3$ 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. (5.91)

t can not go to infintity because then $x, y, z \rightarrow \infty$ which is not possible.

Lastly we could have $t = 0$ however if we look at our transformation equations for $p > 7$, ${}_{-1}r$ must share q with xyz hence common factor solutions. For $p = 3, t = 0$ we get $3xyz = 0$

For $p = 5, 7$ we have $xyz = 0$ or ${}_{-1}r = 0$, which gives $x^2 = yz$ and we get common factors again. (5.92)

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

Theorem 6 The General Case (Beal's Conjecture).

$x^a + y^b - z^c = 0$ *has no integer co-prime solutions in* $x,y,z > 1$ *for* $a,b,c > 2$.

Proof

Make q a prime decomposition factor of $R = x^{2a} + y^b z^c$ which is odd > 0 and must also be a prime decomposition factor of $y^{2b} + x^a z^c$ and $z^{2c} - x^a y^b$. Again one of x,y,z is even so q is *odd* > 0 and q must be > 3 because at least 2 of $x,y,z > 1$. (6.01)

Lemma 6 *q can not be a power of* $3 \to 3^n$ *for* $n > 1$.

Firstly all of $x,y,z = M3 \pm 1$ (if one of $x,y,z = M3$ and $R = M3$ we would have the common factor 3)

Assume $q = 3^n$ We have, $x^a + y^b - z^c = (m_1 3 \pm *1)^a + (m_2 3 \pm *1)^b - (m_3 3 \pm *1)^c = 0$

* sign depends on odd/even exponents such that the sum equals ± 3.

$\therefore M9 \pm am_1 3 \pm bm_2 3 \pm cm_3 3 \pm 3 = 0$.

We also have, $x^{4a} + y^{4b} + z^{4c} = MT + 2R^2 = 2(M9^n), (T = 0)$ hence $(m_1 3 \pm *1)^{4a} + (m_2 3 \pm *1)^{4b} + (m_3 3 \pm *1)^{4c} = M9^n$

$\therefore M9 \pm 4am_1 3 \pm 4bm_2 3 \pm 4cm_3 3 + 3 = M9^n$ and we get for $\pm am_1 3 \pm bm_2 3 \pm cm_3 3 = 3$ we get $12 + 3 = M9$ which is false.

$\therefore \pm am_1 3 \pm bm_2 3 \pm cm_3 3 = -3$ and with $x^{2a} + y^{2b} + z^{2c} = MT + 2R = M3^n$ we get $M9 - 3 = M3^n$. Therefore $n = 1$.

Furthermore, we have **Case 1.)** $q = s3 - 1$,

Let,
$$la = u_1 q - v_1 \quad \text{where } u_N - v_N = 0$$
$$lb = u_2 q - v_2$$
$$lc = u_3 q - v_3$$

hence,
$$la = v_1(q-1),\ lb = v_2(q-1),\ lc = v_3(q-1) \tag{6.02}$$

$\therefore l = q - 1$, l is even $\neq M3$ and we can write,

$$x^{al} + y^{bl} + z^{cl} = 0 + 2(R)^{\frac{l}{2}} + \frac{l(\frac{l-4}{2})}{2!}(x^a y^b z^c)^2 (R)^{\frac{l-6}{2}} + \frac{l(\frac{l-6}{2})(\frac{l-8}{2})(\frac{l-10}{2})}{4!}(x^a y^b z^c)^4 (R)^{\frac{l-12}{2}} +$$
$$\frac{l(\frac{l-8}{2})(\frac{l-10}{2})...(\frac{l-16}{2})}{6!}(x^a y^b z^c)^6 (R)^{\frac{l-18}{2}} + ... \frac{l(\frac{l-(m+2)}{2})(\frac{(l-(m+4))}{2})...(\frac{l-(3m-2)}{2})}{m!}(x^a y^b z^c)^m (R)^{\frac{l-3m}{2}} \tag{6.03}$$

$LHS \equiv 3 \bmod q$ if $x,y,z \neq Mq$

$RHS \equiv 0 \bmod q$ (Note: $R = {}_{x^a/T} R$ when $T = 0$)

$\therefore q/3$ is a null result.

Therefore, we have $q = (3s+1)$ or a combination $q_1 q_2 = 3(3s+1)$ but $q > 3$ hence there must be a prime decomposition factor $q = 3s + 1$ which we will use.

Writing double partial congruences,

$$g^m x^a z^c \equiv y' \bmod q \qquad g^{n_1} x' z' \equiv y' \bmod q$$
$$g^m y^b z^c \equiv x' \bmod q \qquad g^{n_2} y' z' \equiv x' \bmod q$$
$$g^m x^a y^b \equiv z' \bmod q \qquad g^{n_3} x' y' \equiv z' \bmod q \tag{6.04}$$

Where $x^a z^c + y^b z^c - x^a y^b = x^{2a} + y^b z^c \equiv x' + y' - z' \equiv 0 \bmod q$ and $x'^2 + y' z' \equiv 0 \bmod q$, $y'^2 + x' z' \equiv 0 \bmod q$, $z'^2 - x' y' \equiv 0 \bmod q$.

Therefore, we have solutions for n_1, n_2, n_3 as before $g^{2n_1 - n_2 - n_3} \equiv 1 \bmod q$, $g^{2n_2 - n_1 - n_3} \equiv 1 \bmod q$, $g^{2n_3 - n_1 - n_2} \equiv 1 \bmod q$ with $n_1, n_2, n_3 < q$ we get two solutions;

2a) $n_1 = n_2 = n_3 \to n$ (6.05)

2b) $3n_1 = 3n_2 = 3n_3 \equiv 0 \bmod q$ (6.06)

where n_1, n_2, n_3 take the 3 values,

$$\frac{1}{3}(q-1),\ \frac{2}{3}(q-1),\ (q-1). \tag{6.07}$$

Case 2a

$$g^n(x'z') \equiv y' \bmod q$$
$$g^n(y'z') \equiv x' \bmod q$$
$$g^n(x'y') \equiv z' \bmod q$$

Make $g^{n+d}x' \equiv y' \bmod q$, $g^{\nu}z' \equiv 1 \bmod q$ hence $g^{d+\nu} \equiv 1 \bmod q$.

and $g^{n+\omega}y' \equiv x' \bmod q$, $g^{\nu}z' \equiv 1 \bmod q'$ hence, $g^{\omega+\nu} \equiv 1 \bmod q$, $\therefore d \equiv \omega \bmod q$ and $\nu \equiv -d \bmod q$.

We have, $g^{2n+2d}(x'y') \equiv (x'y') \bmod q$,

$$\therefore g^{(2n+2d)} \equiv 1 \bmod q \tag{6.08}$$

Next write $g^{n+e}z' \equiv x' \bmod q$, $g^{w}y' \equiv 1 \bmod q$, hence $g^{e+w} \equiv 1 \bmod q$.

and $g^{n+m}x' \equiv z' \bmod q$, $g^{w}y' \equiv 1 \bmod q$, hence $g^{m+w} \equiv 1 \bmod q$ $\therefore e \equiv m \bmod q$ and $w \equiv -e \bmod q$.

Hence, $g^{2n+2e}(x'z') \equiv (z'x') \bmod q$,

$$\therefore g^{2n+2e} \equiv 1 \bmod q \tag{6.09}$$

and write $g^{n+f}z' \equiv y' \bmod q$, $g^{\mu}x' \equiv 1 \bmod q$, hence $g^{f+\mu} \equiv 1 \bmod q$,

and $g^{n+l}y' \equiv z' \bmod q$, $g^{\mu}x' \equiv 1 \bmod q$, hence $g^{l+\mu} \equiv 1 \bmod q$ $\therefore l \equiv f \bmod q$ and $\mu \equiv -f \bmod q$.

Hence, $g^{2n+2f}(y'z') \equiv (z'y') \bmod q$.

$$\therefore g^{2n+2f} \equiv 1 \bmod q \tag{6.10}$$

Therefore, we have 3 equations if one of $d, e, f \neq 0$ *or* $q-1$ or one of $2d, 2e, 2f \neq 0$ or $q-1$.

$$g^{(2n+2d)} \equiv 1 \bmod q$$
$$g^{(2n+2e)} \equiv 1 \bmod q$$
$$g^{(2n+2f)} \equiv 1 \bmod q$$
$$(2n+2d) = 0, (q-1), (2q-2)\ldots$$
$$(2n+2e) = 0, (q-1), (2q-2)\ldots$$
$$(2n+2f) = 0, (q-1), (2q-2)\ldots \tag{6.11}$$

$$\therefore e \equiv d \bmod q,\ e \equiv f \bmod q,\ d \equiv f \bmod q \quad \text{as } d, e, f < q. \tag{6.12}$$

If $e \equiv d \bmod q$ then $z' \equiv y' \bmod q$, if $e \equiv f \bmod q$ then $x' \equiv y' \bmod q$, if $d \equiv f \bmod q$ then $z' \equiv x' \bmod q$ again giving $x', y', z' \equiv 0 \bmod q$ because $x' + y' + z' \equiv 0 \bmod q$. If $x', y', z' \equiv 0 \bmod q$ then $x, y, z \equiv 0 \bmod q$ and we have common factor solutions q. (6.13)

Otherwise:

If one of $e, f = 0$ or $q-1$, say f, then $g^n z' \equiv y' \bmod q$, $g^n y' \equiv z' \bmod q$, $x' \equiv 1 \bmod q$ hence since $x' + y' - z' \equiv 0 \bmod q$ then $1 + y' - z' \equiv 0 \bmod q$, and $g^n \equiv 1 \bmod q$, $n = 0$, $y'z' \equiv 1 \bmod q$, but $x'^2 \equiv 1 \bmod q$ hence $x'^2 + y'z' \equiv 2 \bmod q$ which is false. Similarly for $e = 0$. (6.14)

If $d = 0$ or $q-1$ then $g^n x' = y' \bmod q$, $g^n y' = x' \bmod q$, $z' \equiv 1 \bmod q$ but $x' + y' - 1 \equiv 0 \bmod q$ hence $g^n \equiv 1 \bmod q$, $n = 0$, $x'y' \equiv 1 \bmod q$, $x^a y^b \equiv 1 \bmod q$, $z^{2c} \equiv 1 \bmod q$, $z^c \equiv \pm 1 \bmod q$. Moreover, $x' \equiv y' \bmod q$ hence $x'^2 \equiv 1 \bmod q$, $x' \equiv \pm 1 \bmod q$ and $y'^2 \equiv 1 \bmod q$, $y' \equiv \pm 1 \bmod q$ which is a contradition in $x' + y' - 1 \equiv 0 \bmod q$. (6.15)

If $2e$ or $2f = q-1$, say $2e$, then $e = \dfrac{q-1}{2}$ hence $\omega \equiv -\dfrac{q-1}{2}$ and $y' \equiv -1 \bmod q$, $g^n z' \equiv -x' \bmod q$, $g^n x' \equiv -z' \bmod q$ but $x' - 1 - z' \equiv 0 \bmod q$ hence $g^n \equiv 1 \bmod q$, $n = 0$, $x'z' \equiv -1 \bmod q$, $y'^2 \equiv 1 \bmod q$, $x^a z^c \equiv -1 \bmod q$, $y^{2b} \equiv 1 \bmod q$, $y^b \equiv \pm 1 \bmod q$, moreover $-z' \equiv x' \bmod q$, $z'^2 \equiv 1 \bmod q$, $z' \equiv \pm 1 \bmod q$, $x' \equiv \pm 1 \bmod q$ which is a contradiction with $x' - 1 - z' \equiv 0 \bmod q$. (6.16)

If $2d = q-1$ then $z' \equiv -1 \bmod q$, $x'y' \equiv -1 \bmod q$ and we get a contradiction $z'^2 - x'y' \equiv 2 \bmod q$. (6.17)

If more than 1 of $d, 2e, 2f = 0$ or $q-1$ then we get 2 or 3 of $z' - y', z' - x', x' - y' \equiv 0 \bmod q$ and we get common factor solutions. (6.18)

Case 2b)

When n_1, n_2, n_3 take the 3 values $\frac{1}{3}(q-1), \frac{2}{3}(q-1), (q-1)$ cube both sides to get,

$$x'^3 z'^3 \equiv y'^3 \bmod q$$
$$y'^3 z'^3 \equiv x'^3 \bmod q$$
$$x'^3 y'^3 \equiv z'^3 \bmod q \tag{6.19}$$

Make $g^{d'} x'^3 \equiv y'^3 \bmod q$, $g^{\nu'} z'^3 \equiv 1 \bmod q$ hence $g^{d'+\nu'} \equiv 1 \bmod q$,

and $g^{\omega'} y'^3 \equiv x'^3 \bmod q$, $g^{\nu'} z'^3 \equiv 1 \bmod q'$ hence $g^{\omega'+\nu'} \equiv 1 \bmod q \ \therefore d' \equiv \omega' \bmod q$ and $\nu' \equiv -d' \bmod q$.

We have, $g^{2d'}(x'^3 y'^3) \equiv (x'^3 y'^3) \bmod q$,

$$\therefore g^{2d'} \equiv 1 \bmod q \tag{6.20}$$

Next write $g^{e'} z'^3 \equiv x'^3 \bmod q$, $g^{w'} y'^3 \equiv 1 \bmod q$, hence $g^{e'+w'} \equiv 1 \bmod q$

and $g^{m'} x'^3 \equiv z' \bmod q$, $g^{w} y'^3 \equiv 1 \bmod q$, hence $g^{m'+w'} \equiv 1 \bmod q \ \therefore e' \equiv m' \bmod q$ and $w' \equiv -e' \bmod q$.

Hence, $g^{2e'}(x'^3 z'^3) \equiv (z'^3 x'^3) \bmod q$,

$$\therefore g^{2e'} \equiv 1 \bmod q \tag{6.21}$$

and write $g^{f'} z'^3 \equiv y'^3 \bmod q$, $g^{\mu'} x'^3 \equiv 1 \bmod q$, hence $g^{f'+\mu'} \equiv 1 \bmod q$

and $g^{l'} y'^3 \equiv z'^3 \bmod q$, $g^{\mu'} x'^3 \equiv 1 \bmod q$, hence $g^{l'+\mu'} \equiv 1 \bmod q \ \therefore l' \equiv f' \bmod q$ and $\mu' \equiv -f' \bmod q$.

Hence, $g^{2f'}(y'^3 z'^3) \equiv (z'^3 y'^3) \bmod q$,

$$\therefore g^{2f'} \equiv 1 \bmod q \tag{6.22}$$

Therefore $2d', 2e', 2f' = 0, q-1, 2q-2$ and we have 8 possibilities: (6.23)

1.) $d', e', f' = 0, q-1 \rightarrow x'^3 \equiv 1 \bmod q, y'^3 \equiv 1 \bmod q, z'^3 \equiv 1 \bmod q$ and from our $n = 3, -3$ equations we get

$1 \equiv -3x'y'z' \bmod q$ and $1 \equiv -3x'^2 y'^2 z'^2 \bmod q$ respectively. Therefore, $x'y'z' \equiv 1 \bmod q$ which is a contradiction $(4 \neq q)$. (6.24)

2.) $2d', 2e', 2f' = q-1, 2q-2. \rightarrow x'^3 \equiv -1 \bmod q, y'^3 \equiv -1 \bmod q, z'^3 \equiv -1 \bmod q$ hence we get

$-1 \equiv -3x'y'z' \bmod q$ and $1 \equiv -3x'^2 y'^2 z'^2 \ \therefore x'y'z' \equiv -1 \bmod q$ again a contradiction $(-4 \neq q)$. (6.25)

3.) $e = 0, q-1, 2d, 2f = q-1, 2q-2 \rightarrow y'^3 \equiv 1 \bmod q, x'^3 \equiv -1 \bmod q, z'^3 \equiv -1 \bmod q$ hence we get $1 \equiv -3x'y'z' \bmod q$

$1 \equiv -3x'^2 y'^2 z'^2 \bmod q \ \therefore x'y'z' \equiv 1 \bmod q$ again a contradiction $(4 \neq q)$. (6.26)

4.) $f = 0, q-1, 2d, 2e = q-1, 2q-2 \rightarrow x'^3 \equiv 1 \bmod q, y'^3 \equiv -1 \bmod q, z'^3 \equiv -1 \bmod q$ hence we get $-1 \equiv -3x'y'z' \bmod q$

$1 \equiv -3x'^2 y'^2 z'^2 \bmod q \ \therefore x'y'z' \equiv -1 \bmod q$ again a contradiction $(-4 \neq q)$. (6.27)

5.) $d, e = 0, q-1, 2f = q-1, 2q-2 \rightarrow y'^3 \equiv 1 \bmod q, x'^3 \equiv -1 \bmod q, z'^3 \equiv 1 \bmod q$ hence we get $-1 \equiv -3x'y'z' \bmod q$

$1 \equiv -3x'^2 y'^2 z'^2 \bmod q \ \therefore x'y'z' \equiv -1 \bmod q$ again a contradiction $(-4 \neq q)$. (6.28)

6.) $d, f = 0, q-1, 2e = q-1, 2q-2 \rightarrow y'^3 \equiv -1 \bmod q, x'^3 \equiv 1 \bmod q, z'^3 \equiv 1 \bmod q$ hence we get $-1 \equiv -3x'y'z' \bmod q$

$1 \equiv -3x'^2 y'^2 z'^2 \bmod q \ \therefore x'y'z' \equiv -1 \bmod q$ again a contradiction $(-4 \neq q)$. (6.29)

7.) $e, f = 0, q-1, 2d = q-1, 2q-2 \rightarrow y'^3 \equiv 1 \bmod q, x'^3 \equiv 1 \bmod q, z'^3 \equiv -1 \bmod q$ hence we get $-3 \equiv -3x'y'z' \bmod q$

$-3 \equiv -3x'^2 y'^2 z'^2 \bmod q \ \therefore x'y'z' \equiv 1 \bmod q$ and no contradiction, but $x'^3 z'^3 \equiv -1 \bmod q$ and $y'^3 \equiv 1 \bmod q$

which is a contradiction. (6.30)

8.) $d' = 0, q-1, 2e', 2f' = q-1, 2q-2 \rightarrow z'^3 \equiv 1 \bmod q, x'^3 \equiv -1 \bmod q, y'^3 \equiv -1 \bmod q$ hence we get

$-3 \equiv -3x'y'z' \bmod q, -3 \equiv -3x'^2 y'^2 z'^2 \bmod q \ \therefore x'y'z' \equiv 1 \bmod q$ and **no contradiction.** (6.31)

Therefore we have only **Case 8.)** possibility.

(Note: The other cases are applicable to the sum/difference combinations in $\pm x^a \pm y^b \pm z^c$)

Case 2b. 8) $x'y'z' \equiv 1 mod\, q'$ but one of n_1, n_2, n_3 must be 0 or $q-1$ hence for n_1 we get $y'^2 \equiv 1 mod\, q$, $y' \equiv \pm 1 mod\, q$ but $+1$ is ruled out above so $y' \equiv -1 mod\, q$, $x'z' \equiv -1 mod\, q \rightarrow x^a z^c \equiv -1 mod\, q$, $y^{2b} \equiv 1 mod\, q$, $y^b \equiv \pm 1 mod\, q$. (6.32)

If $n_2 = 0$ or $q-1$, $x'^2 \equiv 1 mod\, q$, $x' \equiv \pm 1 mod\, q$ but +1 is ruled out above so $x' \equiv -1 mod\, q$, $y'z' \equiv -1 mod\, q \rightarrow y^b z^c \equiv -1 mod\, q$, $x^{2a} \equiv 1 mod\, q$, $x^a \equiv \pm 1 mod\, q$. (6.33)

If $n_3 = 0$ or $q-1$, $z'^2 \equiv 1 mod\, q$, $z' \equiv \pm 1 mod\, q$ but -1 is ruled out above so $z' \equiv 1 mod\, q$, $y'x' \equiv 1 mod\, q \rightarrow x^a y^b \equiv 1 mod\, q$, $z^{2c} \equiv 1 mod\, q$, $z^a \equiv \pm 1 mod\, q$. Moreover, we can write; (6.34)

$$\begin{array}{lll} \mp y^b \equiv y' mod\, q \equiv -1 mod\, q & \pm z^c \equiv y' mod\, q & \pm x^a \equiv y' mod\, q \\ \pm z^c \equiv x' mod\, q & \mp x^a \equiv x' mod\, q \equiv -1 mod\, q & \pm y^b \equiv x' mod\, q \\ \pm x^a \equiv z' mod\, q & \pm y^b \equiv z' mod\, q & \pm z^c \equiv z' mod\, q \equiv 1 mod\, q \end{array} \quad (6.35)$$

Choose $n_1 = 0$ this time. We have $x^{2a} \pm z^c \equiv 0 mod\, q$, $z^{2c} \mp x^a \equiv 0 mod\, q$ for $n_1 = 0$ we have,

$$\begin{aligned} y^b &\equiv \pm 1 mod\, q \\ x^{3a} &\equiv \pm 1 mod\, q \\ z^{3c} &\equiv \mp 1 mod\, q \end{aligned} \quad (6.36)$$

without the g^m phase number as these are redundant with the methods we use *(*i.e multiplying R or $x^a + y^b - z^c$ by g^{4m} or g^{2m}*)*. So $x^a \neq \pm 1 mod\, q$ for we would get $z^c \equiv \pm 2 mod\, q \rightarrow 3 \neq 0 mod\, q$ hence $x^{2a} \pm x^a + 1 \equiv 0 mod\, q$, $z^c \neq \mp 1 mod\, q$ for we would get $x^a \equiv \mp 2 mod\, q \rightarrow 3 \neq 0 mod\, q$ hence, $z^{2c} \mp z^c + 1 \equiv 0 mod\, q$.

If x^a or $z^c \equiv \pm 1 mod\, q$ then z^c, $x^a \equiv 2 mod\, q$ respectively. Hence, $3 \equiv 0 mod\, q$ which it is not. Hence we have 2 quadratic congruence solutions for x^a with z^c being the other negative $mod\, q$ solution since $x^a + z^c \neq 0 mod\, q$ otherwise, $2x^a \equiv \mp 1 mod\, q$, $2z^c \equiv \pm 1 \rightarrow 4x^{2a} \equiv 1 mod\, q$, $4z^c \equiv 1 mod\, q$ contradiction. (6.37)

Computer Verification. One may choose discrete equations where one or more of $a,b,c = 1$ or 2 and once the phase number m is found we verify the form of the solutions. From our Example 1.) 5+7=12, $_{x/t}r = 109$, $m = 28$ we get $g^{14} y \equiv -1 mod\, q$ $g^{42} x^3 \equiv -1 mod\, q$, $g^{42} z^3 \equiv 1 mod\, q$. Example 2.) we have $x + y^3 - z^5 = 0$ and $x = 118$, $y = 5$ and $z = 3$, $R = (31)(1429) \rightarrow m = 0$, $q = 31$ we get $x^{3a} \equiv 1 mod\, q$, $y^b \equiv 1 mod\, q$ and $z^{3c} \equiv -1 mod\, q$, $m = 24$, $q_2 = 1429$. This gives $g^{12} y^b \equiv 1 mod\, 1429$ in this example and $g^{36} x^{3a} \equiv 1 mod\, q$, $g^{36} z^{3c} \equiv -1 mod\, q$. In fact we can choose g^m such that any of $n_1, n_2, n_3 = 0$.

Lets assume, $x^3 \neq \pm 1 mod\, q$ and $z^3 \neq \mp 1 mod\, q$ with a,b,c odd *(*this assumption therefore excludes $a,c = 1$*)* we have, $y^{2b} + x^a z^c \equiv 0 mod\, q$. We know x^a, $z^c \neq \pm 1, \mp 1 mod\, q$ otherwise we get our $3 \equiv 0 mod\, q$ contradiction. Therefore, write $x^a \equiv u_1 z^2 mod\, q$, hence $u_1^{3c} \equiv \pm 1 mod\, q$ etc. and there must exist a $(\pm 1) mod\, q$ congruence at u_N.

Now, we can include the g^m phase number but we don't need too because the methods deal with the same exponents in the congruence sequences and these have the same $g^{m's}$ which become redundant.

So we can write our congruence sequence;

$$x^a \equiv \pm (z)^2, \pm (z)^4 \ldots \pm (z)^{6c-2} mod\, q \quad (6.38)$$

Likewise, $$z^c \equiv \mp (x)^2, \mp (x)^4 \ldots \mp (x)^{6a-2} mod\, q \quad (6.39)$$

Remark: If a,c are composite and a',c' is a factor of a,c respectively and is such that $x^{a'} \equiv \pm 1 mod\, q$, $z^{c'} \equiv \mp 1 mod\, q$ then $x^a, z^c \equiv \pm 1, \mp 1 mod\, q$ contradiction.

Furthermore, write $x^a \equiv u'_1 x^2 mod\, q$ etc. and $z^c \equiv w' z^2 mod\, q$ etc. to get,

$$x^a \equiv \pm (x)^2, \pm (x)^4 \ldots \pm (x)^{6a-2} mod\, q \quad (6.40)$$

$$z^c \equiv \mp (z)^2, \mp (z)^4, \ldots \mp (z)^{6c-2} mod\, q \quad (6.41)$$

Make $x^{2a} \equiv u''_1 (xz)^2 mod\, q$ hence $u''_1{}^{3ac} \equiv 1 mod\, q$ etc. and $z^{2c} \equiv w''(xz)^2$ hence $w_1''^{3ac} \equiv 1 mod\, q$ *etc*. therefore,

$$x^{2a} \equiv (xz)^2, (xz)^4 \ldots (xz)^{6ac-2} mod\, q \quad (6.42)$$

$$z^{2c} \equiv (xz)^2, (xz)^4 \ldots (xz)^{6ac-2} mod\, q \quad (6.43)$$

Since $x^a z^c \equiv -1 mod\ q$ we can't write a congruence sequence for this but we can use a longer stepwise method to solve this. If $x^a \equiv x^{2N} mod\ q$ then $x^a \equiv z^{2N} mod\ q$ hence $x^{2N} \equiv z^{2N} mod\ q$.

Therefore, we have one of 3 results $x^{2c} \equiv z^{2c} mod\ q \equiv x^a mod\ q$ or $x^{4c} \equiv z^{4c} mod\ q \equiv -z^c mod\ q \equiv x^{2a} mod\ q$ or $x^{6c} \equiv x^{3a} mod\ q$. Hence, we get $2Nc - a = M3a$ or $4Nc - 2a = M3a$ or $6Nc = M3a$ respectively.

$\therefore c$ and a must share common factors or $N = Ma$, (M stands for 'multiple of') which leaves $x^a \equiv \mp z^{2a}, \mp z^{4a} ... mod\ q.$ (6.44)

Repeating $\rightarrow 2N'a - c = M3c$ and hence $N' = Mc$, but z^{2ac} is outside our range.

The only way to avoid this is if a,c share common factors. (6.45)

If $2Nc - a = M3$ only then we will reduce to $x^3 \equiv \pm 1 mod\ q$ which is a contradiction or $a,c = M3$.

Likewise, $2Na - c = M3c$ etc. or $z^c \equiv \pm x^{2c}, \pm x^{4c} ... mod\ q$, $2N''c - a = M3a$ but x^{2ac} is outside our range. (6.46)

(Remark 1: To put it another way we know that along the x sequence that $x^a \equiv \pm x^{4a} mod\ q$ and along the z sequence $x^a \equiv z^{2c} mod\ q$ then $x^{4a} z^{2c} \equiv (xz)^{2N} mod\ q$ and with $x^a z^c \equiv -1 mod\ q$ then $x^{4a-2N} \equiv x^a mod\ q$, $z^{2c-2N} \equiv z^c \therefore 2N = 3a$ and $2N = c$, $N = 3ac$, $2N = 6ac$ which is outside our range unless a,c share common factors) (6.47)

(Remark 2: One may wonder what if $2Nc - a = q - 1$ where $q - 1 \neq M(a,c)$ which is possible if R is a power of small primes but then $2Nc - a = 2Na - c \rightarrow (c - a)(2N + 1) = 0$ hence, $c = a$). (6.48)

If a,c are not co-prime then we can repeat but with the non common factor or co-prime exponents a',c'

$$x^{a'} \equiv \pm (z)^2, \pm (z)^4, ... \pm (z)^{6c-2} mod\ q \quad (6.39)$$

$$z^{c'} \equiv \mp (x)^2, \mp (x)^4 ... \mp (x)^{6a-2} mod\ q \quad (6.50)$$

$$x^{a'} \equiv \pm (x)^2, \pm (x)^4 ... \pm (x)^{6a-2} mod\ q \quad (6.51)$$

$$z^{c'} \equiv \mp (z)^2, \mp (z)^4, .. \mp (z)^{6c-2} mod\ q \quad (6.52)$$

$$x^{2a'} \equiv (xz)^2, (xz)^4 ... (xz)^{6ac-2} mod\ q \quad (6.53)$$

$$z^{2c'} \equiv (xz)^2, (xz)^4 ... (xz)^{6ac-2} mod\ q \quad (6.54)$$

$$x^{a'} z^{c'} \equiv -(xz)^2, -(xz)^2 ... -(xz)^{6ac-2} mod\ q \quad (6.55)$$

where if $x^{a'} z^{c'} \neq -1 mod\ q \therefore x^{a'} \equiv -z^{c'}$ and we get our $3 \equiv 0 mod\ q$ contradictions. (6.56)

If $x^{a'} z^{c'} \equiv -1 mod\ q$ then we need y congruence sequences. If $y^3 \neq \pm 1 mod\ q$ write;

$$x^3 \equiv \pm (x)^2, \pm (x)^4 ... \pm (x)^{6a-2} mod\ q \quad (6.57)$$

$$y^3 \equiv \pm (y)^2, \pm (y)^4 ... \pm (y)^{2b-2} mod\ q \quad (6.58)$$

$$x^6 \equiv (xy)^2, (xy)^4 ... (xy)^{6ab-2} mod\ q \quad (6.59)$$

$$y^6 \equiv (xy)^2, (xy)^4 ... (xy)^{6ab-2} mod\ q \quad (6.60)$$

$$x^3 y^3 \equiv (xy)^2, (xy)^4 ... (xy)^{6ab-2} mod\ q \quad (6.61)$$

We are missing 2 sequences as we can't write x^3, y^3 in terms of y,x respectively.

However, if $x^3 y^3 \neq 1 mod\ q$ then we have that $x^3 \equiv x^2, x^4 ... mod\ q$ must have the same exponents as $y^3 \equiv y^2, y^4 ... mod\ q$ but we have $x^3 \equiv x^6, x^{12} ... x^{6a-6} mod\ q$ so then $y^3 \equiv y^6, y^{12} ... y^{2b-2} mod\ q$ hence $b = M3$ otherwise $y = \pm 1 mod\ q$ which we have assumed $\neq \pm 1$. If $x^3 y^3 \equiv 1 mod\ q$ then use the z^3, y^3 congruence sequences to show that $b = M3$ and if $z^3 y^3 \equiv -1 mod\ q$ also then see below.* If $b = M3$ then we can now write; (6.62)

$$x^a \equiv \pm y^2, \pm y^4 ... \pm y^{2b-2} mod\ q \quad (6.63)$$

$$z^c \equiv \mp y^2, \mp y^4 ... \mp y^{2b-2} mod\ q \quad (6.64)$$

$$x^{2a} \equiv (xy)^2, (xy)^4 ... (xy)^{6ab-2} mod\ q \quad (6.65)$$

$$z^{2c} \equiv (xy)^2, (xy)^4 ... (xy)^{6ab-2} mod\ q \quad (6.66)$$

and with, $$x^a \equiv \pm (x)^2, \pm (x)^4 ... \pm (x)^{6a-2} mod\ q \quad (6.67)$$

$$z^c \equiv \mp (x)^2, \mp (x)^4 ... \mp (x)^{6a-2} mod\ q \quad (6.68)$$

gives us our common factor exponent method as before i.e.

If $x^a \equiv x^{2N} \; mod\; q$ then $x^a \equiv y^{2N} \; mod\; q$ hence $x^{2N} \equiv y^{2N} \; mod\; q$. Therefore, we have $x^{2b} \equiv 1 mod\; q$, $x^{4b} \equiv 1 mod\; q$, $x^{6b} \equiv 1 mod\; q$...etc. Hence, $2Nb \equiv M3a$ therefore, b and a must share common factors or $N = Ma$ which leaves $x^a \equiv \mp y^{2a}, \mp y^{4a} ... mod\; q \rightarrow y^{2ba} \equiv 1 mod\; q$ but this is not in the range so b and a must share common factors. (6.69)

Likewise $2Nc \equiv M3b$ and c and b must share common factors. (6.70)

Therefore, if all a,b,c share the same common factor, say p, we have the special case with $t' = x^{a'} + y^{b'} - z^{c'}$ and $x^{a'p} + y^{b'p} - z^{c'p} = 0$ where $t' \rightarrow \infty$ and has no solutions or common factor solutions in x,y,z. (6.71)

If a,b,c don't all share the same common factor then we can write the congruence sequences for $x^{a''}$ and $y^{b'}$ or $z^{c''}$ and $y^{b''}$ where a'', b' and c'', b'' are the co-prime factors respectively. But this just gives our contradictions or $x^{a''} y^{b'} \equiv 1 mod\; q$ and $y^{b''} z^{c''} \equiv -1 mod\; q$ so raising these to the common factors gives $x^a y^b \equiv -y^b z^c \; mod\; q$ and we get our $3 \equiv 0 \; mod\; q$ contradictions. (6.72)

*If $y^3 \equiv \pm 1 mod\; q$ or if $x^3 y^3 \equiv 1 mod\; q$ and $z^3 y^3 \equiv -1 mod\; q$ write;

$$x^3 \equiv \pm (z)^2, \pm (z)^4 ... \pm (z)^{6a-2} \; mod\; q \quad (6.73)$$

$$z^3 \equiv \mp (x)^2, \mp (x)^4 ... \mp (x)^{6a-2} \; mod\; q \quad (6.74)$$

$$x^3 \equiv \pm (x)^2, \pm (x)^4 ... \pm (x)^{6a-2} \; mod\; q \quad (6.75)$$

$$z^3 \equiv \mp (z)^2, \mp (z)^4 ... \mp (z)^{6a-2} \; mod\; q \quad (6.76)$$

$$x^6 \equiv (xz)^2, (xz)^4 ... (xz)^{2a-2} \; mod\; q \quad (6.77)$$

$$z^6 \equiv (xz)^2, (xz)^4 ... (xz)^{2a-2} \; mod\; q \quad (6.78)$$

$$x^3 z^3 \equiv -(xz)^2, -(xz)^2 ... -(xz)^{2a-2} \; mod\; q \quad (6.79)$$

Firstly, if $x^3 z^3 \neq -1 mod\; q$ we get $x^3 \equiv -z^3 \; mod\; q$. We then repeat above with x^3 and z^c congruence sequences and since $x^3 z^c \neq 1 mod\; q$ unless $a = 3$ then $x^3 \equiv -z^c \; mod\; q$, likewise $z^3 \equiv -x^a \; mod\; q$ unless $c = 3$. Therefore, $x^a \equiv -z^a \; mod\; q \rightarrow 2x^a \equiv \pm 1 mod\; q$ contradiction.

If $a = c = 3$ then $x^3 z^3 \equiv -1 mod\; q$. So we have $(y^6 + x^3 z^3) \equiv 0 \; mod\; q$ with $y^3 \equiv \pm 1$modq but $(y^{2b} + x^a z^c) \equiv 0 \; mod\; q$ which is not factorizable into $y^6 + x^3 z^3$ unless $a,b,c = M3$ but then we will have the special case with $p = 3$. $\therefore x^3 z^3 \equiv -1 mod\; q$ which now excludes the $y^3 \equiv \pm 1 mod\; q$ case as above. Furthermore, when we have with $x^3 y^3 \equiv 1 mod\; q$ and $z^3 y^3 \equiv -1 mod\; q$ also then $z^3 \equiv -y^3 \; mod\; q$, $z^3 \equiv -x^3 \; mod\; q$, $x^3 \equiv y^3 \; mod\; q$ and one can see we again get common factor exponents if we raise them to a,b,c i.e $z^{3c} \equiv -y^{3c} \; mod\; q \equiv 1 mod\; q$, $3c - b = Mb \therefore c = Mb$ otherwise $y \equiv \pm 1 moq$ (b is odd) but $y^3 \neq 1$modq likewise $3a - b = Mb$ so a,b,c share common factors and we get the special case. (6.82)

Conclusion we can only have common factor solutions in the exponents for when $x^3 \neq \pm 1 mod\; q$ and $z^3 \neq \mp 1 mod\; q$ with a,b,c odd, which leads to the special case.

Next, lets assume $x^3 \equiv \pm 1 mod\; q$, $z^3 \neq \mp 1 mod\; q$ we know $x \neq \pm 1 mod\; q$ then if we repeat above we can see our **first exception** $\rightarrow a = 1$.

$$x^a \equiv \pm (z)^2, \pm (z)^4 ... \pm (z)^{6c-2} \; mod\; q \quad (6.83)$$

$$z^c \equiv \mp (z)^2, \mp (z)^4 ... \mp (z)^{6c-2} \; mod\; q \quad (6.84)$$

$$x^a \equiv \pm x^2, \pm x^4 \; mod\; q \quad (6.85)$$

$$z^c \equiv \mp x^2, \mp x^4 \; mod\; q \quad (6.86)$$

$$x^{2a} \equiv (xz)^2, (xz)^4 ... (xz)^{6c-2} \; mod\; q \quad (6.87)$$

$$z^{2c} \equiv (xz)^2, (xz)^4 ... (xz)^{6c-2} \; mod\; q \quad (6.88)$$

But $x^a z^c \equiv 1 mod\; q$ so we can't write a congruence sequence for this. Although we have only 2 choices for x^a, z^c in terms of the x sequence we don't necessarily have the same exponents because $x^{N6} \equiv 1 mod\; q$. So we have $x^2 \equiv z^{2N} \; mod\; q$ or $x^4 \equiv z^{4N} \; mod\; q$. $\therefore$ we get $x^{2c} \equiv z^{2Nc} \; mod\; q \equiv x^a \; mod\; q$ or $x^{4c} \equiv z^{4Nc} \; mod\; q \equiv x^{2a} \; mod\; q$ like before. Hence we get $2c - a \equiv M3a$ or $4c - 2a \equiv M3a$ Therefore c and a must share common factors unless $a = 1$ where we get $2c - 1 = M3$, $x^{M3} \equiv \pm 1 mod\; q$ which it is. (6.89)

But we also have $x^{2a} \equiv z^{2Na} \; mod\; q \rightarrow -z^c \equiv z^{2Na} \; mod\; q$ so $2Na - c = M3c$ is possible too with $a = 1$ and $N = Mc$ and because with $a = 1$ then $2ac$ does not fall outside our range. However, when $a \geq 3$ we get $2ac$ falling outside the range, hence we need common factor exponents to avoid this. (6.90)

Therefore, $a = 1$ is our **first exception.** We can carry on as before but with a smaller x congruence range to show shared common factor exponents in a,b,c and we get the special case with $t' \rightarrow \infty$ giving no solutions or common factor solutions in x,y,z. (6.91)

Similarly with $z^3 \equiv \mp 1 \, mod\, q$ and $x^3 \neq \pm 1 \, mod\, q$ with the **first exception** $c = 1$. (6.92)

If $x^3 \equiv \pm 1 \, mod\, q$ and $z^3 \equiv \mp 1 \, mod\, q$ we get an even smaller range with the exceptions $a, c = 1$. (6.93)

Next we need to demonstrate our methods work with even exponents and to get our second exception with $a, c = 2$ so we choose a = even, c = odd, b = odd. We have the same form of the solutions for any of a, b, c even/odd and in this case we continue with $x^{3a} \equiv \pm 1 \, mod\, q$, $z^{3c} \equiv \mp 1 \, mod\, q$, $y^b \equiv \pm 1 \, mod\, q$.

It's best to write $x^a \equiv \mp u_1 z^2 \, mod\, q$ for even a, hence $u_1^{3c} \equiv \pm 1 \, mod\, q$ and $u_1 \equiv u_2 z^2 \, mod\, q$ where $u_2^{3c} \equiv \pm 1 \, mod\, q$ etc.

Therefore there must be a $(\pm 1) \, mod\, q$ in our congruence range. As before assume $x^3 \neq \pm 1 \, mod\, q$, $z^3 \neq \mp 1 \, mod\, q$.

$$x^a \equiv \mp z, \mp z^3, \mp z^5 \ldots \mp z^{6c-1} \, mod\, q \tag{6.94}$$

$$z^c \equiv \pm x, \pm x^3, \pm x^5 \ldots \pm x^{3a-1} \, mod\, q \tag{6.95}$$

$$x^a \equiv \pm x, \pm x^3, \pm x^5 \ldots \pm x^{3a-1} \, mod\, q \tag{6.96}$$

$$z^c \equiv \mp z, \mp z^3, \mp z^5 \ldots \mp z^{6c-1} \, mod\, q \tag{6.97}$$

$$x^{2a} \equiv \pm (xz), \pm (xz)^3, (xz) \ldots \pm (xz)^{3ac-1} \, mod\, q \tag{6.98}$$

$$z^{2c} \equiv \pm (xz), \pm (xz)^3 \ldots \pm (xz)^{3ac-1} \, mod\, q \tag{6.99}$$

Therefore, we have $x^{(2N-1)} \equiv z^{(2N-1)} \, mod\, q$ thus $x^c \equiv z^c \equiv -x^{2a} \, mod\, q$ or $x^{3c} \equiv z^{3c} \, mod\, q$ or $x^{5c} \equiv z^{5c} \equiv \mp z^{2c} \equiv \pm x^{2a}$ ...etc. so $(2N-1)c - 2a = 3a$, $(2N-1)c - 3a = 3a$, $(2N-1)c - a = 3a$ respectively but $2N-1$ is odd, hence c is even also.

Likewise, $x^a \equiv z^a \equiv z^{2c} \, mod\, q$, $x^{3a} \equiv z^{3a} \, mod\, q$, $x^{5a} \equiv z^{5a} \equiv -z^c \, mod\, q \rightarrow (2N-1)a - 2c = 3c$ etc.

Hence we can now write,

$$x^a \equiv \pm (x)^2, \pm (x)^4 \ldots \pm (x)^{6a'-2} \, mod\, q \quad \text{where } a' = a/2 \tag{6.100}$$

$$z^c \equiv \mp (x)^2, \mp (x)^4 \ldots \mp (x)^{6a'-2} \, mod\, q \tag{6.101}$$

$$x^a \equiv \pm (z)^2, \pm (z)^4, \ldots \pm (z)^{6c'-2} \, mod\, q \quad \text{where } c' = c/2 \tag{6.102}$$

$$z^c \equiv \mp (z)^2, \mp (z)^4, \ldots \mp (z)^{6c'-2} \, mod\, q \tag{6.103}$$

$$x^{2a} \equiv (xz)^2, (xz)^4 \ldots (xz)^{6ac-2} \, mod\, q \tag{6.104}$$

$$z^{2c} \equiv (xz)^2, (xz)^4 \ldots (xz)^{6ac-2} \, mod\, q \tag{6.105}$$

Therefore we have a smaller range and with $2Nc - a = 3a$ so if $N = Ma'$ then $x^a \equiv \mp z^{2a'}, \mp z^{4a'} \ldots mod\, q \rightarrow 2Na' - c = M3c$ and $N' = Mc'$ but $z^{2a'c'}$ is outside our range unless $a' = 1$ then we have $a = 2$ or $a' = 2$ then $a = 4$ and so must $c = M4$. Similarly $c' = 1, 2 \rightarrow c = 2, 4$. These are the first cases of our **second exceptions**. (6.106)

Now, we can extend this to powers of 2 where we put x^a, z^c in terms of smaller ranges until we have odd term common factors or we could show $b = M4$ also as below $\triangle$ to get an equation to the power of 4 which has no solutions by Fermat.

If a, c are not co-prime but share odd common factors then we can repeat but with the non common factor exponent a', c'.

$$x^{a'} \equiv -z, -z^3, \ldots -z^{6c-1} \, mod\, q \tag{6.107}$$

$$z^{c'} \equiv \pm x, \pm x^3, \pm x^5 \ldots \pm x^{3a-1} \, mod\, q \tag{6.108}$$

$$x^{a'} \equiv \pm x, \pm x^3, \pm x^5 \ldots \pm x^{3a-1} \, mod\, q \tag{6.109}$$

$$z^{c'} \equiv \mp z, \mp z^3, \mp z^5 \ldots \mp z^{6c-1} \, mod\, q \tag{6.110}$$

$$x^{2a'} \equiv \pm (xz), \pm (xz)^3 \ldots \pm (xz)^{3ac-1} \, mod\, q \tag{6.111}$$

$$z^{2c'} \equiv \pm (xz), \pm (xz)^3 \ldots \pm (xz)^{3ac-1} \, mod\, q \tag{6.112}$$

$$x^{a'} z^{c'} \equiv \pm xz, \pm xz^3 \ldots \pm xz^{6ac-1} \, mod\, q \tag{6.113}$$

where if $x^{a'} z^{c'} \neq -1 \, mod\, q \therefore x^{a'} \equiv -z^{c'}$ and we get our $3 \equiv 0 \, mod\, q$ contradiction.

If $x^{a'} z^{c'} \equiv -1 \, mod\, q$ then we need y congruence sequences as before. If $y^3 \neq \pm 1 \, mod\, q$ write;

$$x^3 \equiv \pm (x)^2, \pm (x)^4 \ldots \pm (x)^{6a-2} \, mod\, q \tag{6.114}$$

$$y^3 \equiv \pm (y)^2, \pm (y)^4 \ldots \pm (y)^{2b-2} \, mod\, q \tag{6.115}$$

$$x^6 \equiv (xy)^2, (xy)^4 \ldots (xy)^{6ab-2} \, mod\, q \tag{6.116}$$

$$y^6 \equiv (xy)^2, (xy)^4 \ldots (xy)^{6ab-2} \, mod\, q \tag{6.117}$$

$$x^3 y^3 \equiv (xy)^2, (xy)^4 \ldots (xy)^{6ab-2} \, mod\, q \tag{6.118}$$

We are missing 2 sequences as we can't write x^3, y^3 in terms of y, x respectively.

How ever, if $x^3y^3 \neq 1 mod\ q$ then we have $x^3 \equiv x^2, x^4 ... mod\ q$ must have the same exponents as $y^3 \equiv y^2, y^4 ... mod\ q$ but $x^3 \equiv x^6, x^{12} ... x^{6a-6}\ mod\ q$ so then $y^3 \equiv y^6, y^{12} ... y^{2b-2}\ mod\ q$ hence $b = M3$ otherwise $y = \pm 1 mod\ q$ which we have assume d $\neq \pm 1$. (6.119)

If $x^3y^3 \equiv 1 mod\ q$ then use the z^3, y^3 congruence sequences and if $z^3y^3 \equiv -1 mod\ q$ also then see below.◊

If $b = M3$ then we can now write;

$$x^a \equiv y, y^3 ... y^{2b-1}\ mod\ q \quad (6.120)$$

$$z^c \equiv -y, -y^3 ... - y^{2b-1}\ mod\ q \quad (6.121)$$

$$x^{2a} \equiv \pm(xy), \pm(xy)^3 ... \pm(xy)^{6ab-1}\ mod\ q \quad (6.122)$$

$$z^{2c} \equiv \mp(xy), \mp(xy)^3 ... \mp(xy)^{6ab-1}\ mod\ q \quad (6.123)$$

and with

$$x^a \equiv \pm x, \pm x^3, \pm x^5 ... \pm x^{3a-1}\ mod\ q \quad (6.124)$$

$$z^c \equiv \pm x, \pm x^3, \pm x^5 ... \pm x^{3a-1}\ mod\ q \quad (6.125)$$

If $x^a \equiv x^{2N-1}\ mod\ q$ then $x^a \equiv y^{2N-1}\ mod\ q$ hence $x^{2N-1} \equiv y^{2N-1}\ mod\ q$. Therefore, we get $x^{2b} \equiv 1 mod\ q$, $x^{4b} \equiv 1 mod\ q$, $x^{6b} \equiv 1 mod\ q$...etc. Hence $(2N-1)b = M3a$, $\therefore b$ must be even or $M4^{\Delta}$ if $a = M4$ *etc*. Therefore we can now write;

$$x^a \equiv \pm y^2, \pm y^4 ... \pm y^{2b'-2}\ mod\ q \quad \text{where } b' = b/2 \quad (6.126)$$

$$z^c \equiv \mp y^2, \mp y^4 ... \mp y^{2b'-2}\ mod\ q \quad (6.127)$$

$$x^a \equiv \pm(x)^2, \pm(x)^4 ... \pm(x)^{6a'-2}\ mod\ q \quad \text{where } a' = a/2 \quad (6.128)$$

$$z^c \equiv \mp(x)^2, \mp(x)^4 ... \mp(x)^{6a'-2}\ mod\ q \quad (6.129)$$

$$x^{2a} \equiv (xy)^2, (xy)^4 ... (xy)^{6ab-2}\ mod\ q \quad (6.130)$$

$$z^{2c} \equiv (xy)^2, (xy)^4 ... (xy)^{6ab-2}\ mod\ q \quad (6.131)$$

Which gives a smaller range and with $2Nb - a = 3a$ so if $N = Ma'$ we have $x^a \equiv \pm y^{2a'}, \pm y^{4a'} ... mod\ q \rightarrow 2N'a' - b = Mb$ and $N' = Mb'$ but $z^{2a'b'}$ is outside our range unless $a' = 1$ then we have $a = 2$ or $a' = 2$ then $a = 4$ and so must $b = M4$. (6.132)

Similarly $b' = 1, 2, b = 2, 4$. If $a, b, c = M4$ then we have a power of 4 equation which has no solutions by Fermat otherwise a, b share common factors. Similarly, b, c share common factors. (6.133)

Therefore, if all a, b, c share the same common factor, say p, we have the special case with $t' = x^{a'} + y^{b'} - z^{c'}$ and $x^{a'p} + y^{b'p} - z^{c'p} = 0$ where $t' \rightarrow \infty$ and has no solutions. (6.134)

If a, b, c don't all share the same common factor then we can write the congruence sequences for $x^{a''}$ and $y^{b'}$ or $z^{c''}$ and $y^{b''}$ but this just gives our contradiction or $x^{a''}y^{b'} \equiv 1 mod\ q$ and $y^{b''}z^{c''} \equiv -1 mod\ q$ so raising these to the common factors gives $x^a y^b \equiv -y^b z^c\ mod\ q$ and we get our $3 \equiv 0\ mod\ q$ contradictions. (6.135)

◊If $y^3 \equiv \pm 1 mod\ q$ or if $x^3y^3 \equiv 1 mod\ q$ and $z^3y^3 \equiv -1 mod\ q$ write;

$$x^3 \equiv \pm(z)^2, \pm(z)^4, ... \pm(z)^{6a-2}\ mod\ q \quad (6.136)$$

$$z^3 \equiv \mp(x)^2, \mp(x)^4 ... \mp(x)^{6a-2}\ mod\ q \quad (6.137)$$

$$x^3 \equiv \pm(x)^2, \pm(x)^4 ... \pm(x)^{6a-2}\ mod\ q \quad (6.138)$$

$$z^3 \equiv \mp(z)^2, \mp(z)^4, ... \mp(z)^{6a-2}\ mod\ q \quad (6.139)$$

$$x^6 \equiv (xz)^2, (xz)^4 ... (xz)^{2a-2}\ mod\ q \quad (6.140)$$

$$z^6 \equiv (xz)^2, (xz)^4 ... (xz)^{2a-2}\ mod\ q \quad (6.141)$$

$$x^3z^3 \equiv -(xz)^2, -(xz)^2 ... -(xz)^{2a-2}\ mod\ q \quad (6.142)$$

If $x^3z^3 \neq -1 mod\ q$ we get $x^3 \equiv -z^3\ mod\ q$. We then repeat above with x^3 and z^c congruence and because $x^3z^c \neq 1 mod\ q$ unless $a = 3$ which it doesn't. We get $x^3 \equiv -z^c\ mod\ q$, likewise $z^3 \equiv -x^a\ mod\ q$ unless $c = 3$. Therefore, $x^a \equiv -z^a\ mod\ q \rightarrow 2x^a \equiv \pm 1 mod\ q$ contradiction. (6.143)

If $x^3z^3 \equiv -1\ mod\ q$ we have $y^6 + x^3z^3 \equiv 0 mod\ q$ but $y^{2b} + x^a z^c \equiv 0 mod\ q$ which is not factorizable into $y^6 + x^3z^3$ unless $a, b, c = M3$ but then we will have the special case with $p = 3$. $\therefore x^3z^3 \equiv -1 mod\ q$ and $y^3 \neq \pm 1 mod\ q$. (6.144)

Furthermore, we have with $x^3y^3 \equiv 1 mod\ q$ and $z^3y^3 \equiv -1 mod\ q$ also then $z^3 \equiv -y^3\ mod\ q$, $z^3 \equiv -x^3\ mod\ q$, $x^3 \equiv y^3\ mod\ q$ and one can see we again get common factor exponents if we raise them to a, b, c i.e $z^{3c} \equiv -y^{3c}\ mod\ q \equiv 1 mod\ q$, $3c - b = Mb$

Therefore, a, b, c share common factors and we have the special case. (6.145)

Next, lets assume $x^3 \equiv \pm 1 mod\ q$, $z^3 \neq \mp 1 mod\ q$, we know $x \neq \pm 1 mod\ q$ then if we repeat above we can see our second case of the **second exception**,

$$x^a \equiv \pm(z)^2, \pm(z)^4, ... \pm(z)^{6c-2}\ mod\ q \tag{6.146}$$

$$z^c \equiv \mp(z)^2, \mp(z)^4, ... \mp(z)^{6c-2}\ mod\ q \tag{6.147}$$

$$x^a \equiv \pm x^2, \pm x^4\ mod\ q \tag{6.148}$$

$$z^c \equiv \mp x^2, \mp x^4\ mod\ q \tag{6.149}$$

$$x^{2a} \equiv (xz)^2, (xz)^4 ... (xz)^{6c-2}\ mod\ q \tag{6.150}$$

$$z^{2c} \equiv (xz)^2, (xz)^4 ... (xz)^{6c-2}\ mod\ q \tag{6.151}$$

but $x^a z^c \equiv 1 mod\ q$ so we can't write a congruence sequence for this. Although we have only 2 choices for x^a, z^c in terms of x we don't necessarily have the same exponents because $x^{N6} \equiv 1 mod\ q$. So we have $x^2 \equiv z^{2N}\ mod\ q$ or $x^4 \equiv z^{4N}\ mod\ q$

Therefore we get $x^{2c} \equiv z^{2Nc} \equiv x^a\ mod\ q$ or $x^{4c} \equiv z^{4Nc} \equiv x^{2a}\ mod\ q$ like before. Hence we get $2c - a \equiv M3a$ or $4c - 2a \equiv M3a$

Therefore, c and a must share common factors unless $a = 2$ where we get $2c - 2 = M6$, $c - 1 = M3$, $x^{M3} \equiv \pm 1 mod\ q$, which it is. (6.152)

But we have $x^{2a} \equiv z^{2Na}\ mod\ q \rightarrow -z^c \equiv z^{2Na}\ mod\ q$ so $2Na - c = M3c$ is possible with $a = 2$ and $N = Mc$ and because with $a = 2$ then $2ac$ does not fall outside our range. However, when $a \geq 3$ we get $2ac$ falling outside the range, hence we need common factor exponents to avoid this. (6.153)

Therefore, $a = 2$ is our **second exception.** We can carry on as before but with a smaller x congruence range to show shared common factor exponents in a,b,c and hence we get the special case with $t' \rightarrow \infty$ giving no solutions. (6.154)

Similarly with $z^3 \equiv \mp 1 mod\ q$ and $x^3 \neq \pm 1 mod\ q$ with the **exception** c **= 2.** (6.155)

If $x^3 \equiv \pm 1 mod\ q$ and $z^3 \equiv \mp 1 mod\ q$ we get an even smaller range with the **exceptions** a,c **= 2.** (6.156)

Thus this method works for even exponents in a,c If b were even then it makes no difference giving b=2 exception or we could choose another n_1, n_2, n_3 symmetry.

Conclusion

One can see that the form of the solutions* $x^{3a} \equiv \pm 1 mod\ q$, $z^{3c} \equiv \mp 1 mod\ q, y^b \equiv \pm 1 mod\ q$ puts a constraint on the exponents with one or more of $a,b,c = 1$ or 2 falling within the constraint, otherwise the exponents themselves have common factor solutions which leads to the special case which has common factor solutions in x,y,z or $t' \rightarrow \infty$.

Therefore, there are only common factor solutions to $x^a + y^b - z^c$ for $a,b,c > 2$. * Excluding phase number.

Continuous Representation

The transformation or $t,r,(xyz)$ represention equation is valid for all $x,y,z \in \Re$.

We write the $t,r,(xyz)$ representation for real number exponents as a continuous summation or infinite series, so for the t independent equation we get with $V = -1$;

$$x^n + y^n + z^n \equiv \Big(\sum_{m=0(even)}^{n} n \frac{(\frac{n-(m+2)}{2})!}{0!\,m!(\frac{n-3m}{2})!}(xyz)^m (r)^{\frac{n-3(m)}{2}} + \sum_{n+m(m=0\ even)}^{\infty} n \frac{(\frac{n-(m+2)}{2})!}{0!\,\Gamma(m+n+1)(\frac{n-3m}{2})!}(xyz)^{m+n}(r)^{\frac{n-3(m+n)}{2}} \Big) \bmod t \tag{7.01}$$

$$x^n + y^n - z^n \equiv \Big(- \sum_{m=1(odd)}^{n} n \frac{(\frac{n-(m+2)}{2})!}{0!\,m!(\frac{n-3m}{2})!}(xyz)^m (r)^{\frac{n-3(m)}{2}} - \sum_{n+m(m=1\ odd)}^{\infty} n \frac{(\frac{n-(m+2)}{2})!}{0!\,\Gamma(m+n+1)(\frac{n-3m}{2})!}(xyz)^{m+n}(r)^{\frac{n-3(m+n)}{2}} \Big) \bmod t \tag{7.02}$$

where $\frac{(\frac{n-(m+2)}{2})!}{(\frac{n-3m}{2})!}$ is written not as a factorial in the second summation but as a finite numerator that we did originally.

We use the gamma function Γ instead of a factorial because we are dealing with real numbers.

This is a convergent series where both $\lim_{m\to\infty} \frac{(xyz)^{m+n}}{(r)^{\frac{n-3(m+n)}{2}}} = 0$ and $\lim_{m\to\infty} n \frac{(\frac{n-(m+2)}{2})(\frac{n-(m+4)}{2}\ldots\frac{n-3m-2}{2})}{0!\,\Gamma(m+n+1)} = 0$

in the second summation.

The negative t independent equation,

$$(xz)^n + (yz)^n \pm (xy)^n$$
$$\equiv \Big(\sum_{m=0}^{n} (-1)^m n \frac{(n-(2m+1))!}{0!\,m!(n-3m)!} r^{(n-3m)} (xyz)^{2m} + \sum_{n+m=0}^{\infty} n \frac{(n-(2m+1))!}{0!\,\Gamma(m+n+1)(n-3m)!}(xyz)^{2(m+n)} r^{(n-3(m+n))} \Big) \bmod t \tag{7.03}$$

This also converges in the second summation.

The general form;

$$x^n + y^n \pm z^n = \sum_{\ell=0}^{n} \sum_{s=0}^{n} \sum_{\substack{m=1\ odd(\#) \\ m=0\ even(*)}}^{n} (-1)^n (-1)^{\ell} n \frac{(\frac{n+(\ell-2s-m-2)}{2})!}{(\ell-2s)!\,m!\,s!(\frac{n-3m-\ell}{2})!} t^{\ell} (xyz)^m r^{\frac{n-3m-\ell}{2}}$$

$$+ \sum_{\ell=0}^{\infty} \sum_{s=0}^{\infty} \sum_{\substack{m+n(m=1\ odd(\#)) \\ m+n(m=0\ even(*))}}^{\infty} n \frac{(\frac{n+(\ell-2s-m-2)}{2})!}{\Gamma(\ell-2s)\Gamma(m+n+1)\Gamma s(\frac{n-3m-\ell}{2})!} t^{\ell} (xyz)^{m+n} r^{\frac{n-3(m+n)-\ell}{2}} \tag{7.04}$$

$* = odd, \ell = odd, n = even, \ell = even$

$\# n = odd, \ell = even, n = even\ \ell = odd$

where we write the factorial as a finite numerator.

References

[1]Gullberg. MATHMATICS, From the birth of numbers. First edition (1997)**. P 289-294**

[2] Wikipedia. Lucas sequence. Congruence relations, http://en.wikipedia.org/wiki/Lucas_number

Email: chrissloane70@gmail.com