

1. A PROOF OF COLLATZ'S CONJECTURE

Ramaswamy Krishnan, Electrical Engineer (rettd.) Meenakshi Ganesh, c-11, RBI Staff Quarters, Kamarajar Salai, K.K, Nagar, Chennai-600078, Tamil Nadu, India.

Received: 30 March 2026; Revised: 15 May 2026; Accepted: 04 June 2026; Available Online: 15 August 2026.

Abstract

The proof of Collatz's Conjecture is divided into three parts. In the first part, it is proved for the set of numbers $\{1, 5, 21, 85, \dots\}$. In the second part, it is proved for odd numbers of the form $(4k+1)$. In the third part, it is shown how numbers of the form $(4k+3)$ iterate into the numbers of the form $(4k+1)$. Thus, the conjecture is proved for all odd 'n'. As even numbers iterate into odd numbers, the conjecture is proved for all positive integers.

Keywords: Proof, Collatz, Conjecture.

Introduction

Consider the following equation for a positive integer 'n':

$$f(n, 1) = \frac{n}{2} \text{ if } n \text{ is even \& } = (3n + 1) \text{ if } n \text{ is odd.}$$

Let, $f(n, r) = f[f(n, r-1), 1]$ for, $r \geq 2$.

Now consider the set,

$$A(n) = \{f(n, 1), \dots, f(n, r), \dots\}$$

Consider an imaginary set.

$$B(n) = \{f(n, 1), \dots, f(n, r), \dots, 1, 4, 2, 1, 4, 2, 1, \dots\}$$

According to Collatz's Conjecture both the sets are identical. That is $A(n) = B(n)$.

Therefore, $A(n) = B(n)$ means Collatz's Conjecture is true for 'n'. It is obvious that, the conjecture has to be proved only for odd values of 'n', because, if 'n' is even, it will iterate in to an odd value and ultimately ending in the odd number '1'.

PART 1 : – An analysis of humbers 1, 5, 21, 85, etc

Consider the number, $n = [4^{r-1} + 4^{r-2} + \dots + 1]$

$$f(n, 1) = (4 - 1)[4^{r-1} + \dots + 1] + 1 = 4^r$$

Therefore, $f(n, 2r + 1) = 1$. Hence $A(n) = B(n)$.

Thus, a set $S_1 = \{1, 5, 21, 85, 341, \dots\}$ is generated.

$$S_1 = \{s_r : s_r = \frac{(4^r - 1)}{3}, r \geq 1\}$$

This set is the 'PRIMARY SET', because every oier number iterates in to a member of this set greater than '1' before iterating in to '1'.

PART 2 : –An Analysis Of. $n = (4k + 1)$

As only odd value is to be analysed it can be divided in to two parts, that is, $n = (4k + 1)$ & $n = (4k + 3)$. An analysis of, $n = (4k + 3)$, is dealt in Part 3. But Part 2 & Part 3 are interconnected.

Consider $n = (4k + 1)$,

$$f(n, 1) = f[(4k + 1), 1] \\ = 12k + 4$$

$$f(n, 3) = 3k + 1$$

If 'k' is odd, then $f(k, 1) = 3k + 1$.

Or if 'n' is an odd number & $A(n) = B(n)$

Then. $A(4n + 1) = B(4n + 1)$.

Obviously the converse is also true. That is, If 'n' is odd &

$A(4n + 1) = B(4n + 1)$ then, $A(n) = B(n)$.

This is an important result. It also derives the Primary

set, $S_1 = \{1, 1 \times 4 + 1, 5 \times 4 + 1, 21 \times 4 + 1, \dots\}$

$S_1 = \{1, 5, 21, 85, \dots\}$. Similarly

$S_3 = \{3, 13, 53, \dots\}$

$S_7 = \{7, 29, 117, \dots\}$ Or in general,

$S_{2n+1} = \{2n + 1, 8n + 5, 32n + 21, \dots\}$

These sets are important in the understanding of the problem. In these sets, except the first member. all the other members are, obviously, of the $4k + 1$ form.

Consider the following numbers iterations ; -

$3 \rightarrow 5 \rightarrow 1$; $9 \rightarrow 7 \rightarrow 11 \rightarrow 17 \rightarrow 13 \rightarrow 5 \rightarrow 1$.

Now, numbers greater than 9 will be considered.

$f[4k + 1, 1] = 12k + 4$; $f[4k + 1, 3] = 3k + 1$

Let $n = 4k + 1$ & $A(n) = B(n)$; $m \equiv 1 \pmod{3}$ & if,

$m \leq n$, $A(m) = B(m)$. Consider $M = 4[k + r] + 1$,

If $A[3(k + r) + 1] = B[3(k + r) + 1]$, $A(M) = B(M)$

Hence $3(k + r) + 1 \leq 4k + 1$; ie, $3k + 3r \leq 4k$.

Hence, if $3r \leq k$, then $A(M) = B(M)$.

On that basis, The following table has been prepared.

Table: 1

1	2	3	4	5
n	k	m	r	M
13	3	7, 10, 13	1	17 7 (part 3)
17	4	16	1	21
21	5	19	1	25 19 (part 3)
25	6	22, 25	1, 2	29
				33
29	7	28	1, 2	37
33	8	31	1, 2	41 31 (part 3)
37	9	34, 37	1, 2, 3	45
				49
41	10	40	1, 2, 3	53 (13 x 4 + 1)
45	11	43	1, 2, 3	57 43 (part 3)
49	12	46, 49	1, 2, 3, 4	61 23 (part 3)
				65
53	13	52	4	69
57	14	55	4	73 55 (part 3)
61	15	58, 61	4, 5	77

----- 81
65 16 64 5 85

It can be seen from the above table that by PMI,
it is clearly proved that if, $n = 4k + 1$ then,

$$A(n) = B(n).$$

This generates the set $K = \{k: k \in N\}$ & The set

$$C(2^2) = \{n: n = 2^2k + 1 \text{ \& } k \in N\}$$

Though, the set, K itself, PROVES COLLATZ'S

CONJECTURE, the proof is complete only with PART 3.

PART 3 : -An analysis of $n = 4k + 3$

$A(4k + 1) = B(4k + 1)$ has been proved. In this Part 3,

it will be proved, how $n = (4k + 3)$, iterates to $(4k + 1)$.

Let, $n = (4k + 3)$; k , can be odd or even. So,

let, $k = 2k_3$ or $2k_3 + 1$,

Therefor, $n_3 = (8k_3 + 3)$ or $n_{31} = (8k_3 + 7)$.

$$(3 - 3) n_3 = (8k_3 + 3)$$

$$f(n_3, 1) = f(2^3k_3 + 2^2 - 1, 1),$$

$$= 3 \cdot 2^3k_3 + (2^3 + 2^2) - 3 + 1$$

$$f(n_3, 2) = 3 \cdot 2^2k_3 + 2^2 + 2 - 1 = 4(3k_3 + 1) + 1$$

$$\text{Therefor, } A(n_3) = B(n_3).$$

Thus the following set is generatrd.

$$C(2^3) = \{3, 11, 19, \dots\} = \{n_3: n_3 = (2^3k + 3), k \in N\}$$

$n_{31} = 8k_3 + 7$ & k_3 can be odd or even. Therefor let,

$$n_4 = 2^4k_4 + 7, \text{ \& } n_{41} = 2^4k_4 + 15.$$

$$(3 - 4) n_4 = 2^4k_4 + 2^3 - 1$$

$$f(n_4, 1) = 3 \cdot 2^4k_4 + (2^4 + 2^3) - 3 + 1$$

$$f(n_4, 2) = 2^4(3k_4 + 1) + 3. \text{ [} 8k + 3 \text{ form]}$$

$$f(n_4, 4) = 2^2(3^2k_4 + 3 + 1) + 1$$

Therefor, $A(n_4) = B(n_4)$.

Thus the following set is genrrated

$$C(2^4) = \{7, 23, 39, \dots\} = \{n_4: n_4 = (2^4k + 7), k \in N\}$$

In, n_{41}, k_4 can be odd or even. Therefore let,

$$n_5 = 2^5k_5 + 15 \text{ \& } n_{51} = 2^5k_{51} + 31$$

$$(3 - 5) n_5 = 2^5k_5 + 2^4 - 1$$

$$f(n_5, 6) = 4(3^3k_5 + 3^2 + 3 + 1) + 1$$

$$\text{Let, } n_r = 2^r k_r + 2^{r-1} - 1 \text{ \& } n_{r1} = 2^r k_r + 2^r - 1$$

$$(3 - r) n_r = 2^r k_r + 2^{r-1} - 1$$

$$f(n_r, 2r - 4) = 4(3^{r-2}k_r + 3^{r-3} + 3^{r-4} + \dots + 1) + 1$$

Thus, the following set is generated.

$$C(2^r) = \{(2^{r-1} - 1), \dots, [(2^{r-1} - 1) + k2^r], \dots\}$$

$$C(2^r) = \{n_r : n_r = (2^r k + 2^{r-1} - 1), k \in N\}$$

PART 4 : - The Conclusion

All these sets put together constitutes the master
set $C(2)$,

$$C(2) = \{C(2^2)UC(2^3)U \dots UC(2^r) \dots : r \rightarrow \infty\}$$

The set, $C(2) = \{1, 3, 5, 7 \dots\}$

$$C(2) = \{n_2 : n_2 = (2k + 1). k \in N\}$$



And $A(n_2) = B(n_2)$.

The above set represents all odd numbers and as all even numbers iterate to an odd number, for all Positive integers,

$$A(n) = B(n)$$

Thus, COLLATZ'S CONJECTURE , is proved for all positive integers' n' .

— — — — — X — — — — —

2. A SHORT ESSAY ON OPPELMANN'S CONJECTURE AND ITS IMPACT ON GOLDBACH'S HYPOTHESIS

I am an amateur mathematician. While browsing the Internet, I came across the Conjecture of Oppermann with respect to Prime numbers. As per his conjecture "There is at least one Prime between $[n^2 - n, n^2]$ & There is at least one Prime between $[n^2, n^2 + n]$ "

I looked in to Wikipedia. As per Wikipedia, the Oppermann's Conjecture is more powerful than the Conjectures of Legendre, Brocard and Andrica. As per Legendre's conjecture there is at least one Prime in the interval $[n^2, (n+1)^2]$. As per Oppermann's Conjecture there are at least two Primes. As per Brocard's Conjecture, if p_n is the n th Prime & $p_{(n+1)}$ is the $(n+1)$ th Prime, there are at least four Primes in the interval $[p_n^2, p_{n+1}^2]$. This obviously is true even for twin Primes, if Opperman's Conjecture is true.

As per Andrica's Conjecture, $\sqrt{p_{n+1}} - \sqrt{p_n} < 1$.

Now let me restate Oppermann's conjecture in a different way. For every positive integer, $m > 1$, There is at least 1 Prime in the interval $[m^2, m^2 + m]$ And For every positive integer, $m \geq 1$ There is at least 1 Prime in the interval, $[m^2 + m, (m+1)^2]$. Please note $(m+1)^2 - (m+1) = (m^2 + m)$ & and as such both the statements are one and the same.

Let $p_n = m^2 + a$ & $p_{n+1} = (m+1)^2 - b$, and $a = 1$ & $b = 2$, if m is even and $a = 2$ & $b = 1$, if m is odd.

$$\begin{aligned} \sqrt{p_{n+1}} - \sqrt{p_n} &= [(m+1)^2 - b]^{\frac{1}{2}} - [m^2 + a]^{\frac{1}{2}} \\ &< [(m+1)^2]^{\frac{1}{2}} - [m^2]^{\frac{1}{2}} = 1. \end{aligned}$$

Therefore, Andrica's and Opperman's conjectures are one and the same.

I decided to find out the distribution of primes from $m = 1$ onwards, in both the intervals namely, the first interval $[m^2, m^2 + m]$ and the second interval $[m^2 + m, (m+1)^2]$. I went up to 100 and that seem to be more than sufficient to form a conclusion. Giving all the 100 is difficult and so I am shortening as follows.

A1 = (sum of Primes in the first interval from $m-4$ to m)/5

A2 = (sum of primes in the second interval from $m-4$ to m)/5

A = [sum of primes less than $(m+1)^2$]/ $2m$

m	A1	A2	A	$\sqrt{m}$	$l_e m$
5	1.00	1.00	1.00	2.24	1.61
10	2.20	1.60	1.45	3.16	2.30
15	2.60	2.20	1.77	3.87	2.71
20	2.60	3.60	2.10	4.47	3.00
25	3.60	3.80	2.42	5.00	3.22
30	4.00	3.60	2.65	5.48	3.40
35	4.80	4.00	2.90	5.92	3.56
40	5.20	4.80	3.16	6.32	3.69
45	5.20	5.80	3.42	6.71	3.81
50	6.60	5.40	3.68	7.07	3.91

55	6.80	6.40	3.95	7.42	4.00
60	7.20	7.80	4.24	7.75	4.09
65	8.20	6.60	4.48	8.06	4.17
70	9.00	7.20	4.74	8.37	4.25
75	8.60	7.80	4.97	8.66	4.32
80	8.40	9.60	5.23	8.94	4.38
85	9.00	9.40	5.46	9.22	4.44
90	8.60	11.20	5.71	9.49	4.50
95	10.00	10.80	5.95	9.75	4.55
100	11.80	10.20	6.21	10.00	4.61

It is obvious from the above table that as m increases, the number of Primes in each interval not only increases, but it also increases faster than $\sqrt{m}$. The average A also increases faster than $\sqrt{m}$. I googled for $m = 1000$. Number of Primes less than 1002001 is 78650. Number of Primes in the first Interval is 75 and second interval is 77. Therefore A for $m = 1000$ is, $[78650 \div 2000] = 39.325$, and $\sqrt{m} = 31.62$. Even A is increasing faster than $\sqrt{m}$. Now consider three parabolic equations: (1) $y = x^2$; (2) $y = x^2 + x$; (3) $y = (x + 1)^2$. Let the Straight lines $y = m$, where m is a positive integer Intersect these parabolas at $A(m)$, $B(m)$, & $C(m)$ reply. All the integers lie on these lines. $A(m) = (m, m^2)$; $B(m) = (m, m^2 + m)$; And $C(m) = [m, (m + 1)^2]$. Every Integer lie on the lines AB & BC . Hence all the Primes lie on the lines AB & BC . If, $X(m)$ and $Y(m)$ represent the number of Primes on lines AB & BC , there is nothing surprising that as $m \rightarrow \infty$, $X(m) \rightarrow \infty$ & $Y(m) \rightarrow \infty$. Both of them tend to infinity much faster than $\sqrt{m}$. In addition $\frac{\sum_1^m \{X(m) + Y(m)\}}{2m} \rightarrow \infty$ faster than $\sqrt{m}$, because, the Primes are also infinite. Thus, all these statements can be considered as GREAT UNDERSTATEMENTS.

Goldbach's Hypothesis

As per Goldbach's Hypothesis "every even number Greater than 4, can be expressed as a sum of two odd Primes". The hypothesis can be proved wrong by giving a counter example. It is possible to give a counter example, if and only if a prime, say the n th prime ' p_n ' exists, such that the $(n + 1)$ th prime $p_{(n+1)} > 2p_n$. Let the number of primes between p_n & $\{\sqrt{p_n} + 1\}^2$ be $U(n)$ and number of primes between p_n & $2p_n$ be $V(n)$. $[2p_n - p_n] \div [\{\sqrt{p_n} + 1\}^2 - p_n] = p_n \div [2\sqrt{p_n} + 1] \cong \frac{1}{2} \sqrt{p_n}$. So as $n \rightarrow \infty$, not only $U(n)$ & $V(n) \rightarrow \infty$, but also $\left[\frac{V(n)}{U(n)}\right] \rightarrow \infty$.

Therefore finding a counter example is impossible. I read, a long time ago, somewhere, probably in one, two, three - to infinity of George Gamov, that "it has been proved that all theorems cannot be proved". The Author, further stated in that book that If someone proves that Fermat's Last Theorem was not provable, then that itself constitutes a proof of the theorem because, if it is untrue, then that can be proved by a counter example. Now as it is not possible to disprove Goldbach's Hypothesis, does it constitute a proof of the Hypothesis?

----- X -----

**3. If $f(a) = 1 - a^p - (1 - a)^p \equiv 0 \pmod{p^3}$, then
 $f(a_r) \equiv 0 \pmod{p^{2r+1}}$ and
 3^{p-1} is not $\equiv 1 \pmod{p^3}$, if $p \equiv 1 \pmod{6}$**

(1) Introduction

Let $\frac{x}{x+y} = a$, & $\frac{y}{x+y} = 1 - a = b$. Then, an analysis of
 $(x + y)^p - x^p - y^p \equiv 0 \pmod{p^3}$ can be analysed by analysing
the equation $1 - a^p - (1 - a)^p \equiv 0 \pmod{p^3}$ --- (1)

That is, $1 - a^p - b^p \equiv 0 \pmod{p^3}$ --- (1)

It has been proved that $2^{p-1} - 1$ is not divisible by p^3
for any prime 'p' Hence '2' is not a solution to eqn (1).

$$f(a) = 1 - a^p - b^p = p \sum P_s \cdot (ab)^{(2s-1)} \cdot (1 - ab)^{(p-6s+3)/2}$$

$$\text{Where } P_s = \frac{2}{p-2s+1} \cdot \frac{p-2s+1}{2} C_{(2s-1)} \text{ --- (2)}$$

(2) If, $(1 - ab) \equiv 0 \pmod{p}$ then $f(a_r) \equiv 0 \pmod{p^{(2r+1)}}$

Let $a \equiv a_1 \pmod{p}$ & $a_1^{p-1} \equiv 1 \pmod{p}$ & not $\equiv 1 \pmod{p^2}$

Then, a_r is defined as, $a_r = (a_{r-1})^p$ --- (3)

Therefore, $a_r^{p-1} \equiv 1 \pmod{p^r}$ & not $\equiv 1 \pmod{p^{r+1}}$

$1 - ab = 1 - a + a^2 = 1 - b + b^2 \equiv 0 \pmod{p}$ & therefore

$$1 - a_r b_r = 1 - a_r + a_r^2 = 1 - b_r + b_r^2 \equiv 0 \pmod{p^r} \text{ --- (4)}$$

From (4), $f(a_r) \equiv 0 \pmod{p^r}$ --- (5)

$1 - a + a^2 \equiv 0 \pmod{p}$ has no solution if $p \equiv 5 \pmod{6}$

So, $p \equiv 1 \pmod{6}$. Hence, In eqn (2) every term on the RHS

are divisible by $p(1 - a_r b_r)^2$ & so $f(a_r) \equiv 0 \pmod{p^{2r+1}}$

It can also be proved in a different way.

From (5), $f(a_{2r+1}) \equiv 0 \pmod{p^{2r+1}}$ & so

$$f(a_{2r+1}) = f(a_r) + [a_{2r+1} - a_r] p [b_r^{p-1} - a_r^{p-1}] + \frac{1}{2!} [a_{2r+1} - a_r]^2 p(p - 1 - b_r p - 2 - a_r p - 2 + \dots) \text{ \& so,}$$

$$\underline{f(a_{2r+1}) \equiv f(a_r) \equiv 0 \pmod{p^{2r+1}}} \text{ --- (6)}$$

(3) $f(a_r) \equiv 0 \pmod{p^{2r+1}}$

$$f(a) = p \sum P_s (ab)^{2s-1} \cdot (1 - ab)^{(p-6s+3)/2} \text{ --- (2)}$$

$$\frac{1}{p} \cdot f(a) = ab (1 - ab)^{(p-3)/2} \cdot \sum P_s \left[\frac{a^2 b^2}{(1 - ab)^3} \right]^{s-1}$$

$$\text{Let } B = ab(1 - ab)^{(p-3)/2}, K = \left[\frac{a^2 b^2}{(1 - ab)^3} \right] \text{ \&}$$

$$\phi(k) = \sum P_s K^{(s-1)}, \text{ Then}$$

$$\frac{1}{p} f(a) = B \phi(K) \text{ --- (7)}$$

In eqn(7), ab is not $\equiv 1 \pmod{p}$, $a \neq 2, -1$ or 2^{-1}

Therefore $B, K, \frac{dB}{da}, \frac{dK}{da}$ are not divisible by "p".

$$\text{Hence } \phi(k_1) \equiv \phi(k_2) \equiv \phi(k_3) \equiv 0 \pmod{p^2} \text{ --- (8)}$$

$$b_1^{p-1} - a_1^{p-1} = \phi(K_1) \frac{dB_1}{da_1} + B_1 \phi'(K_1) \frac{dK_1}{da_1}, \text{ Therefore}$$

$$\phi'(K_1) \equiv 0 \pmod{p} \text{ \& not } \equiv 0 \pmod{p^2} \text{ --- (9)}$$

$$\text{Hence, } [\phi(K_1) \div \phi'(K_1)] \equiv 0 \pmod{p} \text{ --- (10)}$$

$$\phi(K_1) = \frac{1}{p} \frac{f(a_1)}{B_1}, \text{ Therefore}$$

$$\phi'(K_1) \frac{dK_1}{da_1} = \frac{b_1^{p-1} - a_1^{p-1}}{B_1} - \frac{1}{p} f(a_1) \frac{1}{B_1^2} \frac{dB_1}{da_1}, \text{ \& so ,}$$

$$\phi(K_1) \div \left[\phi'(K_1) \frac{dK_1}{da_1} \right] = \frac{1}{p} \frac{f(a_1)}{B_1} \div \left\{ \frac{b_1^{p-1} - a_1^{p-1}}{B_1} - \frac{f(a_1)}{p B_1^2} \frac{dB_1}{da_1} \right\}$$

$$\phi(K_1) \div \left[\phi'(K_1) \frac{dK_1}{da_1} \right] = f(a_1) \div \left\{ p(b_1^{p-1} - a_1^{p-1}) - \frac{f(a_1)}{B_1} \frac{dB_1}{da_1} \right\}$$

$$\frac{\phi(K_1)}{\phi'(K_1) \frac{dK_1}{da_1}} \left\{ p(b_1^{p-1} - a_1^{p-1}) - \frac{f(a_1)}{B_1} \frac{dB_1}{da_1} \right\} = f(a_1)$$

$$\frac{\phi(K_1)}{\phi'(K_1) \frac{dK_1}{da_1}} p(b_1^{p-1} - a_1^{p-1}) = f(a_1) + \frac{\phi(K_1)}{\phi'(K_1) \frac{dK_1}{da_1}} \frac{f(a_1)}{B_1} \frac{dB_1}{da_1} \quad \text{--- (12)}$$

LHS of eqn (12) $\equiv 0 \pmod{p^3}$ and

not $\equiv 0 \pmod{p^4}$. Hence, as $f(a_1) \equiv 0 \pmod{p^3}$

RHS of eqn (12) $\equiv 0 \pmod{p^3}$ & not $\equiv 0 \pmod{p^4}$

The second term of RHS of eqn(12) $\equiv 0 \pmod{p^4}$ --- (13)

$$\frac{\phi(K_2)}{\phi'(K_2) \frac{dK_2}{da_2}} p(b_2^{p-1} - a_2^{p-1}) \equiv f(a_2) + \frac{\phi(K_2)}{\phi'(K_2) \frac{dK_2}{da_2}} \frac{f(a_2)}{B_2} \frac{dB_2}{da_2} \quad \text{--- (14)}$$

LHS of eqn (14) $\equiv 0 \pmod{p^4}$

Therefore, $f(a_2) \equiv 0 \pmod{p^4}$ --- (15)

Therefore, from eqns (12), (13), (14), (15)

$f(a_3) \equiv 0 \pmod{p^5}$ and so

$f(a_2) \equiv f(a_3) \equiv 0 \pmod{p^5}$ --- (16)

From eqn (16). by PMI, $f(a_r) \equiv 0 \pmod{p^{2r+1}}$ --- (17)

(4) If, $p \equiv 1 \pmod{6}$, 3^{p-1} is not $\equiv 1 \pmod{p^3}$

It is assumed that for a prime, "p"

$p \equiv 1 \pmod{6}$ & $3^{p-1} \equiv 1 \pmod{p^3}$. --- (18)

If $p \equiv 1 \pmod{6}$, Then solution exists for the equation

$$1 + a + a^2 \equiv 0 \pmod{p}$$

So let, $1 + a_r + a_r^2 \equiv 0 \pmod{p^r}$ --- (19)

$$1 + a_1 + a_1^2 = 1 + (1 - b_1) + (1 - b_1^2) = 3(1 - b_1) + b_1^2$$

$$\text{Hence, } b_1^2 \equiv -3(1 - b_1) \equiv -3a_1 \pmod{p}$$

$$\text{Therefore, } b_1^{2p} \equiv -3^p a_1^p \equiv -3a_2 \equiv b_2^2 \equiv 0 \pmod{p^2}$$

$$\text{Hence, } b_1^p \equiv b_2 \equiv 1 - a_2 \equiv 1 - a_1^p \pmod{p^2}$$

$$\text{So, } (1 - a_1)^p \equiv (1 - a_1^p) \pmod{p^2}$$

$$\text{ie, } f(a_1) = 1 - a_1^p - (1 - a_1)^p \equiv 0 \pmod{p^2} \quad \text{--- (20)}$$

$$\text{Similarly, } f(a_2) \equiv 0 \pmod{p^3} \quad \text{--- (21)}$$

$$\text{So, } f(a) \equiv 0 \pmod{p^3}$$

$$\text{\& hence } f(a_r) \equiv 0 \pmod{p^{2r+1}} \quad \text{--- (22)}$$

$$b_3^2 \equiv -3a_3 \pmod{p^3} \text{ \& So, } b_3^{2p} \equiv -3^p a_3^p \pmod{p^4}$$

$$\text{That is, } b_4^2 \equiv -3^p a_4 \pmod{p^4}$$

$$\text{That is, } -3a_4 \equiv -3^p a_4 \pmod{p^4}$$

$$\text{Therefore, } 3^{p-1} \equiv 1 \pmod{p^4}$$

$$\text{Hence by PMI, } 3^{p-1} \equiv 1 \pmod{p^r} \text{ for all values of } r \quad \text{--- (23)}$$

Eqn (23) is possible if and only if $p = 1$. Therefore

3^{p-1} is not $\equiv 1 \pmod{p^3}$ if $p \equiv 1 \pmod{6}$

----- X -----



Author Contribution Statement: NIL.

Author Acknowledgement: NIL.

Author Declaration: I declare that there is no competing interest in the content and authorship of this scholarly work.



The content of the article is licensed under <https://creativecommons.org/licenses/by/4.0/> International License.