On a Modular Property of Tetration

Pranjal Jain
Indian Institute of Science Research and Education, Pune
pranjal.jain@students.iiserpune.ac.in

Abstract

This paper generalizes problem 3 of the 2019 PROMYS exam, which asks to show that the last 10 digits (in base 10) of the n-th tetration of 3 are independent of n if $n > 10$. The generalization shows that given any positive integers a and b satisfying certain conditions, the last n digits (in base b) of the m-th tetration of a are independent of m if $m > n$.

We use numerical patterns as a guide towards the solution and explore an additional numerical pattern which shows a relation between decimal expansions and multiplicative inverses of powers of 3 modulo powers of 10.

Keywords : tetration, modular arithmetic
2020 Mathematics Subject Classification : 11A05 , 11A63

Introduction

Definition 1. $\mathbb{N} = \{1, 2, \ldots\}$, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$

Definition 2. Define $mod_x(y) \in \mathbb{N}$ (for integers x and y, with $x \neq 0$) to be the smallest positive integer s.t. (such that)

$$mod_x(y) \equiv y \pmod{x}$$

Definition 3. For $x, y, n \in \mathbb{N}$ with $y > 1$ and x, y co-prime, define $\alpha_{x,y}(n)$ to be the smallest positive integer s.t.

$$a^{\alpha_{x,y}(n)} \equiv 1 \pmod{y^n}$$

Remark. The proof of existence of $\alpha_{x,y}(n)$ follows from the fact that the sequence $\left\{mod_{y^n}(x^i)\right\}_{i\in\mathbb{N}}$ is periodic and x and y are co-prime.

Definition 4. Given any $x \in \mathbb{N}$, let $f(x) \in \mathbb{N}_0$ be the largest integer s.t. $2^{f(x)}$ is a factor of x.

Problem definition
Let $a, b \in \mathbb{N}$ satisfying the following conditions

- a and b are co-prime.
- $0 < f(b) < f(a^2 - 1)$.
- $\alpha_{a,b}(1)$ is a power of 2.
- $a \equiv 1 \pmod{\alpha_{a,\alpha_{a,b}(1)}(1)}$.

Remark. A few examples of cases which satisfies all these criteria :

- $a > 1$ is any odd integer and $b = a^2 + 1$.
- $a > 1$ is any odd integer and $b = \frac{a^2-1}{2^k}$ for $0 < k < f(a^2 - 1)$.
- $a > 1$ is co-prime with b, $\frac{b}{2^{f(b)}} > 1$ is square-free and has only Fermat Primes as prime factors, and $a \equiv 1 \pmod{\alpha_{a,\alpha(1)}(1)}$. The last condition can be framed in a simpler way with some loss of generality by saying $a \equiv 1 \pmod{\phi(\phi(b))}$, where ϕ is the Euler Totient Function.

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

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

We shall show that given any $n, m \in \mathbb{N}$, with $m \geq n$,

$$t_m \equiv t_n \pmod{b^n}$$

The original question from PROMYS 2019 only considered special case of $a = 3$ and $b = n = 10$.

In §1 we show several numerical patterns for the case $a = 3, b = 10$ in quantities which are closely related to the set-up. These patterns are then explained and generalised in the theorems proved in §2 and §3, some of which help us generalise the PROMYS question.

§2 builds up to prove the generalisation of the PROMYS question, and §3 proves a result explaining numerical patterns which does not help in

the proof but is interesting on its own. This result gives a connection of the base-b expansion of $1-\frac{1}{a^k}$ and the modular multiplicative inverse of a^k modulo b^n.

1 Some Curious Patterns in the Numbers

First, let us explore what values we obtain for $\alpha_{a,b}(n)$ for some trial values of a, b and n, since $\alpha_{a,b}(n)$ will play a pivotal role in proving the result we're after. For this section we will let $\alpha(n)$ be the short-hand for $\alpha_{3,10}(n)$.

n	$\alpha(n)$
1	4
2	20
3	100
4	500

So far, the pattern seems like a geometric progression with common ratio 5 (for general values of b, this would suggest that the common ratio is $\frac{b}{2}$). However, this pattern doesn't last beyond this point. Following are some more values to demonstrate this.

n	$\alpha(n)$
5	5×10^3
6	5×10^4
7	5×10^5
8	5×10^6
9	5×10^7

The most conservative conjecture regarding this pattern would be saying that $\alpha(n+1)$ is a multiple of $\alpha(n)$. We prove this in *Lemma 2*, and then strengthen this result by proving in *Theorem 1* that $\frac{\alpha(n+1)}{\alpha(n)}$

is also a factor of b.

A slightly bolder conjecture would be that for large n we must have $\frac{\alpha(n+1)}{\alpha(n)} = b$. Although we do not prove that here, a trivial consequence of *Theorems 2* and *3* that there is some N s.t. $\frac{\alpha(n+1)}{\alpha(n)}$ is odd for all $n < N$, and is an odd multiple of $2^{f(b)}$ for all $n > N$.

One might also notice a connection between the powers of b and the values of $\alpha(n)$, namely that for $n < 3$, $\alpha(n)$ is 'pretty close' to being a factor of 10^{n-1} and for $n \geq 3$, it is a factor of 10^{n-1}. This holds in general and is pivotal in proving the generalised version of the PROMYS question; we frame and prove it formally as *Theorem 4*.

Now, we will explore what happens just before the sequence $\left\{mod_{b^n}(a^i)\right\}_{i\in\mathbb{N}}$ falls to 1 and starts repeating, i.e. we look at numbers of the form $mod_{b^n}\left(a^{\alpha_{a,b}(n)-k}\right)$, with $n, k \in \mathbb{N}$ and $k \leq \alpha_{a,b}(n)$. Below are some values for the case $a = 3, b = 10$.

	$n=1$	$n=2$	$n=3$	$n=4$	$n=5$	$n=6$
$k=1$	7	67	667	6667	66667	666667
$k=2$	9	89	889	8889	88889	888889
$k=3$	3	63	963	2963	62963	962963
$k=4$	1	21	321	4321	54321	654321
$k=5$	—	7	107	8107	18107	218107

The values for $k = 1, 2$ most certainly look suggestive, if not familiar! One might notice a connection with the decimal expansions of $\frac{2}{3}$ and $\frac{8}{9}$. In fact, all of these values are related to the decimal expansion of $1 - \frac{1}{3^k}$ for the respective values of k.
As we can see, the pattern seems to be that $mod_{b^n}\left(a^{\alpha(n)-k}\right)$ is given by the last n digits in the recurring part of the base b expansion of $1 - \frac{1}{a^k}$, with the last digit being increased by 1. If the recurring part is too short (for example, consider $n = 5, k = 3$), we simply extend it by adding as many repetitions as necessary. This pattern turns out to hold in general, and is proved as *Theorem 5*. This pattern also gives an interesting way of finding modular multiplicative inverses.

k	$1-\frac{1}{3^k}$
1	$0.666666\bar{6}$
2	$0.888888\bar{8}$
3	$0.962\overline{962}$
4	$0.\overline{987654321}$
5	$0.\overline{99\ldots218106}$

Another thing one may wonder about is that what if the last digit of the recurring part is 9? Do we convert it to 0 or do we consider carry-overs? *Theorem 5* saves us the trouble and shows that the last digit can never be 9 in the first place!

2 Solving the Generalised Problem

For this section, we will assume the following.

- $a, b \in \mathbb{N}$ are co-prime integers. $n \in \mathbb{N}$.
- $b = 2^p r$ where $p \in \mathbb{N}$ and r is odd. Hence, $f(b) = p$.
- $\alpha_{a,b}(n) = \alpha(n)$.
- $\alpha(1) = 2^q$ and $a \equiv 1 \pmod{\alpha_{a,\alpha(1)}(1)}$.
- $f(a^2 - 1) = t$ for some $t \in \mathbb{N}$ with $t > p$.
- $j_n = \dfrac{a^{\alpha(n)} - 1}{b^n}$.

Lemma 1. *Given any* $c, d \in \mathbb{N}_0$, $a^c \equiv a^d \pmod{b^n}$ *iff* $c \equiv d \pmod{\alpha(n)}$.

Lemma 2. $\alpha(n+1)$ *is a multiple of* $\alpha(n)$.

Proof.

$$a^{\alpha(n+1)} \equiv 1 \pmod{b^{n+1}}$$
$$\implies a^{\alpha(n+1)} \equiv 1 \pmod{b^n}$$
$$\implies \alpha(n+1) \equiv 0 \pmod{\alpha(n)} \text{ (using } \textit{Lemma 1}\text{)} \quad \square$$

Theorem 1. *$\alpha(n+1) = k\alpha(n)$ where $k \in \mathbb{N}$ is the smallest factor of b s.t. $j_n k \equiv 0 \pmod{b}$.*

Proof. By *Lemma 2*, there is some $k \in \mathbb{N}$ s.t. $\alpha(n+1) = k\alpha(n)$. Hence, we have

$$\frac{a^{\alpha(n)} - 1}{b^n} = j_n \in \mathbb{N}$$

$$\frac{a^{k\alpha(n+1)} - 1}{b^{n+1}} \in \mathbb{N}$$

$$\iff \frac{a^{\alpha(n)} - 1}{b^n} \times \frac{1 + a^{\alpha(n)} + a^{2\alpha(n)} + \ldots + a^{(k-1)\alpha(n)}}{b} \in \mathbb{N}$$

$$\iff j_n \left(1 + a^{\alpha(n)} + a^{2\alpha(n)} + \ldots + a^{(k-1)\alpha(n)}\right) \equiv 0 \pmod{b}$$

We know that $a^{m\alpha(n)} \equiv 1 \pmod{b}$ $\forall\ m \in \mathbb{N}_0$ and $n \in \mathbb{N}$. Hence,

$$j_n k \equiv 0 \pmod{b}$$

Since k is the smallest positive integer satisfying this relation (by definition of $\alpha(n+1)$), the proof is complete. □

Identity 1.

$$x^{2^k} - 1 = (x-1) \prod_{i=0}^{k-1} (x^{2^i} + 1) \ \forall\ k \in \mathbb{N}$$

Proof. The identity is clearly true for $k = 1$. Since $x^{2^k} - 1 = (x^{2^{k-1}} - 1)(x^{2^{k-1}} + 1)$ $\forall\ k \in \mathbb{N}$, induction proves it for all $k \in \mathbb{N}$. □

Corollary 1 (Identity 1)**.** *If $x, k \in \mathbb{N}$, $x > 1$, then $f(x^{2^k} - 1) = f(x^2 - 1) + k - 1$.*

Proof. The statement is clearly true if x is even or $k = 1$. For x odd and $k > 1$, notice that $x^2 \equiv 1 \pmod{4}$ and so $x^{2^i} \equiv 1 \pmod{4}$ $\forall\ i \in \mathbb{N}$. Hence, $x^{2^i} + 1$ is an odd multiple of 2 for all $i \in \mathbb{N}$. By *Identity 1*, we have

$$x^{2^k} - 1 = (x^2 - 1) \prod_{i=1}^{k-1} (x^{2^i} + 1)$$

Hence, the result follows. □

Lemma 3. *Let $x, y \in \mathbb{N}$ be odd integers.Then, $f(x^{2y}-1) = f(x^2-1)$.*

Proof.

$$\begin{aligned}(x^{2y}-1) &= (x^y+1)(x^y-1)\\ &= (x^2-1)(1-x+x^2-...+x^{y-1})(1+x+x^2+..+x^{y-1})\end{aligned}$$

To justify the last line, recall that y is odd. Now, we have

$$1-x+x^2-...+x^{y-1} \equiv 1+x+x^2+..+x^{y-1} \equiv 1 \pmod 2$$

Hence, the desired result follows. □

Corollary 2. *(Corollary 1, Lemma 3)*

$$f(j_n) = f(\alpha(n)) + t - 1 - np$$

Theorem 2. *For all $n \leq \left\lfloor \frac{q+t-1}{p} \right\rfloor$, we have that $f(\alpha(n)) = q$ and $\frac{\alpha(n)}{2^q}$ is a factor of r^{n-1}.*

Proof. Define the statement $s(n)$="$n > \left\lfloor \frac{q+t-1}{p} \right\rfloor$ or $\frac{\alpha(n)}{2^q}$ is a factor of r^{n-1}". We will show by induction that $s(n)$ is true for all $n \in \mathbb{N}$.

Clearly, $s(1)$ is true. We will now show that $s(n) \implies s(n+1)$.If $n \geq \left\lfloor \frac{q+t-1}{p} \right\rfloor$, the proof is complete. Hence, assume $0 < n < \left\lfloor \frac{q+t-1}{p} \right\rfloor$.

Now, we know from *Theorem 1* that $\frac{\alpha(n+1)}{\alpha(n)} = k$ is the smallest possible integer s.t. $j_n k \equiv 0 \pmod b$. Hence, showing that there is some odd k satisfying $j_n k \equiv 0 \pmod b$ will complete the proof.

By the induction hypothesis and using *Corollary 2*, $f(j_n) = q + t - 1 - pn$. Since $n < \left\lfloor \frac{q+t-1}{p} \right\rfloor$, we have $(q+t-1) - pn \geq p$. Hence, it suffices for k to be odd and the proof is complete. □

Theorem 3. *For all* $n > \left\lfloor \frac{q+t-1}{p} \right\rfloor$, $f(\alpha(n)) = np-(t-1)$ *and* $\frac{\alpha(n)}{2^{np-(t-1)}}$ *is a factor of* r^{n-1}.

Proof. Let $m = \left\lfloor \frac{q+t-1}{p} \right\rfloor$. We know that $f(j_m) = (q+t-1) - mp < p$ and $f(\alpha(m)) = q$ (by *Corollary 2*). Hence, *Theorem 1* yields

$$\begin{aligned} f\left(\frac{\alpha(m+1)}{\alpha(m)}\right) &= p - f(j_m) \\ f(\alpha(m+1)) &= f(\alpha(m)) + f\left(\frac{\alpha(m+1)}{\alpha(m)}\right) \\ &= (m+1)p - (t-1) \end{aligned}$$

By *Theorem 2*, $\frac{\alpha(m)}{2^q}$ is a factor of r^{m-1}. Hence, by *Theorem 1* and the equation above, we must have that $\frac{\alpha(m+1)}{2^{(m+1)p-(t-1)}}$ is a factor of r^m. Hence, the claim holds for $n = m+1$. By *Theorem 1*, induction proves the claim for all $n > m+1$ as well. □

Corollary 3 (Theorem 3)**.** *For all* $n > \left\lfloor \frac{q+t-1}{p} \right\rfloor$, $\alpha(n)$ *is a factor of* b^{n-1}.

Proof. By *Theorem 3*, we know that for all $n \leq \left\lfloor \frac{q+t-1}{p} \right\rfloor$, we have $f(\alpha(n)) = np - (t-1) \leq (n-1)p$ (since $t > p$). Hence, the fact that $\frac{\alpha(n)}{2^{f(\alpha(n))}}$ is a factor of r^{n-1} (by *Theorem 3*) proves the desired result. □

Theorem 4. $t_n \equiv t_m \pmod{\alpha(n+1)}$ $\forall\ m, n \in \mathbb{N}_0$ *with* $m \geq n$.

Proof. We will prove the claim by induction on n. Let $s(n)$ be the induction hypothesis "$t_n \equiv t_m \pmod{\alpha(n+1)}$ $\forall\ m \geq n$".

(I) For $n = 0$
We will use induction on m. The claim is clearly true for $m = 0$. For $m = 1$, we have

$$\begin{aligned} a &\equiv 1 \pmod{\alpha_{a,\alpha(1)}(1)} \\ \implies t_1 = a^a \equiv a = t_0 &\pmod{\alpha(1)} \end{aligned}$$

Hence, the claim is true for $m = 1$. For induction, assume that it is true for some $m \geq 1$ and we will now prove it for $m+1$.

$$t_m \equiv t_0 \pmod{\alpha(1)} \text{ (induction hypothesis)}$$

$$\implies t_m \equiv t_0 \pmod{2^q}$$
$$\implies t_m \equiv t_0 \pmod{2^{q-1}}$$
$$\implies a^{t_m} \equiv a^{t_0} \pmod{2^q}$$

The last line uses the fact that $\phi(2^q) = 2^{q-1}$, where ϕ is the Euler Totient Function. Hence,

$$t_{m+1} \equiv t_1 \equiv t_0 \pmod{2^q}$$

This completes the proof.

(II) For $n \geq 1$ assuming true for $n-1$
Case 1 : $n \leq \left\lfloor \frac{q+t-1}{p} \right\rfloor$

$$t_m \equiv t_{n-1} \pmod{\alpha(n)} \ \forall\ m \geq n-1 \text{ (by } s(n-1))$$
$$\implies t_{m+1} \equiv t_n \pmod{b^n} \ \forall\ m \geq n-1$$
$$\implies t_m \equiv t_n \pmod{b^n} \ \forall\ m \geq n \tag{1}$$

$$t_m \equiv t_{n-1} \equiv t_n \pmod{\alpha(n)} \ \forall\ m \geq n \text{ (by } s(n-1)) \tag{2}$$

By (1) and (2), we see that for all $m \geq n$, $t_m - t_n$ must be a multiple of the least common multiple of $\alpha(n)$ and $b^n = 2^{np} \times r^n$. If $n = \left\lfloor \frac{q+t-1}{p} \right\rfloor$, then by *Corollary 3* $\alpha(n+1)$ is a factor of b^n, proving the desired result. If $n < \left\lfloor \frac{q+t-1}{p} \right\rfloor$, $f(\alpha(n+1)) = q = f(\alpha(n))$. Hence, by *Theorem 2* the desired result follows.

Case 2 : $n > \left\lfloor \frac{q+t-1}{p} \right\rfloor$
Clearly, (1) holds in this case as well (since it only uses the definition of $\alpha(n)$). Hence, by *Corollary 3* the result follows. □

Now, the solution to the generalisation of the PROMYS problem follows as a corollary to *Theorem 4*.

Corollary 4 (Theorem 4)**.**

$$t_m \equiv t_n \pmod{b^n} \ \forall\ m, n \in \mathbb{N} \text{ with } m \geq n$$

Proof. Theorem 4 grants us

$$t_{m-1} \equiv t_{n-1} \pmod{\alpha(n)} \ \forall\ m \geq n \geq 1$$

$$\implies t_m \equiv t_n \pmod{b^n} \ \forall\ m \geq n \geq 1 \quad \square$$

3 Decimal Expansions and Modular Multiplicative Inverses

The theorems of §2 were proved in order to build up to the generalisation of the PROMYS question. Although they explained most of the numerical patterns observed in §1, one remains unexplained. In this section, we explain and generalise the pattern related to the base b expansion of $1 - \frac{1}{a^k}$. We will be only assume a and $b > 1$ to be co-prime henceforth.

Definition 5. Given any $x \in \mathbb{R}$, let $[x]$ denote the base b expansion of x. Given any $k \in \mathbb{Z}$, let $[x]_k$ denote the coefficient of b^k in $[x]$. Let $[x]_k^- = [x]_{-k}$.

Definition 6. Given any $x \in \mathbb{Q}$, let $P(x)$ be the length of the recurring part of the base b expansion of the fractional part of x. For example, if $b = 10$ then we have $P(1) = P(\frac{1}{3}) = 1$ and $P(\frac{8}{7}) = 6$.

Theorem 5. *For all $a, b, n, k \in \mathbb{N}$ with a, b co-prime, $b > 1$ and $k \leq \alpha_{a,b}(n)$, the last n digits (in base b) of $a^{\alpha_{a,b}(n)-k}$ are given (from left to right) by $[x]_{c-n+1}^-$, $[x]_{c-n+2}^-$, $\ldots [x]_{c-1}^-$, $[x]_c^- + 1$, where $x = 1 - \frac{1}{a^k}$ and $c = P(x)\left\lceil \frac{n}{P(x)} \right\rceil$. Formally,*

$$a^{\alpha_{a,b}(n)-k} \equiv \sum_{i=0}^{n-1} [x]_{c-i}^- b^i + 1 \pmod{b^n}, \ [x]_c^- < b - 1$$

Proof. To find the base b expansion of $\frac{1}{a^k}$, we will show that there are $s, t \in \mathbb{N}_0$ with $s < b^t$ which satisfy

$$\frac{1}{a^k} = \sum_{i=1}^{\infty} \frac{s}{b^{it}} \tag{3}$$

Note that the use of t here is not the same as in §2. Hence, we have

$$1 - \frac{1}{a^k} = \sum_{i=1}^{\infty} \frac{b^t - 1}{b^{it}} - \sum_{i=1}^{\infty} \frac{s}{b^{it}} = \sum_{i=1}^{\infty} \frac{b^t - 1 - s}{b^{it}}$$

Hence, the base b expansion of $x = 1 - \frac{1}{a^k}$ will be given by

$$1 - \frac{1}{a^k} = \sum_{i=0}^{\infty} \sum_{j=1}^{t} \frac{[b^t - 1 - s]_{t-j}}{b^{it+j}} = \sum_{i=0}^{\infty} \sum_{j=1}^{t} \frac{b - 1 - [s]_{t-j}}{b^{it+j}}$$

$$[x]_m^- = b - 1 - [s]_{t-mod_t(m)} \tag{4}$$

To find s and t, (3) yields

$$\frac{1}{a^k} = \frac{s}{b^t - 1}$$

$$\implies sa^k = b^t - 1$$

$$\implies b^t \equiv 1 \pmod{a^k}$$

By Euler's Totient Theorem, we know that $t = r\phi(a^k)$ (where ϕ is the totient function) satisfies the last congruence for every $r \in \mathbb{N}$. Hence, we may assume $r = n + 1$ to get

$$t = (n+1)\,\phi\left(a^k\right),\ s = \frac{b^t - 1}{a^k}$$

We also have that $t > n$ is a period (not necessarily the fundamental period) of the fractional part of the base b expansions of $\frac{1}{a^k}$ and x, so our problem reduces to proving that

$$a^{\alpha_{a,b}(n)-k} \equiv \sum_{i=0}^{n-1} [x]_{t-i}\, b^i + 1 \pmod{b^n},\ [x]_t < b - 1$$

Using (4), we see that we need to prove

$$a^{\alpha_{a,b}(n)-k} \equiv \sum_{i=0}^{n-1} \left(b-1-[s]_{t-mod_t(t-i)}\right) b^i + 1 \pmod{b^n},\ [s]_0 > 0$$

Since $n < t$, this reduces to showing

$$a^{\alpha_{a,b}(n)-k} \equiv \sum_{i=0}^{n-1} \left(b-1-[s]_i\right) b^i + 1 \pmod{b^n},\ [s]_0 > 0$$

We can see that $[s]_0 > 0$ by simply noticing that s is not a multiple of b. We will now show that the congruence holds.

$$\sum_{i=0}^{n-1} \left(b-1-[s]_i\right) b^i + 1 \equiv b^n - s \pmod{b^n}$$

$$b^n - s \equiv -s \pmod{b^n}$$

$$-s = -\frac{b^t-1}{a^k}$$

$$\implies a^k \times \left(\sum_{i=0}^{n-1} \left(b-1-[s]_i\right) b^i + 1\right) \equiv 1 \pmod{b^n}$$

$$\implies a^k \times \left(\sum_{i=0}^{n-1} \left(b-1-[s]_i\right) b^i + 1\right) \equiv a^{\alpha_{a,b}(n)} \pmod{b^n}$$

$$\implies \sum_{i=0}^{n-1} \left(b-1-[s]_i\right) b^i + 1 \equiv a^{\alpha_{a,b}(n)-k} \pmod{b^n} \quad \square$$