INVARIANT FOR ODD NUMBERS UNDER TETRATION

Pranjal Jain

October 2020

1 Introduction

The aim of this paper is to generalize the result of Problem 3 of the 2019 PROMYS exam.

Problem definition

Define the sequence $\{t_k\}_{k\in\mathbb{N}_0}$ as

$$t_0 = p,\ t_{k+1} = p^{t_k}\ \forall\, k \in \mathbb{N}_0$$

where p is odd, $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ and $\mathbb{N} = \{1, 2, \ldots\}$. We shall show that given any $n, m \in \mathbb{N}$, with $m \geq n$,

$$t_m \equiv t_n\ (mod\ \ (p^2+1)^n)$$

In the original question that was in PROMYS 2019, only the special case of $p = 3$ and $n = 10$ was considered.

Since the claim is trivially true for $p = 1$, we will be neglecting that case. Henceforth it is assumed that $p \geq 3$.

The arguments used in this article may seem out of the blue to most, so I'd like to point out that all of them have their origins in the generalization of several numerical patterns I noticed on computing the values of the functions involved for the special case of $p = 3$ and values of n as large as my computer could handle.

2 Some useful identities and definitions

Identity 2.1

$ad \equiv bd \ (mod \ c) \implies a \equiv b \ (mod \ c)$, where $d, c \neq 0$ and d and c are co-prime, for $a, b, c, d \in \mathbb{Z}$.

Identity 2.2

$1 + x + x^2 + \ldots + x^{4k-1} = (x+1)(x^2+1)(1 + x^4 + x^8 + \ldots + x^{4(k-1)})$

Proof

$$\begin{aligned} 1 + x + x^2 + \ldots + x^{4k-1} &= \frac{x^{4k} - 1}{x - 1} \\ &= \frac{x^{4k} - 1}{x^4 - 1}(x+1)(x^2+1) \\ &= (x+1)(x^2+1)(1 + x^4 + x^8 + \ldots + x^{4(k-1)}) \end{aligned}$$

Definition 2.3

Define $mod_a(b)$ (for integers a and b, with $a \neq 0$) to be the smallest non-negative integer s.t.

$$mod_a(b) \equiv b \ (mod \ a)$$

Definition 2.4

Define $\phi(n) \in \mathbb{N}$ to be the smallest positive integer s.t.

$$p^{\phi(n)} \equiv 1 \ (mod \ (p^2+1)^n)$$

Proof that such a $\phi(n)$ must exist

We know that the sequence $\{mod_{(p^2+1)^n}(p), \ mod_{(p^2+1)^n}(p^2), \ mod_{(p^2+1)^n}(p^3), \ldots\}$ is periodic. If we assume that its period is some $a \in \mathbb{N}$ s.t. $\forall$ positive integers k greater than or equal to some positive integer $A \geq 1$, we have

$$p^{k+a} \equiv p^k \ (mod \ (p^2+1)^n)$$

Using *Identity 2.1*, we can 'cancel' p^k from both sides (since p and p^2+1 are co-prime), which yields that $a = \phi(n)$. ■

3 Some lemmas about the setup

Lemma 3.1

$\phi(n)$ is a multiple of 4 $\forall\, n \in \mathbb{N}$.

Proof by contradiction

Assume $\phi(n) = 4a + b$, where $a, b \in \mathbb{N}_0$ and $1 \leq b \leq 3$. We will now show that this leads to the contradiction that $b \neq 1, 2, 3$.

Since $p^{\phi(n)} \equiv 1 \ (mod \ \ (p^2+1)^n)$ (by definition), we have

$$\frac{p^{4a+b}-1}{p^2+1} \in \mathbb{N}$$

$$\implies \frac{p-1}{p^2+1}(1 + p + p^2 + \ldots + p^{4a+b-1}) \in \mathbb{N} \tag{1}$$

Let $k_1 = 1 + p + p^2 + \ldots + p^{4a-1}$. Hence, *Identity 2.2* guarantees that $\frac{p-1}{p^2+1} \times k_1 \in \mathbb{N}$. Also define k_2 as

$$k_2 = \sum_{r=4a}^{4a+b-1} p^r$$

In order for (1) to hold, we must have $\frac{p-1}{p^2+1} \times k_2 \in \mathbb{N}$.

Case I : $b = 1$

In this case, $k_2 = p^{4a}$. Since p and p^2+1 are co-prime, this means that $p-1$ must be a multiple of p^2+1, which is clearly false. Hence, $b = 1$ isn't possible.

Case II : $b = 2$

In this case, $k_2 = p^{4a} + p^{4a+1} = p^{4a}(p+1)$. Since p^{4a} and p^2+1 are co-prime, this must mean that $(p-1)(p+1) = p^2 - 1$ is a multiple of p^2+1, which is clearly false. Hence, $b = 2$ isn't possible.

Case III : $b = 3$

In this case, $k_2 = p^{4a} + p^{4a+1} + p^{4a+2} = p^{4a}(p^2+p+1)$. Since p^{4a} and p^2+1 are co-prime, this must mean that $(p-1)(p^2+p+1) = (p-1)(p^2+1) + (p-1)p$ is a multiple of p^2+1. Hence, $(p-1)p = p^2 - p$ is a multiple of p^2+1, which is clearly false. Hence, $b = 3$ isn't possible. ■

Lemma 3.2
$\forall\, n \in \mathbb{N}\ \exists\ k \in \mathbb{N}$ s.t $\phi(n+1) = k\,\phi(n)$.

Proof
Assume that $\phi(n+1) = a\,\phi(n) + b$, where $a, b \in \mathbb{N}_0$ and $b < \phi(n)$.

Since $p^{\phi(n+1)} \equiv 1\ (mod\ \ (p^2+1)^{n+1})$, that must also mean that $p^{\phi(n+1)} \equiv 1\ (mod\ \ (p^2+1)^n)$. Hence, we have

$$p^{a\phi(n)+b} \equiv 1\ (mod\ \ (p^2+1)^n)$$

$p^{a\phi(n)} \equiv 1\ (mod\ \ (p^2+1)^n)$, so we have

$$p^b \equiv 1\ (mod\ \ (p^2+1)^n)$$

which is only possible if $b = 0$, since any other value of b would contradict the definition of $\phi(n)$. ■

Lemma 3.3
$\forall\, n \in \mathbb{N}\ \exists\ k \in \mathbb{N}$ s.t $\phi(n+1) = k\,\phi(n)$ and $k \,|\, p^2+1$ (k divides p^2+1).

Proof
Let $\phi(n) = 4q$ for some $q \in \mathbb{N}$ (using *Lemma 3.1*), and hence, let $\phi(n+1) = 4kq$ (using *Lemma 3.2*). Hence, we have

$$\frac{p^{4q}-1}{(p^2+1)^n} = j \in \mathbb{N} \tag{2}$$

$$\frac{p^{4qk}-1}{(p^2+1)^{n+1}} \in \mathbb{N}$$

$$\iff \frac{p^{4q}-1}{(p^2+1)^n} \times \frac{1+p^{4q}+p^{8q}+\ldots+p^{4q(k-1)}}{p^2+1} \in \mathbb{N} \tag{3}$$

Since $p^{4q} \equiv 1\ (mod\ \ (p^2+1)^n)$, that also means that $p^{4q} \equiv 1\ (mod\ \ p^2+1)$. Hence (3) gives us

$$j \times \frac{1+p^{4q}+p^{8q}+\ldots+p^{4q(k-1)}}{p^2+1} \in \mathbb{N}$$

$$\iff j(1 + p^{4q} + p^{8q} + \ldots + p^{4q(k-1)}) \equiv 0 \ (mod \ p^2 + 1)$$

$$\iff jk \equiv 0 \ (mod \ p^2 + 1) \tag{4}$$

Since k is the smallest positive integer s.t. (4) holds (since the existence of some positive integer lesser than k with this property will violate the definition of $\phi(n+1)$), k must be a factor of $p^2 + 1$. ■

Lemma 3.4

$\phi(n)$ is a factor of $(p^2+1)^{n-1} \ \forall \ n \geq 3$.

Proof by induction on n

(I) Proof for $n = 3$

We have

$$p^4 = (p^2+1)(p^2-1) + 1 \equiv 1 \ (mod \ p^2 + 1)$$

Hence, $\phi(1) = 4$ (using *Lemma 3.1* and the definition of $\phi(1)$).

Assume $\phi(2) = 4k$ for some $q \in \mathbb{N}$ (using *Lemma 3.1*). Also, we have $k \,|\, p^2+1$ (using *Lemma 3.3*). Using (4) (from the proof for *Lemma 3.3*), we have

$$\frac{p^4 - 1}{p^2 + 1} \times k \equiv 0 \ (mod \ p^2 + 1)$$

$$\implies (p^2 - 1) \times k \equiv 0 \ (mod \ p^2 + 1) \tag{5}$$

Since p is odd, $p^2 - 1$ and $p^2 + 1$ are multiples of 2. More importantly, $p^2 - 1$ is a multiple of 4 (since all odd numbers have a residue of 1, 3 or 5 modulo 6), whereas $p^2 + 1$ is an odd multiple of 2.

Hence, it suffices for k to be a factor of $\frac{p^2+1}{2}$ for (5) to hold. Hence, $\phi(2)$ is a factor of $2(p^2+1)$.

Assume that $\phi(3) = 4kk'$, for some $k' \in \mathbb{N}$ (using *Lemma 3.3*). Hence, (4) (from the proof *Lemma 3.3*) yields

$$\frac{p^{4k} - 1}{(p^2+1)^2} \times k' \equiv 0 \ (mod \ p^2 + 1) \tag{6}$$

Note that k' is also the smallest positive integer which satisfies (6) (by definition of $\phi(3)$).

p is odd, so that must mean that p^4 (and hence, p^{4k}) leaves residue 1 modulo 16. Moreover, since p^2+1 is an odd multiple of 2, this must mean that $\frac{p^{4k}-1}{(p^2+1)^2}$ is a multiple of 4. Hence, it suffices for k' to be a factor of $\frac{p^2+1}{2}$ for (6) to hold. Hence, $4kk' = \phi(3)$ is a factor of $(p^2+1)^2$, as desired.

(II) Proof for $n+1$ assuming true for n
Assume that $\phi(n)$ is a factor of $(p^2+1)^{n-1}$ for some $n \geq 3$. Hence, *Lemma 3.3* implies that $\phi(n+1)$ must be a factor of $(p^2+1)^n$, as desired. ■

Lemma 3.5
$t_m \equiv t_n \ (mod \ \phi(n+1)) \ \forall \ m \geq n \geq 0$.

Proof by induction on n

(I) Proof for $n = 0$
Consider the following pair of mutually exclusive cases which cover all possibilities. Also, recall that $\phi(1) = 4$.

Case a : $p \equiv 1 \ (mod \ 4)$
In this case, $t_m \equiv 1 \ (mod \ 4) \ \forall \ m \geq 0$, hence proving the desired result.

Case b : $p \equiv -1 \ (mod \ 4)$
In this case, $t_m \equiv -1 \ (mod \ 4) \ \forall \ m \geq 0$ (since t_k is odd $\forall \ k \in \mathbb{N}_0$), hence proving the desired result.

(II) Proof for $n = 1$ by induction on m
It's trivially true for $m = 1$. We shall now prove it for $m+1$ assuming it's true for some $m \geq 1$. The induction hypothesis guarantees that

$$t_m \equiv t_1 \ (mod \ \phi(2))$$

$$\implies p^{t_m} \equiv p^{t_1} \ (mod \ (p^2+1)^2)$$

$$\implies t_{m+1} \equiv t_2 \ (mod \ (p^2+1)^2) \tag{7}$$

$\phi(2)$ is a factor of $2(p^2+1)$, so that must mean that it's also a factor of $(p^2+1)^2$ (since p^2+1 is even). Hence, the desired result is trivially implied from (7).

(III) Proof for $n \geq 2$ assuming true for $n-1$
The induction hypothesis guarantees that

$$t_m - t_{n-1} \equiv 0 \ (mod \ \phi(n)) \ \forall \ m \geq n-1$$

$$\implies p^{t_m - t_{n-1}} \equiv 1 \ (mod \ (p^2+1)^n)$$

$$\implies p^{t_m - t_{n-1}} \equiv 1 \ (mod \ \phi(n+1)) \text{ (by } \textit{Lemma 3.4}\text{)}$$

$$\implies p^{t_m} \equiv p^{t_{n-1}} \ (mod \ \phi(n+1))$$

$$\implies t_m \equiv t_n \ (mod \ \phi(n+1)) \ \forall \ m \geq n \ \blacksquare$$

4 Proving the final result

Lemma 3.5 grants us

$$t_m \equiv t_n \ (mod \ \phi(n+1)) \ \forall \ m \geq n \geq 0$$

$$\implies p^{t_m} \equiv p^{t_n} \ (mod \ (p^2+1)^{n+1}) \ \forall \ m \geq n \geq 0$$

$$t_{m+1} \equiv t_{n+1} \ (mod \ (p^2+1)^{n+1}) \ \forall \ m \geq n \geq 0$$

$$t_m \equiv t_n \ (mod \ (p^2+1)^n) \ \forall \ m \geq n \geq 1 \ \blacksquare$$