Modular Exponentiation Identities in Number Theory: Classification and Minimal Exponents

Subhraneel Dutta
Srihan Dutta

Abstract

This paper investigates two specific modular exponentiation identities involving fixed integers. First, we determine the set of non-negative integers m satisfying $a^N \equiv a^m \pmod{N}$ for a fixed $N > 1$ and all integers a, deriving the minimum such m. Second, we analyze the minimum positive integer n such that $a^{mn} \equiv a^n \pmod{x}$ holds for a fixed $x > 1$ and all integers a, m. We provide explicit formulas for these minimal exponents in terms of the prime factorization exponents and the Carmichael function $\lambda(\cdot)$.

1 Introduction

Modular exponentiation is a cornerstone of elementary number theory and cryptography. While Fermat's Little Theorem and Euler's Theorem provide conditions for $a^{\phi(n)} \equiv 1 \pmod{n}$ when $\gcd(a, n) = 1$, general identities valid for *all* integers a (including those not coprime to the modulus) require more careful analysis of prime power divisors.

In this paper, we utilize the Carmichael function $\lambda(n)$ and p-adic valuations to solve two minimization problems.

1.1 Preliminaries and Notation

Let the prime factorization of a positive integer K be given by:

$$K = \prod_{i=1}^{r} p_i^{e_i}$$

We define the following parameters relative to K:

- $E(K) = \max_{1 \leq i \leq r}\{e_i\}$ is the maximum exponent in the prime factorization.
- $\lambda(K)$ denotes the Carmichael function, defined as $\operatorname{lcm}(\lambda(p_1^{e_1}), \ldots, \lambda(p_r^{e_r}))$, where:

  Definition 1 (Carmichael Function for Prime Powers)**.** *The Carmichael function $\lambda(n)$ is defined for prime powers as follows:*

$$\lambda(p^r) = \begin{cases} p^{r-1}(p-1) & \text{if } p \geq 3 \text{ is an odd prime, } r \geq 1 \\ 1 & \text{if } p = 2, r = 1 \\ 2 & \text{if } p = 2, r = 2 \\ 2^{r-2} & \text{if } p = 2, r \geq 3 \end{cases} \tag{1}$$

- $v_p(x)$ denotes the p-adic valuation of x, defined as the largest integer k such that $p^k \mid x$.
- $\lceil x \rceil$ denotes the ceiling function (least integer greater than or equal to x).

2 Part I: The First Identity

2.1 Problem Statement

For a fixed integer $N > 1$, we seek to classify all non-negative integers m such that:

$$a^N \equiv a^m \pmod{N} \quad \text{for all } a \in \mathbb{Z} \tag{2}$$

and to determine the minimum such value $m_{\min}$.

2.2 Main Result

Theorem 1. *Let $N = \prod_{i=1}^{r} p_i^{e_i}$. Let $E = \max(e_i)$ and $L = \lambda(N)$. The minimum non-negative integer m satisfying $a^N \equiv a^m \pmod{N}$ for all a is given by:*

$$m_{\min} = N + \left\lceil \frac{E - N}{L} \right\rceil \cdot L$$

Proof. The congruence $a^N \equiv a^m \pmod{N}$ is equivalent to $a^N - a^m \equiv 0 \pmod{p_i^{e_i}}$ for each factor ${p_i}^{e_i}$ of N. This implies:

$$a^m(a^{N-m} - 1) \equiv 0 \pmod{p_i^{e_i}}$$

Case 1: $\gcd(a, p_i) = 1$
If a is coprime to p_i, then a^m is a unit modulo $p_i^{e_i}$. The condition simplifies to:

$$a^{N-m} \equiv 1 \pmod{p_i^{e_i}}$$

By the definition of the Carmichael function, the exponent must be a multiple of $\lambda(p_i^{e_i})$. For this to hold for all a, we must have:

$$\lambda(p_i^{e_i}) \mid (N - m)$$

Since $L = \operatorname{lcm}_i(\lambda(p_i^{e_i}))$, this implies:

$$N \equiv m \pmod{L}$$

Case 2: $p_i \mid a$
Let $a = p_i^k \cdot u$ where $\gcd(u, p_i) = 1$ and $k \geq 1$. The p-adic valuation of the expression is:

$$v_{p_i}(a^N - a^m) = v_{p_i}(a^m(a^{N-m} - 1))$$

Since $p_i \mid a$, $a^{N-m} - 1$ is not divisible by p_i (assuming $N \neq m$, otherwise trivial). Thus, the valuation is determined entirely by a^m:

$$v_{p_i}(a^m) = m \cdot v_{p_i}(a) = m \cdot k$$

For the congruence to hold modulo $p_i^{e_i}$, we require $mk \geq e_i$ for all $k \geq 1$. The strictest constraint occurs at $k = 1$, yielding:

$$m \geq e_i$$

Since this must hold for all i, we derive:

$$m \geq \max(e_i) = E$$

Therefore,
Combining both cases, the set of valid m is:

$$\{m \in \mathbb{Z}_{\geq 0} \mid m \geq E \text{ and } m \equiv N \pmod{L}\}$$

This forms an arithmetic progression $m = N + kL$. We seek the smallest integer k such that:

$$N + kL \geq E \implies kL \geq E - N \implies k \geq \frac{E - N}{L}$$

Since k must be an integer, $k_{\min} = \lceil (E - N)/L \rceil$. Substituting this back yields the theorem. □

3 Part II: The Second Identity

3.1 Problem Statement

For a fixed integer $x > 1$, we seek the minimum positive integer n such that:

$$a^{mn} \equiv a^n \pmod{x} \quad \text{for all } a, m \in \mathbb{Z} \tag{3}$$

3.2 Main Result

Theorem 2. *Let $x = \prod_{i=1}^{r} p_i^{e_i}$, with $E = \max(e_i)$. The minimum positive integer n satisfying the condition is:*

$$n_0 = \lambda(x) \cdot \left\lceil \frac{E}{\lambda(x)} \right\rceil$$

Proof. The condition is equivalent to $a^{mn} - a^n \equiv 0 \pmod{p_i^{e_i}}$ for all i. Factoring the expression:

$$a^n(a^{(m-1)n} - 1) \equiv 0 \pmod{p_i^{e_i}}$$

Case 1: $\gcd(a, p_i) = 1$
If a is coprime to p_i, a^n is invertible. We require:

$$a^{(m-1)n} \equiv 1 \pmod{p_i^{e_i}}$$

For this to hold for *any* integer m, the exponent $(m-1)n$ must be a multiple of $\lambda(p_i^{e_i})$ regardless of the value of $(m-1)$. This implies that n itself must be divisible by $\lambda(p_i^{e_i})$:

$$\lambda(p_i^{e_i}) \mid n$$

Consequently, $\lambda(x) \mid n$.

Case 2: $p_i \mid a$
Let $a = p_i$. Then $p_i \nmid (a^{(m-1)n} - 1)$. The valuation is:

$$v_{p_i}(a^{mn} - a^n) = v_{p_i}(a^n) = n$$

To satisfy the congruence modulo $p_i^{e_i}$, we must have $n \geq e_i$. This must hold for all i, so:

$$n \geq E$$

Therefore,
We require n to be a multiple of $\lambda(x)$ such that $n \geq E$. Let $n = k \cdot \lambda(x)$.

$$k \cdot \lambda(x) \geq E \implies k \geq \frac{E}{\lambda(x)}$$

The minimum integer k is $\lceil E/\lambda(x) \rceil$. Therefore, $n_0 = \lambda(x) \cdot \lceil E/\lambda(x) \rceil$. □

4 Numerical Examples

In this section, we verify the main theorems using specific values of N and x.

4.1 Examples for Part I: Minimal Exponent m

We examine the identity $a^N \equiv a^m \pmod{N}$ and the formula $m_{\min} = N + \lceil (E-N)/L \rceil \cdot L$.

Example 1 ($N = 12$)**.** *Let* $N = 12 = 2^2 \cdot 3^1$.

- ***Parameters:*** $E = \max(2, 1) = 2$.
- ***Carmichael Function:*** $\lambda(2^2) = 2$, $\lambda(3) = 2 \implies L = lcm(2, 2) = 2$.
- ***Theorem Calculation:***

$$m_{\min} = 12 + \left\lceil \frac{2-12}{2} \right\rceil \cdot 2 = 12 + (-5)(2) = 2$$

  The theorem predicts $m \geq 2$ *and* $m \equiv 12 \equiv 0 \pmod{2}$. *Thus, any even* $m \geq 2$ *works.*

- ***Verification:*** *Let* $a = 5$.

$$5^{12} \equiv 1 \pmod{12}, \quad 5^2 = 25 \equiv 1 \pmod{12}$$

  Since $1 \equiv 1$, *the condition holds.*

Example 2 ($N = 18$)**.** *Let* $N = 18 = 2^1 \cdot 3^2$.

- ***Parameters:*** $E = \max(1, 2) = 2$.
- ***Carmichael Function:*** $\lambda(2) = 1$, $\lambda(3^2) = 6 \implies L = lcm(1, 6) = 6$.
- ***Theorem Calculation:***

$$m_{\min} = 18 + \left\lceil \frac{2-18}{6} \right\rceil \cdot 6 = 18 + \lceil -2.66\ldots \rceil \cdot 6 = 18 + (-2)(6) = 6$$

  The admissible values are $m \in \{6, 12, 18, \ldots\}$.

- ***Verification:*** *Let* $a = 8$.

$$8^{18} \equiv 10 \pmod{18} \quad \textit{and} \quad 8^6 = 262144 \equiv 10 \pmod{18}$$

  The identity holds as predicted.

4.2 Examples for Part II: Minimal Exponent n

We examine the identity $a^{mn} \equiv a^n \pmod{x}$ and the formula $n_0 = \lambda(x) \cdot \lceil E/\lambda(x) \rceil$.

Example 3 ($x = 15$)**.** *Let* $x = 15 = 3^1 \cdot 5^1$.

- ***Parameters:*** $E = \max(1, 1) = 1$.
- ***Carmichael Function:*** $\lambda(3) = 2$, $\lambda(5) = 4 \implies \lambda(15) = 4$.
- ***Theorem Calculation:***

$$n_0 = 4 \cdot \left\lceil \frac{1}{4} \right\rceil = 4 \cdot 1 = 4$$

- ***Verification:*** *Let $a = 7, m = 3$.*

$$7^{12} \equiv 1 \pmod{15} \quad \textit{and} \quad 7^4 \equiv 1 \pmod{15}$$

The congruence holds.

Example 4 ($x = 72$)**.** *Let $x = 72 = 2^3 \cdot 3^2$.*

- ***Parameters:*** $E = \max(3, 2) = 3$.
- ***Carmichael Function:*** $\lambda(2^3) = 2$, $\lambda(3^2) = 6 \implies \lambda(72) = 6$.
- ***Theorem Calculation:***

$$n_0 = 6 \cdot \left\lceil \frac{3}{6} \right\rceil = 6 \cdot 1 = 6$$

- ***Verification:*** *Let $a = 11, m = 3$. We check if $11^{18} \equiv 11^6 \pmod{72}$. Calculation confirms:*

$$11^{18} \equiv 1 \pmod{72} \quad \textit{and} \quad 11^6 \equiv 1 \pmod{72}$$

5 Conclusion

We have explicitly classified the exponents for two general modular identities. The interplay between the maximality of prime exponents (E) and the period of units (L) completely determines the minimal solutions. These results generalize standard cases where a is restricted to units.

Acknowledgements

The authors would like to thank our teachers and friends for their invaluable support, guidance, and encouragement throughout the preparation of this manuscript.

References

[1] R. D. Carmichael, *Note on a new number-theoretic function*, Bulletin of the American Mathematical Society, 16(5), 232-238, 1910.

[2] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 6th ed., Oxford University Press, 2008.

[3] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., John Wiley & Sons, 1991.

[4] K. H. Rosen, *Elementary Number Theory and Its Applications*, 6th ed., Pearson, 2011.