Finity of solutions to exponential Diophantine Equation $p^n - q^m = C$ for primes p, q

Kosuke Sato and Ziyan Fang

November 2023

1 Abstract

In 1936 and in 1945, Subbayya Sivasankaranarayana Pillai suggested the conjecture that for any given $k \geq 1$, the number of positive integer solutions (a, b, x, y) with $x \geq 2$ and $y \geq 2$, to the diophantine equation $a^x - b^y = k$ is finite for some positive integer k[1]. This was inspired by the Catalan's Conjecture in 1844, proven by Preda Mihailescu in 2002, which stated that the only solution (a, b, x, y) where $x, y > 1$ to the equation $a^x - b^y = 1$ is $(3, 2, 2, 3)$. This paper investigates into the other generalization of Pillai's Conjecture that there is an finite number of positive integer solutions (x, y) for each equation $p^x - q^y = C$. **The current progress is* $C = 1, 3$.

2 Proof of only finite number of solutions (m, n) that satisfies $p^n - q^m = 1$ for all ordered pairs (p, q)

Claim 1. There are finitely many integral solutions $m, n \in \mathbb{Z}$ to the equation $2^n - 3^m = 1$.

Proof. If $n \leq 0, 2^0 - 3^m = 1$ has no solution. If $n = 1$, $2^1 - 3^0 = 1$. If $n = 2$, $2^2 - 3^1 = 1$. Then $n \geq 3$. We have

$$\begin{aligned} 2^n - 3^m &\equiv 1 \pmod 8 \\ -3^m &\equiv 1 \pmod 8. \end{aligned}$$

Note that $3^2 \equiv 1 \pmod 8$. If m is odd, $-3^1 \equiv 1 \pmod 8$, contradiction. If m is even, $-3^0 \equiv 1 \pmod 8$, contradiction. Thus there are no solutions for $n \geq 3$. Therefore, there are only two solutions, which is finite! ∎

[1] arXiv:0908.4031v1 [math.NT]

Claim 2. If $m, n \in \mathbb{Z}$ is a solution to $p^n - q^m = 1$, then $m, n \geq 0$.

Proof. If $n < 0$, then $p^n < 1 \implies q^m < 0$, which is impossible. Thus $n \geq 0$, so p^n is an integer. Thus q^m must also be an integer, so $m \geq 0$. $\square$

Claim 3. If p, q are odd primes, then $p^n - q^m = 1$ has no integral solutions.

Proof. By *Claim 2*, we know that $m, n \geq 0$. Since p, q are odd, p^m and q^n are both odd, meaning that their difference has to be even. However, 1 is odd, contradiction. Thus $p^n - q^m = 1$ has no integral solutions. $\square$

Claim 4. The only integral solution to the equation $2^m - 2^n = 1$ is $(m, n) = (1, 0)$.

If $m, n > 1$, then 2^m and 2^n are both even, so their difference will never by odd. Thus at least one of m, n is 0. If $m = 0$, then $1 - 2^n = 1$, which has no solution. If $n = 0$, then $2^m - 1 = 1 \implies 2^m = 2 \implies m = 1$. Thus the only solution is $(1, 0)$. $\square$

Claim 5. There are finitely many integral solutions $m, n \in \mathbb{Z}$ to the equation $2^n - q^m = 1$ where q is an odd prime.

Proof. Let $q + 1 = 2^k \cdot \ell$ where ℓ is odd. Then note that $q \equiv -1 \pmod{2^k}$ and $q \equiv 2^k - 1 \pmod{2^{k+1}}$. Furthermore, since q is odd, $k \geq 1$, so

$$q^2 \equiv (2^k - 1)^2 \equiv 2^{2k} - 2^{k+1} + 1 \equiv 1 \pmod{2^{k+1}}$$

If $n \leq k$, then similarly there are finite solutions. If $n > k$,

$$2^n - q^m \equiv -q^m \pmod{2^{k+1}}.$$

Let $m = 2m' + r$ where $r \in \{0, 1\}$ by the Division Algorithm, then

$$-q^m \equiv -q^{2m'+r} \equiv -(q^2)^{m'} \cdot q^r \equiv -q^r \pmod{2^{k+1}}.$$

If $r = 0$, then $-q^r \equiv -1 \not\equiv 1 \pmod{2^{k+1}}$. If $r = 1$, then $-q^r \equiv -q \equiv 1 - 2^k \not\equiv 1 \pmod{2^{k+1}}$. Therefore, there are no solutions with $n > k$, so there are finitely many solutions in total. $\square$

Claim 6. There are finitely many integral solutions $m, n \in \mathbb{Z}$ to the equation $p^n - 2^m = 1$ where p is an odd prime.

Proof: Rearrange to get $p^n - 1 = 2^m$, which implies that $p^n - 1$ has only factors of 2.

$$p^n - 1 = (p-1)(p^{n-1} + p^{n-2} + \cdots + 1)$$

For the rest of the proof, let $f(n) = p^{n-1} + p^{n-2} + \cdots + 1$. Because $p^n - 1$ is a power of 2, then $p - 1$ is also a power of 2. Let $p = 2^k + 1$ for some $k \in \mathbb{Z}$, $k \geq 0$. We can split into cases by the parity of n.

1. n is odd. Then since p is odd, we have

$$p^{n-1} + p^{n-2} + \cdots + 1 \equiv 1 + 1 + \cdots + 1 \equiv n \equiv 1 \pmod 2,$$

which is a power of 2 if and only if $n = 1$, so the expression simplifies to $p - 1 = 2^m$. Thus there is at most one solution, which is finite.

2. n is even, then

$$f(n) = (p+1)(p^{n-2} + p^{n-4} + ... + 1) = 2(2^{k-1} + 1)(p^{n-2} + p^{n-4} + \cdots + 1).$$

If $k = 0$, we have $p = 1$, which is not a prime. Thus all three terms are integers. Thus we need $2^{k-1} + 1$ to be a power of 2. That is, $2^{k-1} + 1 = 2^{\zeta}$ for some $\zeta \in \mathbb{Z}$. By *Claim 4*, this is only possible when $k - 1 = 0 \implies k = 1$. This leads to $p = 3 \implies 3^n - 2^m = 1$. Since n is even, let $n = 2n_1$, we get that $3^{2n_1} - 1 = 2^m \implies (3^{n_1} - 1)(3^{n_1} + 1) = 2^m$. Therefore, $3^{n_1} - 1$ and $3^{n_1} + 1$ are both powers of 2. Thus we have two powers of 2 with difference 2. Thus the only possible pair is 2 and 4. Then we have $3^2 - 2^3 = 1$. Therefore, $(n, m) = (2, 1)$ is the only solution when n is even. □

Claim. If p and q are primes then $p^n - q^m = 1$ has at most finitely many solutions $m, n \in \mathbb{Z}$.

Proof. By *Claim 3*, *Claim 4*, *Claim 5*, *Claim 6*, we are done. □

3 Proof of only finite number of solutions (m,n) that satisfies $p^n - q^m = 3$ for all ordered pairs (p,q)

By parity, one of p, q must be equal to 2.

Problem 2.1 Prove that there are only a finite number of ordered pairs (m,n) that satisfies $2^n - p^m = 3$ for each fixed value of p.

Theorem 2.1.0. Lifting the Exponent Lemma: Consider the expression $p^m - 1$ and p is a prime.

1. If $m \equiv 1 \pmod 2$, $v_2(p^m - 1) = v_2(p-1)$
2. If $m \equiv 0 \pmod 2$, $v_2(p^m - 1) = v_2(p-1) + v_2(p+1) + v_2(m) - 1$
3. If $p = 2$ and $2 \mid m$, $v_3(p^m - 1) = v_3(p-1) + v_3(m)$

Claim 2.1.1. $m \equiv 1 \pmod 2$ and $p \equiv 5 \pmod 8$

Proof. Assume that $m \equiv 0 \pmod 2$, then $v_2(p^m - 1) \geq 3$ because $v_2(p-1) + v_2(p+1) \geq 2$ since $p \equiv 1$ or $3 \pmod 4$, which one of $p-1$ or $p+1$ must be divisible by 4 and the other only divisible by 2. Furthermore, since $m \equiv 0 \pmod 2$, $v_2(m) - 1 \geq 1 - 1 \geq 0$. $\therefore v_2(p^m - 1) \geq 3$.

However, $v_2(2^n - 2^2) = v_2(2^{n-2} - 1) + v_2(2^2) = 2$ for all $n > 0$. Therefore, $v_2(2^n - 4) \neq v_2(p^m - 1)$. Contradiction. □

Now, $m \equiv 1 \pmod 2 \implies v_2(p^m - 1) = v_2(p-1) = v_2(2^n - 4) \implies p \equiv 1 \pmod 4$ but not $1 \pmod 8$. Therefore, $p \equiv 5 \pmod 8$. ■

Claim 2.1.2. Assume $n \geq 4$, $p \equiv -3, 5 \pmod{16}$ and $m \equiv 1 \pmod 4$

Proof. Plug in $8k + 5$ back gives $2^n - (8k+5)^m = 3 \implies 5^m + 3 \equiv 0 \pmod 8$. Consider modulo 16.
If $k \equiv 0 \pmod 2$, $2^n - (8k+5)^m \equiv 5^m \pmod{16} \implies 5^m \equiv -3 \pmod{16}$, which is achievable since $5^3 \equiv -3 \pmod{16}$ and $\mathrm{ord}_{16}(5) = 4$.

When $k \equiv 1 \pmod 2$, $2^n - (16k + 13)^m \equiv 3 \pmod{16}$, which is clearly achievable since $13 + 3 = 16$. □

Notice that $5^3 + 3 = 2^7$. Consider modulo 256. Since $\text{ord}_{256}(5) = 8$, We only seek to check from 4 to 7.

1. $5^4 \equiv 113 \pmod{256}$
2. $5^5 \equiv 53 \pmod{256}$
3. $5^6 \equiv 9 \pmod{256}$
4. $5^7 \equiv 45 \pmod{256}$

$\therefore 5^m \equiv -3 \pmod{256}$ doesn't exist a solution, and therefore, $p = 5$ is finite. $\square$

From $5 \pmod{16}$, when $n > 4$, $32 \mid 2^n$. Let $p = 16a_1 + 2^3 - 3 = 2^3(2a_1+1) - 3$, then this still remains to be $5 \pmod{16}$, but if $2a_1 + 1 \equiv 3 \pmod 4$, then this will result in $21 \pmod{32}$. Furthermore, from $13 \pmod{16}$, rewrite as $16a_1 + 2^4 - 3 = 16(a_1+1) - 3$, which $a_1 \equiv 1 \pmod 2 \implies p \equiv -3 \pmod{32}$ and otherwise $p \equiv 13 \pmod{32}$.

$$p \equiv 2^3 - 3, 2^4 - 3 \pmod{16}$$

$$p \equiv 2^3 - 3, 2^4 + 2^3 - 3, 2^4 - 3, 2^5 - 3 \pmod{32}$$

$$p \equiv 2^3 - 3, 2^5 + 2^3 - 3, 2^4 + 2^3 - 3, 2^5 + 2^4 + 2^3 - 3, 2^4 - 3, 2^5 + 2^4 - 3, 2^5 - 3, 2^6 - 3 \pmod{64}$$

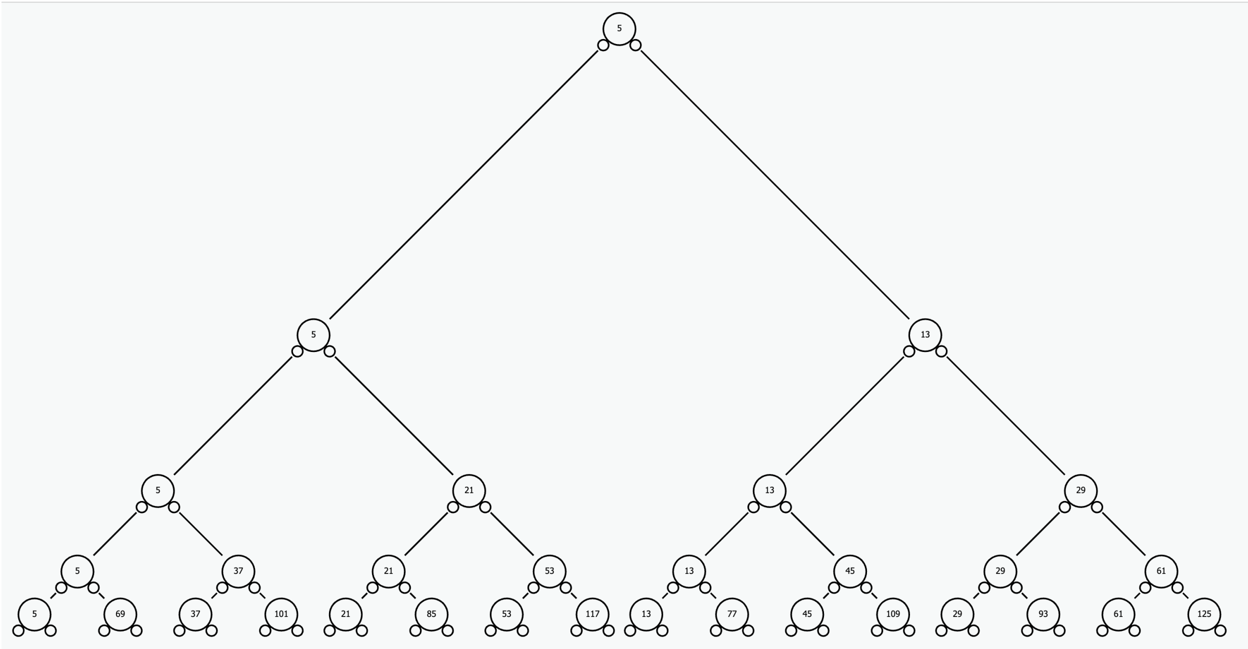

Figure 1: The binary tree of all possibilities of $p \pmod{2^n}$

Claim 2.1.3.1. $G_n = 8\mathbb{N}_{2^{n-3}} - 3$

Proof by Induction:

Base Case. $G_3 = 5 = 8 - 3 \in \mathbb{Z}_8$, and $\{1\} = \mathbb{N}_{2^{3-3}}$ $\square$

Inductive Step. Assume that all the elements in G_n can be expressed as $8x - 3$ for some x, then S_n, by definition, would include $8x + 2^n - 3 = 8(x + 2^{n-3}) - 3$ in $\mathbb{Z}_{2^{n+1}}$. Now, consider $p(x) = \frac{3}{8}x$, for all elements s in S_n, $2^{n-3} < p(s)2^{n-3} \leq 2^{n-2}$, while for all elements g in G_n, $p(g) \leq 2^{n-3}$. Thus, $G_n \cup S_n$ contains all $8k + 1$ such that $k \in \mathbb{N}_{2^{n-2}}$, which implies $G_n \cup S_n$ is G_{n+1}. $\square$

Claim 2.1.4. $p = (2a + 1)2^k - 3$ and $m = a_1 2^{k-2} + 1$ for some odd positive integer a_1.

Proof. The first part by *Claim 2.1.3*, and the second part follows by *Theorem 2.1.0*, since $v_2(3^m - 3) = k$. By *Claim 2.1.1*, $m \equiv 1 \pmod 2 \implies 3^{m-1} - 1 = 3^{m-1} - 1^{m-1} = v_2(3 - 1) + v_2(3 + 1) + v_2(m - 1) - 1 = 2 + v_2(m - 1) \implies v_2(m - 1) = k - 2$, which implies that $m = a_1 2^{k-2} + 1$ such that $\gcd(a_1, 2) = 1$ $\square$

Conjecture 2.1.3. $2^n - p^m = 3$ exists an ordered pair (n, m) iff $p = 2^k - 3$ for some positive integer k, and $m = a_1 2^{k-2} + 1$.

$*$ *I cannot prove or disprove this conjecture, but this seems correct because for all the values of* $p = (2a + 1)2^k - 3$ *that cannot be expressed in the form* $2^k - 3$*, such as* $21, 37, 53, 101$*, doesn't exist an ordered pair* (n, m) *that satisfies* $2^n - p^m = 3$*. Hope to continue working on this during the rest of the school year and in college.*

Assume that this conjecture is true, then we have

$$2^n - (2^k - 3)^{a_1 2^{k-2} + 1} = 3$$

$$\frac{2^n - 3}{2^k - 3} = (2^k - 3)^{a_1 2^{k-2}}$$

$$2^{n-k} + \frac{3}{2^k - 3}(2^{n-k} - 1) = (2^k - 3)^{a_1 2^{k-2}}$$

Corollary 2.1.4. $\frac{2^{n-k} - 1}{2^k - 3}$ is a power of 3.

Remark. If $n - k$ is odd, there will be a contradiction since $\mathrm{ord}_3(2) = 2$, and therefore,

$2^{n-k} \equiv 2 \pmod 3$, and $3\left(\frac{2^{n-k}-1}{2^k-3}\right) \equiv 0 \pmod 3$ since $\gcd(2^k-3, 3) = 1$, but $(2^k-3)^{a_1 2^{k-2}}$ is a square, and 2 is not a quadratic residue in $\mathbb{Z}_3$ and k must be larger than 2. Contradiction. $\square$

Claim 2.1.4 $\frac{2^{n-k}-1}{2^k-3} \in \{1, 3\}$.

Proof. Assume otherwise that $v_3(\frac{2^{n-k}-1}{2^k-3}) \geq 2$, then we have $\frac{2^{n-k}-1}{2^k-3} = 3^{a_1 2^{k-2}-1}$ for some positive integer a_1, since $\gcd(2^k-3, 3) = \gcd(2^k, 3) = 1$. Now, by *Theorem 2.1.0*, $2 \mid n-k$, and $v_3(2^{n-k}-1) = v_3(3) + v_3(n-k) = 1 + v_3(n-k) = a_1 2^{k-2} - 1 \implies v_2(v_3(n-k)) = v_2(2^{k-2}-2) = 1$. $\therefore 18 \mid n-k$

Consider $\frac{-1}{3}$ in $\mathbb{Z}_{32}, \mathbb{Z}_{64}, \mathbb{Z}_{128}, \mathbb{Z}_{256}, \mathbb{Z}_{512}, \mathbb{Z}_{1024}$, which we have $21, 21, 85, 85, 341, 341$, which are all not expressed in $2^a - 3$.

Claim 2.1.5. $-\frac{1}{3} \neq 2^a - 3 \in \mathbb{Z}_{2^n}$ for all $n \geq 5$.

Proof. We proceed with induction to show that $-\frac{1}{3} = 8x - 3 \in \mathbb{Z}_{2^n}$ such that $\gcd(x, 2) = 1$.
Base Case. $-\frac{1}{3} \in \mathbb{Z}_{32} = 21$, and $21 + 3 = 24 = 3 \cdot 8$ $\square$
Inductive Step. Assume that $-\frac{1}{3} = 8a_1 - 3$, then we have $8a_1 - 3 \equiv -1 \pmod{2^n}$.

If $v_2(8a_1 - 2) \geq n+1$, then we are done.

If $v_2(8a_1-2) = n$, then $8a_1 - 2 + 2^n = 2^3(2^{n-3} - a_1) - 2 \equiv 0 \pmod{2^{n+1}} \implies 8(2^{n-3}-a_1) - 3 \equiv -1 \pmod{2^{n+1}}$ and by the definition of a_1, $\gcd(2^{n-3} - a_1, 2) = 1$. $\square$

$\therefore -\frac{1}{3} \neq 2^a - 3 \in \mathbb{Z}_{2^n}$ for all $n \geq 5$. $\blacksquare$

Now, we seek to prove that $\left(-\frac{1}{3}\right)^{18y} \neq 2^a - 3 \in \mathbb{Z}_{2^n}$ for all $n \geq 5$, which implies that $(8a_1-3)^{18} \neq 2^\beta - 3$ in $\mathbb{Z}_{2^n}$. $(8a_1-3)^{18y} \equiv 3^{18} \pmod 8$, and because we want to assume that β is infinite, then $8 \mid 2^\beta$. Thus, we have $3^{18y} + 3 = 3(3^{18y-1}+1) \equiv 0 \pmod 8 \implies 3^{18y-1} \equiv -1 \pmod 8$, which is false since $\text{ord}_8(3) = 2$, so $3^{2k+1} \equiv 3 \pmod 8$ is always true. We have a contradiction. $\square$

$$\frac{2^{n-k}-1}{2^k-3} = 1 \implies 2^{n-k} = 2^k - 2 \implies k = 2, n = 3$$

Which contradicts because $2^k - 3 = 1$ is not a prime. $\square$

$$\frac{2^{n-k}-1}{2^k-3}=3 \implies 2^{n-k}=3\cdot 2^k-2^3=2^3(3\cdot 2^{k-3}-1)$$

Which implies that k must be equal to 3, and therefore, $n=7$, and $2^3-3=5$ is a prime. $\square$
The conclusion is that if $m>1$ in the equation $2^n-p^m=3$, then $(m,n,p)=(3,7,5)$ is the only solution, which is finite. Furthermore, when $m=1$, p must be 2^n-3 and it must be a prime. Therefore, for all the pairs $(2,2^n-3)$, then can be at most 1 solution. $\square$

Problem 2.2. Prove that there are only a finite number of ordered pairs (m, n) that satisfy $p^n - 2^m = 3$

Proof. The problem statement is equivalent to $p^n = 2^m + 2 + 1 = 2^m + 2^2 - 1$.

Claim 2.2.1. If $m \equiv a \pmod 6$ such that $a \in \{2, 4, 5\}$, then there is a finite number of solution pairs.

Proof. $2^m + 2 + 1 = 2^m - 2^2 + 2^2 + 2 + 1$, and $2^m + 2^2 - 1 = 2^m + 2^4 - 2^4 + 2^2 - 1$. Let $m = 6k + r$ for some k, r such that $0 \le r \le 5$,

$$2^{6k+r} + 2 + 1 = (2^{6k+r} - 2^2) + 2^2 + 2 + 1 = 2^2(2^{6k+r-2} - 1) + 2^2 + 2 + 1$$

$$2^{6k+r} + 2^2 - 1 = (2^{6k+r} + 2^4) - 2^4 + 2^2 - 1 = 2^4(2^{6k+r-4} + 1) - 2^4 + 2^2 - 1$$

Since $x^2 + x + 1 = \Phi_3(x) \in \mathbb{Z}(\zeta_3)$, when $3 \mid 6k + r - 2$, then $2^{6k+r-2} - 1$ is divisible by $2^2 + 2 + 1$. Since $x^4 - x^2 + 1 = \Phi_{12}(x) \in \mathbb{Z}(\zeta_{12})$, when $6 \mid 6k + r - 4$, $2^{6k+r-4} - 1$ is divisible by $2^4 - 2^2 + 1$.

1. $m \equiv 2, 5 \pmod 6$, then $2^2 + 2 + 1 \mid 2^m + 2 + 1 \implies p = 2^2 + 2 + 1 = 7$ since 7 is a prime. This simplifies to $7^n - 2^m = 3 \implies (2^3 - 1)^n - 2^m = 3$. By binomial theorem, all terms in $(2^3 - 1)^n$ will be expressed as $\binom{n}{k} 2^{3k}(-1)^{n-k}$, which are all divisible by 8 other than $(-1)^n$ term, but $8 \nmid 3 + 1$. $\therefore m \le 2$, which is obviously finite. $\square$

2. $m \equiv 4 \pmod 6$, then $2^4 - 2^2 + 1 \mid 2^m + 2^2 - 1 \implies p = 2^4 - 2^2 + 1 = 13$ and 13 is a prime. $13^n - 2^m = 3$ doesn't exist any solution because when taking modulo 7, $2^m = 1, 2, 4 \in \mathbb{Z}_7$, which $2^m + 3 \ne 1$ or $-1 \pmod 7$. $\square$

When $m \equiv 0, 3 \pmod 6$, then 2^m is a perfect cube. We seek to show that -3 is either not a cubic residue in $\mathbb{Z}_p$, or if it is, it cannot be achived by power of 2. Consider the legendre symbol $\left(\frac{-3}{p}\right)_3$

Lemma 2.2.2. $-3 \pmod p$ is absolutely achievable when $p \equiv 2 \pmod 3$

Proof. We seek to prove that all elements in $\frac{\mathbb{Z}}{p\mathbb{Z}}$ is the set of all the cubic residues modulo p. Write p as $3j + 2$, then let $a \in \frac{\mathbb{Z}}{p\mathbb{Z}}$, we have

$$(a^{2j+1})^3 = a^{6j+3} = a^{3j+2} a^{3j+1} = a(1) = a \pmod p$$

Which implies that ther is a bijective relationship between $\frac{\mathbb{Z}}{p\mathbb{Z}}$ and the set of cubic residues modulo p. $\square$

Conjecture 2.2.3. $-3 \pmod p$ is never a cubic residue in $\mathbb{Z}_p$ when $p \equiv 1 \pmod 3$.
Disproved. When $a = 4$ and $p = 67$. ■

Salvaged Conjecture 2.2.4. $x^3 + 3$ in $\mathbb{Z}_p$ can exist at most one root x_1 such that x_1 is a power of 2.

1. $p = 7$.

x	0	1	2	3	4	5	6
$x^3 + 3 \pmod p$	3	4	4	2	4	2	2

   Which there isn't a solution since none of them is divisible by 7.

2. $p = 13$.

x	0	1	2	3	4	5	6	7	8	9	10
$x^3 + 3 \pmod p$	3	4	11	4	2	11	11	8	8	4	2

   There also isn't a solution in $\mathbb{Z}_{13}$

Claim 2.2.5. $x^3 + 3$ has exactly one root in $\mathbb{Z}_p$ where $p \equiv 2 \pmod 3$

Proof.

Subclaim 2.2.6. $x^3 - a$ is always reducible in $\mathbb{Z}_p$ if $p \equiv 2 \pmod 3$.

Proof. $x^3 \equiv a \pmod p$ is always solvable when $a = 3$ because $a^{\frac{p-1}{\gcd(3,p-1)}} \equiv 1 \pmod p$ is true when $a = -3$ by Fermat's Little Theorem.

Let ω be the third roots of unity, and let r be the root of $x^3 \equiv -3 \pmod p$

$$\begin{aligned} x^3 + 3 = (x-r)x^2 + rx^2 + 3 &= (x-r)x^2 + (x-r)rx + r^2x + 3 \\ &= (x-r)x^2 + (x-r)rx + r^2(x-r) + r^3 + 3 \\ &= (x-r)(x^2 + rx + r^2) = (x-r)(x-r\omega)(x-r\omega^2) \end{aligned}$$

Subclaim 2.2.6. -3 is not a quadratic residue modulo p if $p \equiv 2 \pmod 3$

Proof.

$$\begin{aligned} \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) &= (-1^{\frac{p-1}{2}})(-1^{\frac{p-1}{2}})\left(\frac{p}{3}\right)^{-1} \\ &= -1^{p-1}\left(\frac{p}{3}\right)^{-1} = \frac{1}{\left(\frac{p}{3}\right)} \end{aligned}$$

Which is equal to -1 since $\left(\dfrac{2}{3}\right) = -1$. $\square$

$\square$

Now from here, for the sake of contradiction, assume there are infinite number of k such that $r + kp$ is a power of 2, which we need infinite number of ordered pairs (x, y) such that $p \mid 2^x - 2^y$