Alabama Journal of Mathematics

Alabama Journal of Mathematics
Volume 49 (1) (2026), 34 – 38

Original Paper

An analogue of Carmichael numbers, or six for infinity

Antonin Jancarik[1], Tomas J. Kepka[2], J. D. Phillips*[3]

[1] *Department of Mathematics and Mathematical Education*
Charles University, Faculty of Education, M. Rettigové 4
116 39 Praha 1, Czech Republic

[2] *Department of Mathematics and Mathematical Education*
Charles University, Faculty of Education, M. Rettigové 4
116 39 Praha 1, Czech Republic

[3] *Department of Mathematics & Computer Science*
Northern Michigan University
Marquette, MI 49855 USA

Abstract

We find all non-negative integers n such that congruence modulo n is stable under exponentiation by positive integers, i.e. we show, that $n = 1, 2, 6, 42, 1806$ are the only numbers for which the condition $a \equiv_n b$ and $c \equiv_n d$ imply that $a^c \equiv_n b^d$, $a, b, c, d \in N$ is satisfied. We also show in what sense this condition is close to the conditions for Carmichael numbers.

Keywords. Fermat's Little Theorem, Dirichlet's Prime Number Theorem, Carmichael numbers, primitive root

Mathematics Subject Classification (2020). 11A99

1. Introduction

We begin by setting notation: let Z be the set of integers, and let N be the set of positive integers. For $n \in Z$, we use the standard notation to denote *congruence modulo* n: for $a, b \in Z$, set $a \equiv_n b$ if and only if $n \mid a - b$. We note, without proof, the following basic facts:

(1) If $a \equiv_n b$ and $c \equiv_n d$, then
  (a) $a + c \equiv_n b + d$,
  (b) $a - c \equiv_n b - d$, and
  (c) $ac \equiv_n bd$;
(2) the congruences $\equiv_n$ and $\equiv_{-n}$ coincide,

*Corresponding Author.
Email address: antonin.jancarik@pedf.cuni.cz, tomas.kepka@pedf.cuni.cz, jophilli@nmu.edu

(3) $\equiv_0$ is the identity equivalence relation id_Z,
(4) $\equiv_1$ is the total equivalence relation $Z \times Z$.

For the balance of the paper, n is an element in Z. Let $n \geq 2$ then $2n \equiv_n n$ and $2 \not\equiv_n 1$, but since $2 = 2n/n$ and $1 = n/n$, the congruence $\equiv_n, n \geq 2$, is never stable under the partial operation of division. What about powers? Obviously, the assignment $(a, b) \to a^b$ is a partial operation on Z, but it is a complete operation on N.

Consider the following condition:

(P1) $a \equiv_n b$ and $c \equiv_n d$ imply that $a^c \equiv_n b^d$, $a, b, c, d \in N$.

Let n satisfy (P1). We have $n+1 \equiv_n 1$ and $a \equiv_n a, a \in N$. Thus, since n satisfies (P1), we have $a^{n+1} \equiv_n a^1$. That is, $n \mid a^{n+1} - a$, and hence, n satisfies:

(P2) $n \mid a^{n+1} - a$ for every positive integer a.

We have shown that (P1) implies (P2). We now show the converse. Let $a \equiv_n b$, $c \equiv_n d$, for positive integers a, b, c, d. We must show that $a^c \equiv_n b^d$. This is clear for $c = d$ (since the congruence $\equiv_n$ is stable under multiplication). Thus, assume that $c > d$. Then $c - d = en$ for some $e \geq 1$ and hence, $c = en + d, a^{ne-1} = (a^n - 1) \cdot (a^{n(e-1)} + \cdots + 1), a^n - 1 \mid a^{ne} - 1, a \mid a^d, a(a^n - 1) \mid a^d(a^{ne} - 1)$, where $a^d(a^{ne} - 1) = a^{ne+d} - a^d = a^c - a^d$. Consequently, $a^{n+1} - a$ divides $a^c - a^d$, and since by (P2), $n \mid a^{n+1} - a$, we therefore have $n \mid a^c - a^d$, i.e., $a^c \equiv_n a^d$. And thus we have (P1) if and only if (P2).

2. Results

We come now to our central question: which positive integers n satisfy (P2)?
Firstly, let us consider $n = 1, 2, \ldots 10$.

(1) $n = 1$ obviously satisfies (P2).
(2) $n = 2$ satisfies (P2), since for each $a \in N$, the numbers a^3 and a possess the same parity (so that the difference $a^3 - a = a(a-1)(a+1)$ is always even).
(3) $n = 3$ does not satisfy (P2), since $2^4 - 2 = 14$ and $3 \nmid 14$.
(4) $n = 4$ does not satisfy (P2), since $2^5 - 2 = 30$ and $4 \nmid 30$.
(5) $n = 5$ does not satisfy (P2), since $2^6 - 2 = 62$ and $5 \nmid 62$.
(6) $n = 6$ satisfies (P2), since $a^7 - a = a(a-1)(a+1)(a^2 + a + 1)(a^2 - a + 1)$ where the prime number 2 divides exactly one of a and $a + 1$ and the prime number 3 divides exactly one of $a, a - 1$, and $a + 1$, and hence $6 \mid a^7 - a$ for every $a \in N$.
(7) $n = 7$ does not satisfy (P2), since $2^8 - 2 = 254$ and $7 \nmid 254$ (as $254 = 7 \cdot 36 + 2$).
(8) $n = 8$ does not satisfy (P2), since $2^9 - 2 = 510 = 8 \cdot 63 + 6, 8 \nmid 2^9 - 2$.
(9) $n = 9$ does not satisfy (P2), since $2^{10} - 2 = 1022 = 9 \cdot 113 + 5, 9 \nmid 2^{10} - 2$.
(10) $n = 10$ does not satisfy (P2), since $2^{11} - 2 = 2046 = 10 \cdot 204 + 6, 10 \nmid 2^{11} - 2$.

Thus, among the integers $1, 2, \ldots, 10$, only 1, 2 and 6 satisfy (P2) (and thus, the equivalent condition (P1) as well). We're not there yet, but hey, it's a start. What about the integers $11, 12$ and beyond?

Let n satisfy (P2), $n \geq 2$. Firstly, we show that n is even. Assume that n is odd. Since n satisfies (P2), we have $n \mid (n-1)^{n+1} - n + 1$ and consequently, $n \mid (n-1)^{n+1} + 1$; that is, $(n-1)^{n+1} + 1 \equiv_n 0$. On the other hand, $n - 1 \equiv_n -1$, and so $(n-1)^{n+1} \equiv_n (-1)^{n+1}$. Since n is odd, $n + 1$ is even and $(-1)^{n+1} = 1$. Thus, $(n-1)^{n+1} \equiv_n 1$ and $(n-1)^{n+1} + 1 \equiv_n 2$. We thus have $0 \equiv_n 2, n \mid 2, n = 2$, a contradiction.

Secondly, we show that n is squarefree. Indeed, if $m \geq 2$, then $n \mid m^{n+1} - m$, where $m^2 \mid m^{n+1}, m^2 \nmid m$, and therefore, $m^2 \nmid n$. Thus, n is squarefree.

We have found that n is a squarefree, even number. The sequence of such numbers commences thusly (A039956):

$$2, 6, 10, 14, 22, 26, 30, 34, 38, 42, 46, 58, 62, 70, 74, 78, 82, 86, 94, 102, \ldots$$

We have shown that 2 and 6 satisfy (P2), but 10 does not. Let us calculate. We have $8 \equiv_7 1, 2^3 = 8, (2^3)^4 \equiv_7 1^4, 2^{12} \equiv_7 1, 2^{14} \equiv_7 4, 7 \mid 2^{14} - 4, 7 \nmid 2^{14} - 1, 14 \nmid 2^{15} - 2, 14$ does not satisfy (P2). Similarly, $2^3 \equiv_{11} -3, 2^6 \equiv_{11} 9 \equiv_{11} -2, 2^{18} \equiv_{11} -8 \equiv_{11} 3, 2^{22} \equiv_{11} 48 \equiv_{11} 4, 2^{22} - 1 \equiv_{11} 3, 11 \nmid 2^{22} - 1, 22 \nmid 2^{23} - 2, 22$ does not satisfy (P2), $2^4 \equiv_{13} 3, 2^{12} \equiv_{13} 27 \equiv_{13} 1, 2^{24} \equiv_{13} 1, 2^{26} \equiv_{13} 4, 2^{26} - 1 \equiv_{13} 3, 13 \nmid 2^{26} - 1, 26 \nmid 2^{27} - 2, 26$ does not satisfy (P2), $2^5 \equiv_{30} 2, 2^{30} \equiv_{30} 2^6 = 2 \cdot 2^5 \equiv_{30} 2^2 = 4, 2^{31} \equiv_{30} 8, 2^{31} - 2 \equiv_{30} 6, 30 \nmid 2^{31} - 2, 30$ does not satisfy (P2), $2^5 \equiv_{34} -2, 2^{30} \equiv_{34} (-2)^6 = 2 \cdot 2^5 \equiv_{34} -4, 2^{35} \equiv_{34} (-4) \cdot 2^5 \equiv_{34} (-4)(-2) = 8, 2^{35} - 2 \equiv_{34} 6, 34 \nmid 2^{35} - 2, 34$ does not satisfy (P2), $2^5 \equiv_{19} -6, 2^{10} \equiv_{19} 36 \equiv_{19} -2, 2^{30} \equiv_{19} -8, 2^{35} \equiv_{19} 48 \equiv_{19} 10, 2^{38} \equiv_{19} 80 \equiv_{19} 4, 2^{38} - 1 \equiv_{19} 3, 19 \nmid 2^{38} - 1, 38 \nmid 2^{39} - 2, 38$ does not satisfy (P2). Further (somewhat laborious) calculations show that none from the numbers $46, 58, 62, 66, 70, 74, 78, 82, 86, 94, 102$ satisfies (P2).

What about 42? Let us calculate! We have $1^6 \equiv_7 1, 2^6 = 64 \equiv_7 1, 3^6 = 27 \cdot 27 \equiv_7 (-1)(-1) = 1, 4^6 = (2^6)^2 \equiv_7 1^2 = 1, 5^6 = 25 \cdot 25 \cdot 25 \equiv_7 4^3 = 2^6 \equiv_7 1$ and $6^6 \equiv_7 (-1)^6 = 1$. If $7 \nmid a$, then $a \equiv_7 1, 2, 3, 4, 5, 6$, and we conclude that $a^6 \equiv_7 1, 7 \mid a^6 - 1$. Consequently, $7 \mid a^7 - a$ for every (positive) integer a. Since $a^{43} - a = (a^7 - a)(a^{36} + a^{30} + a^{24} + a^{18} + a^{12} + a^6 + 1)$, we realize that $7 \mid a^{43} - a$. And since 6 satisfies (P2), we have $6 \mid a^7 - a$, and hence $42 \mid a^{43} - a$. Thus, 42 satisfies (P2).

We now generalize the foregoing. Let $n \geq 1$ satisfy (P2) and, moreover, assume that $n + 1$ is a prime. We claim that $n(n + 1)$ satisfies (P2). For, let $a \geq 1$ be arbitrary. Since n satisfies (P2), we have $n \mid a^{n+1} - a, a^{n+1} \equiv_n a$. Of course, $a^{n(n+1)} = (a^{n+1})^n$, so that $a^{n(n+1)} \equiv_n a^n, a^{n(n+1)+1} \equiv_n a^{n+1} \equiv_n a, n \mid a^{n(n+1)+1} - a$. The number $n+1$ is a prime. By appealing to Fermat's well known Little Theorem, we have that $n+1 \mid a^{n+1} - a, a^{n+1} \equiv_{n+1} a, a^{n(n+1)+1} \equiv_{n+1} a^{n+1} \equiv_{n+1} a, n + 1 \mid a^{n(n+1)+1} - a$. The numbers $n, n + 1$ are relatively prime, and hence $n(n + 1) \mid a^{n(n+1)+1} - a$.

1 satisfies (P2), $1 + 1 = 2$ is prime. And now: 2 satisfies (P2), $2 + 1 = 3$ is a prime, $2 \cdot 3 = 6$ satisfies (P2), $6 + 1 = 7$ is a prime, $6 \cdot 7 = 42$ satisfies (P2), $42 + 1 = 43$ is a prime, $42 \cdot 43 = 1806$ satisfies (P2). However, $1806 + 1 = 1807 = 13 \cdot 139$ is *not* a prime.

We gather more information about numbers satisfying (P2). Let $n \geq 2$ satisfy (P2), and let p be a prime that divides n. We show that $p-1$ divides n as well. This is clear for $p = 2$, and so let p be odd. Assume that we are given a positive integer w such that $p \nmid w^k - w$ for $k = 2, 3, \ldots p - 1$. We have $n = r(p - 1) + s$, where $r \geq 1$ and $p - 2 \geq s \geq 0$. Furthermore, $n \mid w^{n+1} - w$, and therefore $p \mid w^{n+1} - w$. With respect to Fermat's Little Theorem, $p \mid w^p - w$. As $p \nmid w^2 - w$, we have $p \nmid w, p \mid w^{p-1} - 1, w^{p-1} \equiv_p 1, w^{r(p-1)} \equiv_p 1, p \mid w^{r(p-1)} - 1$. But $w^{n+1} - w = (w^{r(p-1)} - 1)w^{s+1} + (w^{s+1} - w)$, and it follows that $p \mid w^{s+1} - w$. Since $1 \leq s + 1 \leq p - 1$, we get $s + 1 = 1, s = 0$, and $p - 1 \mid n$, and our claim is proved.

The question remains: Why does such a "nice" number w exist? Of course, it is easy to check that we can choose $w = 2$ for $p = 3, 5, 11, 13, 19, 29, 37, 53$ and $w = 3$ for $p = 7, 17, 31, 43$. Alas, there are infinitely many prime numbers; happily, the desired numbers w are known as "primitive roots modulo p" and their existence was proved by none other than C. F. Gauss [1, article 315].

We are now able to formulate the main scholium of this paper.

Theorem 2.1. *The following five conditions are equivalent for a positive integer n:*

(P1) $a^c \equiv_n b^d$ *whenever a, b, c, d are positive integers such that $a \equiv_n b$ and $c \equiv_n d$.*
(P2) $n \mid a^{n+1} - a$ *for every positive integer a.*
(P3) *n is squarefree and $n \mid a^n - 1$ for every positive integer a such that* $\gcd(n, a) = 1$.
(P4) *n is squarefree and $p - 1$ divides n for every prime p dividing n.*
(P5) $n = 1, 2, 6, 42, 1806$.

Proof. We have already proved that the conditions (P1) and (P2) are equivalent, that (P2) implies both (P3) and (P4), and that (P5) implies (P2). To complete the proof, we show that (P3) implies (P4) and that (P4) implies (P5). We turn our attention first to (P4) implies (P5). Let n satisfy (P4), $n \geq 2$. Then there are $k \geq 1$ primes $p_1 < p_2 < \cdots < p_k$ (if $k \geq 2$) such that $n = p_1 p_2 \cdots p_k$.

If p_1 were odd, then n would be odd, contradicting the fact that the even number $p_1 - 1$ divides n. Thus, $p_1 = 2$ and $n = 2$, provided that $k = 1$. Hence, assume that $k \geq 2$. Then p_2 is odd, $p_2 - 1 \mid n, 2 \leq p_2 - 1 < p_2, p_2 - 1$ is squarefree and no odd prime divides $p_2 - 1$. Thus, $p_2 - 1 = 2$ and $p_2 = 3$.

If $k = 2$ then $n = 6$. Assume therefore, that $k \geq 3$. Then $5 \leq p_3, 4 \leq p_3 - 1 < p_3, p_3 - 1 \mid n, p_3 - 1$ is squarefree, $p_3 - 1 \mid 6, p_3 - 1 = 6, p_3 = 7$ and $n = 42$, provided that $k = 3$. If $k \geq 4$ then $11 \leq p_4, 10 \leq p_4 - 1 < p_4, p_4 - 1 \mid p_1 p_2 p_3, p_1 p_2 p_3 = 42, p_4 - 1$ is even and squarefree, $p_4 - 1 = 14, 42, p_4 = 15, 43$. But 15 is not a prime, and hence $p_4 = 43$. If $k = 4$, then $n = 1806$. Assume, finally, that $k \geq 5$. We have $43 = p_4 < p_5$, so that $47 \leq p_5, 46 \leq p_5 - 1 < p_5, p_5 - 1$ is an even number dividing $1806, p_5 - 1 = 86, 258, 602, 1806, p_5 = 87, 259, 603, 1807$.

On the other hand, none of these numbers is a prime: $87 = 3 \cdot 29, 259 = 7 \cdot 37, 603 = 3^2 \cdot 67, 1807 = 13 \cdot 139$. We have shown that $k \leq 4$ and $n = 2, 6, 42, 1806$.

The final step is to demonstrate that (P3) implies (P4). Let $n \geq 2$ satisfy (P3) and take an odd prime p dividing n. Let w be a primitive root modulo p ($w \geq 1$ and $p \nmid w^k - w$ for $k = 2, 3, \ldots p - 1$) such that $\gcd(n, w) = 1$. Now, proceeding as before, we write $n = r(p-1) + s, r \geq 1, p - 2 \geq s \geq 0, n \mid w^n - 1, p \mid w^{p-1} - 1, w^n - 1 = (w^{r(p-1)} - 1)w^s + (w^s - 1), p \mid w^s - 1, s = 0, p - 1 \mid n$.

Why should a primitive root w coprime to n exist at all? Well, take any primitive root $w_0 \geq 1$ and put $w_k = w_0 + kp$ for every $k = 0, 1, \ldots$. We get an increasing sequence $w_0 < w_1 < w_2 < \ldots$ of primitive roots modulo p. Now we make use of Dirichlet's magnificent Prime Number Theorem, according to which, our sequence of primitive roots contains infinitely many prime numbers. Consequently, $w = w_k$ is a prime primitive root greater than n for at least one k. The equality $\gcd(n, w) = 1$ follows trivially.

The equivalence of the five conditions (P1), (P2), (P3), (P4), and (P5) is now fully established! □

Regarding (P3) and (P4), notice that all the products $n = 2^a \cdot 3^b, a \geq 1, b \geq 0$ fulfill weaker conditions:

(P3′) $n \mid a^n - 1$ for every positive integer a such that $\gcd(n, a) = 1$,
(P4′) $p - 1$ divides n for every prime p dividing n.
[Notice also that $n = 0$ satisfies (P1), (P2), (P3′), (P4′) and (P5′) where P5′ means $n = 0, 1, 2, 6, 42, 1806$.]

This means that the conditions (P1), (P2) and (P5′) are equivalent for every non-negative integer n. It is worth mentioning that $42 + 1806 = 1848$ where 1848 is generally believed to be the greatest integer m such that $m \neq ab + ac + bc$ for any three distinct positive integers a, b, c (known to be true, provided that the generalized Riemann Hypothesis holds).

Finally, we note that the following conditions are equivalent for a positive integer n:

(Q1) $(a + b)^n \equiv_n a^n + b^n$ for all positive integers a, b (the "Freshman's dream", [2, p. 121]).
(Q2) $n \mid a^n - a$ for every positive integer a.
(Q3) $n \mid a^{n-1} - 1$ for every positive integer a such that $\gcd(n, a) = 1$.
(Q4) n is squarefree and $p - 1$ divides $n - 1$ for every prime p dividing n (Korselt's criterion, [3]).

It is a known fact all prime numbers satisfy the (equivalent) conditions $(Q_1), (Q_2), \ldots (Q_4)$; moreover, there exist infinitely many composite numbers satisfying the conditions [4]. The latter numbers are known as *Carmichael numbers* [5], [6] (and many other names as well), and their sequence (A002997) starts as follow:

$$561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, \ldots$$

The first members of this sequence were first published in 1885 by the Czech mathematician Šimerka [7].

References

[1] C. F. Gauss, *Disquisitiones Arithmeticae* (Artur, A., Clarke, S. J., trans.) Yale Univ. Press, 1966.
[2] T. W. Hungerford, *Algebra*, Springer 1974.
[3] A. R. Korselt, Problème chinois, *L'intermé diaire des mathématiciens.* **6** (1899), 142–143.
[4] W. R. Alford, A. Granville, and C. Pomerance, There are Infinitely Many Carmichael Numbers. *Annals of Mathematics*, **139** (1994), 703–722
[5] R. D. Carmichael, Note on a new number theory function, *Bull. A.M.S.* **16** (1910), 232–238
[6] R. D. Carmichael, On composite numbers P which satisfy the Fermat congruence $a^{p-1} \cong 1 \pmod{p}$. *Amer. Math. Monthly* **19** (1912), 22–27.
[7] V. Šimerka, Zbytky z arithmetické posloupnosti (On the remainders of an arithmetic progression). *Časopis Pro Pěstování Matematiky a Fysiky.* **14** (1885), 221–225.