P3: There are only finitely many integral solutions $m, n \in \mathbb{Z}$ to the equation

$$2^n - 3^m = 1.$$

More generally, if p and q are primes then

$$p^n - q^m = 1$$

has at most finitely many solutions $m, n \in \mathbb{Z}$. Can you generalize these assertions?

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! $\square$

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. □

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

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

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. □

Problem 2 Only finite umber of ordered pairs (m, n) that satisfies $2^n - p^m = 3$

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 $\text{ord}_{16}(5) = 4$.

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. □

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 $p \equiv 13 \pmod{32}$.

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

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

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

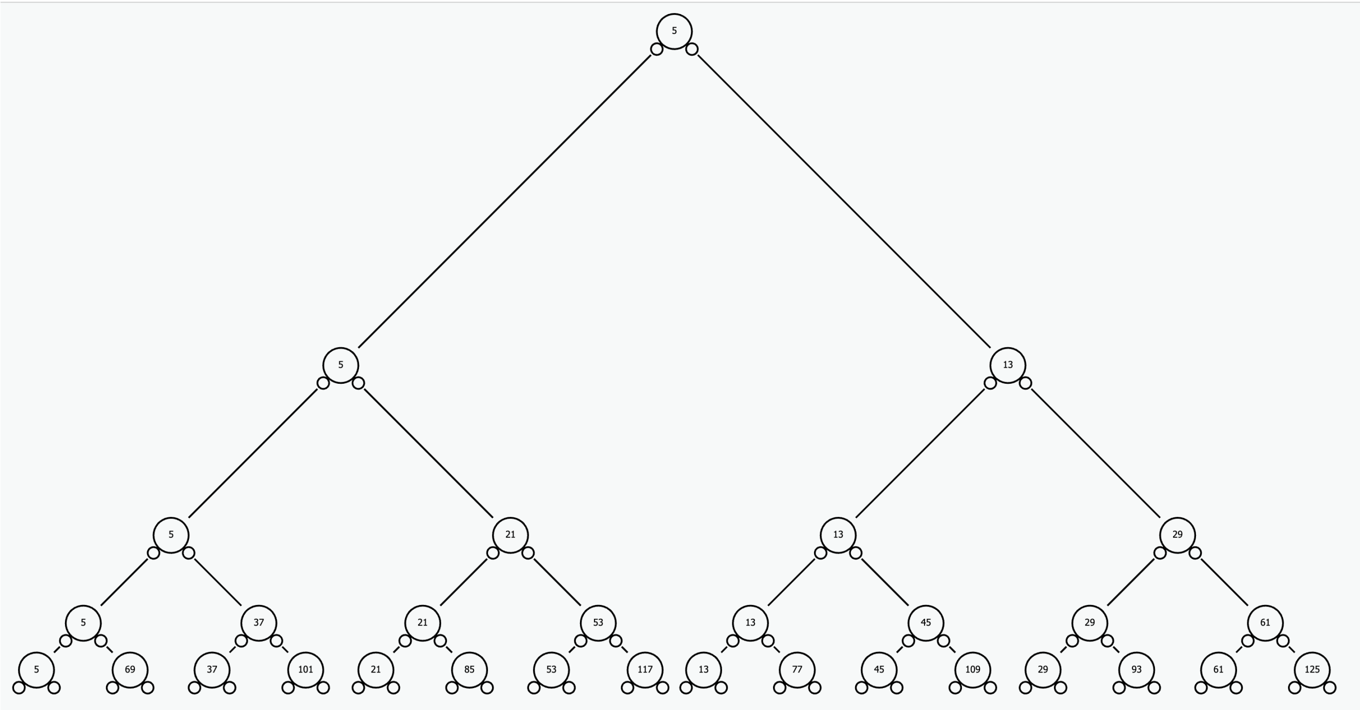

Figure 1: The binary tree of all possibilities of $p \pmod{2^n}$

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 $m = a_1 2^{k-2} + 1$

FTSOC assume that $p = (2b_1 + 1)2^k - 3$ such that $b_1 > 1$,

Assume true, then we have

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

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

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

The only odd part of LHS is $\frac{3}{2^k-3}(2^{n-k} - 1)$, while the odd part of RHS is $3^{a_1 2^{k-2}}$, so they must be equal.

Remark. The other case is when $n-k$ is odd, which creates a contradiction since $\text{ord}_3(2) = 2$, 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 $21 + 3 = 24 = 3 \cdot 8$ ☐
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, $\gcd(2^{n-3} - a_1, 2) = 1$. ☐

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

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 $3^{18y} + 3 = 3(3^{18y-1} + 1) \equiv 0 \pmod 8 \implies 3^{17} \equiv -1 \pmod 8$, which is false since $\text{ord}_8(3) = 2$, so $3^{2k+1} \equiv 3 \pmod 8$ is always true. We have a contradiction. ☐

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

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

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

Which implies that k must be equal to 3, and therefore, $n = 7$, and $2^3 - 3 = 5$ is a prime. ☐
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. ☐

Claim 2.1.3. For all n, there is 1 ordered pair (p, m) that satisfies the condition if $2^n - 3$ is a prime.

Proof. We prove by Induction that $p \equiv -3 \pmod{2^n}$
Base Case. Claim 2.1.1.
Inductive Step. Assume that $p \equiv -3 \pmod{2^k}$ for some $k < n$, then $2^n - p^m = 2^n - (a_1 2^k - 3)^m = 3$. By Binomial Theorem,

$$2^n - (a_1 2^k - 3)^m \equiv \binom{m}{1} a_1 2^k 3^{m-1} - 3^m \pmod{2^{k+1}}$$

Assume that $a_1 \equiv 0 \pmod 2$, then this is only equivalent to $-3^m \pmod{2^{k+1}}$ which implies $3^m + 3 = 3(3^{m-1} + 1) \equiv 0 \pmod{2^{k+1}}$, contradiction because when $k = 3$, $\text{ord}_{16}(3) = 4$ and $3^2 \equiv 9 \pmod{16}$.

$\therefore$ a_1 must be even, which $p = a_1 2^k - 3 \equiv -3 \pmod{2^{k+1}}$. Therefore, $p \equiv -3 \pmod{2^n}$, which must be equal to $2^n - 3$ ■

Problem 2: There are only finitely many integral solutions $m, n \in \mathbb{Z}$ to the equation

$$p^n - q^m = C.$$

such that p and q are primes, and $C \in \mathbb{N}$.

Proposition 2.1. If there are a finite number of ordered pairs (a_1, a_2) such that

$$\frac{p^{a_1} - C}{p^{a_2} - C} = q^b$$

For some positive integer b, then this is equivalent to the condition that there are a finite number of ordered pairs (m, n) such that $p^n - q^m = C$. Furthermore, if A is the size of the set of all ordered pairs (a_1, a_2), then there will be a total of at most $2A$ solutions.

Proof. Given that (a_1, b_1) and (a_2, b_2) both satisfies the equation where $a_1 > a_2$. Then

$$b_1 = \log_q(p^{a_1} - C)$$

$$b_2 = \log_q(p^{a_2} - C).$$

Note that since p^x is monotonically increasing, $p^{a_1} - C > p^{a_2} - C$. Again since $\log_q$ is monotonically increasing, $b_1 > b_2$. Therefore,

$$\begin{cases} p^{a_1} - C = q^{b_1} \\ p^{a_2} - C = q^{b_2} \end{cases}$$

Which we can divide to get that $\frac{p^{a_1}-C}{p^{a_2}-C} = q^{b_1-b_2}$. Now, rewrite the left hand side as $p^{a_1-a_2} + \frac{Cp^{a_1-a_2}-C}{p^{a_2}-C} = q^{b_1-b_2}$. Since $p^{a_2} - C = q^{b_2}$, $q \mid C(p^{a_1-a_2} - 1)$

Subclaim 2.1.1. $v_q(C(p^{a_1-a_2} - 1)) = b_2$

Proof. $\frac{C(p^{a_1-a_2}-1)}{p^{a_2}-C} \in \mathbb{N} \implies C(p^{a_1-a_2} - 1) = q^{b_3}$ such that $b_3 \geq b_2$. FTSOC assume that $b_3 > b_2$, then $p \mid \frac{C(p^{a_1-a_2}-1)}{p^{a_2}-C} \implies q \mid p^{a_1-a_2}$, contradiction since p is a prime not equal to q. □

Subclaim 2.1.2. There will be at most 1 solution ordered pair (m, n) to the equation

$$p^n - p^m = C$$

when $C > 1$.

Proof.

$$p^n - p^m = p^m(p^{n-m} - 1)$$

Which when $C \equiv 0 \pmod{p}$, consider the value $\frac{C}{v_p(C)}$ which is relatively prime to p, then $\frac{C}{v_p(C)}$ must be equal to $p^{n-m} - 1$. Therefore,

$$(m, n) = \left(v_p(C), v_p(C) + \log_p\left(\frac{C}{v_p(C)} + 1\right)\right)$$

$\square$

Subclaim 2.1.3. $C = p^{a_2} - p^n$