ON A FORMULA AND SOME PROPERTIES OF CARMICHAEL INDICES

Atsushi Yamagami
Department of Information Systems Science, Soka University, Tokyo, Japan
yamagami@soka.ac.jp

Youichi Inaba
Department of Information Systems Science, Soka University, Tokyo, Japan
inabamily1@gmail.com

Received:7/12/23 , Accepted: 3/28/24, Published: 4/8/24

Abstract

The notion of Carmichael indices $N(n)$ for positive integers n was defined, and some relevant properties were investigated by Matsukuma in his graduation thesis in 2012. In this article, we examine a formula for the Carmichael indices $N(n)$ for any positive integers n, as a generalization of specific results given by Matsukuma. We then give a proof of Korselt's criterion for Carmichael numbers by means of the formula. To address a question posed by Matsukuma, we also find that there is no positive integer n such that $N(n) = n - 1$.

1. Introduction

In [1, Definition 1.2], the notion of Carmichael indices $N(n)$ for positive integers n is defined as follows.

Definition 1. For any integer $n \geq 1$, we define

$$N(n) := \#\{a \in \mathbb{Z} \mid 0 \leq a \leq n-1,\ a^n \equiv a \pmod{n}\}$$

and call it the *Carmichael index* of n, where $\#X$ denotes the cardinality of a finite set X. Namely, $N(n)$ is the number of solutions in the residue ring $\mathbb{Z}/n\mathbb{Z}$ modulo n for the equation $x^n = x$.

We can immediately observe that $N(1) = 1$ and $N(p) = p$ for any prime number p by Fermat's little theorem. Moreover, we know that for any composite number n, $N(n) = n$ if and only if n is a Carmichael number. This is the reason why $N(n)$ is called the Carmichael index of n.

DOI: 10.5281/zenodo.10944058

Example 1. In Table 1, we present the list of Carmichael indices for composite numbers $4 \le n \le 105$, as calculated by the second author.

n	4	6	8	9	10	12	14	15	16	18	20	21	22	24	25
$N(n)$	2	4	2	3	4	4	4	9	2	4	4	9	4	4	5
n	26	27	28	30	32	33	34	35	36	38	39	40	42	44	
$N(n)$	4	3	8	8	2	9	4	9	4	4	9	4	8	4	
n	45	46	48	49	50	51	52	54	55	56	57	58	60	62	
$N(n)$	15	4	4	7	4	9	8	4	9	4	9	4	8	4	
n	63	64	65	66	68	69	70	72	74	75	76	77	78	80	
$N(n)$	9	2	25	24	4	9	16	4	4	9	8	9	8	4	
n	81	82	84	85	86	87	88	90	91	92	93	94	95	96	
$N(n)$	3	4	8	25	4	9	4	8	49	4	9	4	9	4	
n	98	99	100	102	104	105									
$N(n)$	4	9	4	8	4	25									

Table 1. The list of Carmichael indices for composite numbers $4 \le n \le 105$.

In [1, Corollaries 1 and 2], it was proven that for any prime number $p \ge 5$,

$$N(3p) = N(3p^2) = 9.$$

In this article, we prove a formula for Carmichael indices $N(n)$ of positive integers $n \ge 2$, as stated in the following theorem.

Theorem 1. *For any positive integer $n \ge 2$, we denote the prime factorization of n by*

$$n = p_1^{e_1} \cdots p_r^{e_r}$$

with distinct prime factors $p_1, \ldots, p_r$ and positive integers $e_1, \ldots, e_r$. For any $1 \le i \le r$, we write

$$N(n; p_i^{e_i}) := \# \left\{ \bar{a} \in (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times \ : \ \mathrm{ord}(\bar{a}) \,\middle|\, \left(p_i - 1, \frac{n}{p_i^{e_i}} - 1 \right) \right\},$$

where $x \mid y$ means that x divides y for any integers $x \ne 0$ and y, $\mathrm{ord}(\bar{a})$ is the order of $\bar{a}$ in $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$, and $\left(p_i - 1, \frac{n}{p_i^{e_i}} - 1 \right)$ is the greatest common divisor of $p_i - 1$ and $\frac{n}{p_i^{e_i}} - 1$. Then,

$$N(n) = \prod_{i=1}^{r} (N(n; p_i^{e_i}) + 1).$$

Example 2. For any prime number $p \geq 5$, we see that

$$N(3p) = (N(3p;3)+1)(N(3p;p)+1)$$

by the formula given in Theorem 1. Then,

$$\begin{aligned} N(3p;3) &= \#\left\{\bar{a} \in (\mathbb{Z}/3\mathbb{Z})^{\times} \mid \operatorname{ord}(\bar{a}) \mid (2, p-1)\right\} \\ &= \#\left\{\bar{a} \in (\mathbb{Z}/3\mathbb{Z})^{\times} \mid \operatorname{ord}(\bar{a}) \mid 2\right\} \\ &= \#\{\bar{1}, \bar{2}\} \\ &= 2 \end{aligned}$$

and

$$\begin{aligned} N(3p;p) &= \#\left\{\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^{\times} \mid \operatorname{ord}(\bar{a}) \mid (p-1, 2)\right\} \\ &= \#\left\{\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^{\times} \mid \operatorname{ord}(\bar{a}) \mid 2\right\} \\ &= \#\{\bar{1}, \overline{-1}\} \\ &= 2 \end{aligned}$$

imply that

$$N(3p) = (2+1)(2+1) = 9.$$

This conclusion agrees with the result obtained in [1, Corollary 1] and the examples with $N(n) = 9$ for

$$n = 15, 21, 33, 39, 51, 57, 69, 87, 93$$

as in Example 1.

Moreover, we see that

$$N(3p^2) = (N(3p^2;3)+1)(N(3p^2;p^2)+1)$$

by the formula given in Theorem 1. Then,

$$\begin{aligned} N(3p^2;3) &= \#\left\{\bar{a} \in (\mathbb{Z}/3\mathbb{Z})^{\times} \mid \operatorname{ord}(\bar{a}) \mid \left(2, p^2-1\right)\right\} \\ &= \#\left\{\bar{a} \in (\mathbb{Z}/3\mathbb{Z})^{\times} \mid \operatorname{ord}(\bar{a}) \mid 2\right\} \\ &= \#\{\bar{1}, \bar{2}\} \\ &= 2 \end{aligned}$$

and

$$\begin{aligned} N(3p^2;p^2) &= \#\left\{\bar{a} \in \left(\mathbb{Z}/p^2\mathbb{Z}\right)^{\times} \mid \operatorname{ord}(\bar{a}) \mid (p-1, 2)\right\} \\ &= \#\left\{\bar{a} \in \left(\mathbb{Z}/p^2\mathbb{Z}\right)^{\times} \mid \operatorname{ord}(\bar{a}) \mid 2\right\} \\ &= \#\{\bar{1}, \overline{-1}\} \\ &= 2 \end{aligned}$$

imply that

$$N(3p^2) = (2+1)(2+1) = 9,$$

which agrees with the result obtained in [1, Corollary 2] and the example $N(75) = 9$ in the list given in Example 1. We note that in the above calculation,

$$\left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/p\mathbb{Z}$$

as abelian groups. Then, $\left\{\bar{a} \in \left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times \mid \mathrm{ord}(\bar{a}) \mid 2\right\}$ is a subset of the prime-to-p component of $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times$, which is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$ under the above isomorphism.

Example 3. Consider the case where $n = 66$ with three distinct prime factors $2, 3, 11$. We see that

$$N(66) = (N(66;2)+1)(N(66;3)+1)(N(66;11)+1)$$

by the formula given in Theorem 1. Then,

$$\begin{aligned}
N(66,2) &= \#\left\{\bar{a} \in (\mathbb{Z}/2\mathbb{Z})^\times \mid \mathrm{ord}(\bar{a}) \mid (1,33)\right\} \\
&= \#\left\{\bar{a} \in (\mathbb{Z}/2\mathbb{Z})^\times \mid \mathrm{ord}(\bar{a}) \mid 1\right\} \\
&= \#\{\bar{1}\} \\
&= 1, \\
N(66,3) &= \#\left\{\bar{a} \in (\mathbb{Z}/3\mathbb{Z})^\times \mid \mathrm{ord}(\bar{a}) \mid (2,21)\right\} \\
&= \#\left\{\bar{a} \in (\mathbb{Z}/3\mathbb{Z})^\times \mid \mathrm{ord}(\bar{a}) \mid 1\right\} \\
&= \#\{\bar{1}\} \\
&= 1, \\
N(66;11) &= \#\left\{\bar{a} \in (\mathbb{Z}/11\mathbb{Z})^\times \mid \mathrm{ord}(\bar{a}) \mid (10,5)\right\} \\
&= \#\left\{\bar{a} \in (\mathbb{Z}/11\mathbb{Z})^\times \mid \mathrm{ord}(\bar{a}) \mid 5\right\} \\
&= \#\{\bar{1}, \bar{3}, \bar{4}, \bar{5}, \bar{9}\} \\
&= 5
\end{aligned}$$

imply that

$$N(66) = (1+1)(1+1)(5+1) = 24,$$

which agrees with the value in the list given in Example 1.

In Section 1, we prove Theorem 1, and subsequently use it to prove Korselt's criterion for Carmichael numbers. In Section 2, we observe that there is no positive integer n such that $N(n) = n - 1$. This result answers a question posed in [1].

Remark 1. In [1, Section 6], some properties of loop lengths in the sequences $\{0^n \pmod n, \dots, (n-1)^n \pmod n\}$ were investigated in the case where $n = p^k$ and $p^k q$ with any distinct prime numbers p, q and any positive integer k. More precisely, it was proven that the length of the loop in $\{0^{p^k} \pmod{p^k}, \dots, (p^k-1)^{p^k} \pmod{p^k}\}$ (resp. $\{0^{p^k q} \pmod{p^k q}, \dots, (p^k q - 1)^{p^k q} \pmod{p^k q}\}$) is equal to p (resp. pq) in [1, Theorem 6.1] (resp. [1, Theorem 6.2]). For example, the second author of this article calculated that in the case where $n = 81 = 3^4$, the sequence

$$\{0^{81} \pmod{81}, \dots, 80^{81} \pmod{81}\}$$

consists of 27 copies of the loop

$$0 \pmod{81},\ 1 \pmod{81},\ 80 \pmod{81}$$

of length 3, and in the case where $n = 104 = 2^3 \times 13$, the sequence

$$\{0^{104} \pmod{104}, \dots, 103^{104} \pmod{104}\}$$

consists of four copies of the loop

$$\bar{0}, \bar{1}, \overline{48}, \bar{9}, \overline{16}, \bar{1}, \overline{16}, \overline{81}, \overline{40}, \overline{81}, \overline{48}, \bar{9}, \overline{40}, \overline{65}, \overline{40}, \bar{9}, \overline{48}, \overline{81}, \overline{40}, \overline{81}, \overline{16}, \bar{1}, \overline{16}, \bar{9}, \overline{48}, \bar{1}$$

of length $26 = 2 \times 13$, where we denote by $\bar{a}$ the residue class modulo 104 represented by an integer a. In this article, we do not examine any properties of the sequences

$$\{0^n \pmod n, \dots, (n-1)^n \pmod n\}$$

for any $n \geq 2$, but we would like to pursue this question for positive integers n of various types in the future.

2. Proof of Theorem 1

We now present a proof of Theorem 1.

Proof of Theorem 1. Recall the notation and definitions introduced in the statement of Theorem 1. By the Chinese Remainder Theorem, for any $a \in \mathbb{Z}$, $a^n \equiv a \pmod n$ if and only if $a^n \equiv a \pmod{p_i^{e_i}}$ for any $1 \leq i \leq r$.

We now fix any $1 \leq i \leq r$ and set $p := p_i$ and $e := e_i$. We then assume that $a^n \equiv a \pmod{p^e}$.

First, in the case where $p \mid a$, if $a \not\equiv 0 \pmod{p^e}$, then

$$0 \not\equiv a \equiv a^n \equiv 0 \pmod{p^e}$$

by the inequality $n \geq p^e > e$, which is a contradiction. On the other hand, $0^n \equiv 0 \pmod{p^e}$. Therefore, $a^n \equiv a \pmod{p^e}$ implies that

$$a \equiv 0 \pmod{p^e};$$

i.e., the equation $\bar{a}^n = \bar{a}$ has only one solution $\bar{a} = \bar{0}$ in $\mathbb{Z}/p^e\mathbb{Z}$ in the case where $p \mid a$. Here, $\bar{a}$ is the residue class in $\mathbb{Z}/p^e\mathbb{Z}$ represented by a.

Next, we assume that $p \nmid a$.

In the case where $p = 2$, because $(a, 2) = 1$ and $\#\left(\mathbb{Z}/2^e\mathbb{Z}\right)^\times = 2^{e-1}$, we see that

$$a^{2^{e-1}} \equiv 1 \pmod{2^e}$$

by Euler's theorem. Therefore the congruence $a^n \equiv a \pmod{2^e}$ implies that

$$a \equiv a^n \equiv a^{2^{e-1} \cdot \frac{n}{2^{e-1}}} \equiv 1 \pmod{2^e};$$

i.e., the equation $\bar{a}^n = \bar{a}$ has only one solution $\bar{a} = \bar{1}$ in $\left(\mathbb{Z}/2^e\mathbb{Z}\right)^\times$.

In the case where $p \neq 2$, because $(a, p) = 1$ and $\#\left(\mathbb{Z}/p^e\mathbb{Z}\right)^\times = p^e - p^{e-1}$, we see that

$$a^{p^{e-1}(p-1)} \equiv a^{p^e - p^{e-1}} \equiv 1 \pmod{p^e}$$

by Euler's theorem. Therefore, the congruence $a^n \equiv a \pmod{p^e}$ implies that

$$a^{p-1} \equiv a^{n(p-1)} \equiv a^{p^{e-1}(p-1) \cdot \frac{n}{p^{e-1}}} \equiv 1 \pmod{p^e}. \tag{1}$$

Because this congruence implies that $a^p \equiv a \pmod{p^e}$, we see that $a^{p^e} \equiv a \pmod{p^e}$ and

$$a \equiv a^n \equiv a^{p^e \cdot \frac{n}{p^e}} \equiv a^{\frac{n}{p^e}} \pmod{p^e}.$$

Because $(a, p) = 1$, we then see that

$$a^{\frac{n}{p^e} - 1} \equiv 1 \pmod{p^e}. \tag{2}$$

The congruences (1) and (2) imply that the order $\mathrm{ord}(\bar{a})$ of the residue class $\bar{a} \in \left(\mathbb{Z}/p^e\mathbb{Z}\right)^\times$ divides $\left(p - 1, \dfrac{n}{p^e} - 1\right)$.

Conversely, for any integer a such that

$$\mathrm{ord}(\bar{a}) \left| \left(p - 1, \frac{n}{p^e} - 1\right) \right.,$$

we see that $a^p \equiv a^{\frac{n}{p^e}} \equiv a \pmod{p^e}$ and

$$a^n \equiv a^{\frac{n}{p^e} \cdot p^e} \equiv a^{p^e} \equiv a \pmod{p^e}.$$

Therefore, for any integer a which is coprime to p, $a^n \equiv a \pmod{p^e}$ if and only if $\mathrm{ord}(\bar{a}) \left| \left(p - 1, \dfrac{n}{p^e} - 1\right) \right.$ in $\left(\mathbb{Z}/p^e\mathbb{Z}\right)^\times$.

Combining the above discussion and the Chinese remainder theorem, we see that

$$N(n) = \prod_{i=1}^{r} (N(n; p^e) + 1),$$

because the Carmichael index $N(n)$ of n is the number of solutions to the equation $\bar{a}^n = \bar{a}$ in $\mathbb{Z}/n\mathbb{Z}$. We note that $\left(2-1, \frac{n}{2^e}-1\right) = 1$ implies that $N(n;2^e) = 1$ by definition. □

Example 4. We can solve the equation $\bar{a}^n = \bar{a}$ in $\mathbb{Z}/n\mathbb{Z}$ by the argument in the proof of Theorem 1. Here, we do this in the case where $n = 66$ as well as in Example 3. By the argument in Example 3 to calculate that $N(66) = 24$, we can obtain solutions to the equation

$$\bar{a}^{66} = \bar{a}$$

in $\mathbb{Z}/66\mathbb{Z}$ by the following system of congruences:

$$a \equiv \begin{cases} 0, 1 \pmod 2 \\ 0, 1 \pmod 3 \\ 0, 1, 3, 4, 5, 9 \pmod{11}. \end{cases}$$

Therefore, the solutions to $\bar{a}^{66} = \bar{a}$ in $\mathbb{Z}/66\mathbb{Z}$ are the following 24 residue classes:

$$\bar{a} = \bar{0}, \bar{1}, \bar{3}, \bar{4}, \bar{9}, \overline{12}, \overline{15}, \overline{16}, \overline{22}, \overline{25}, \overline{27}, \overline{31}, \overline{33},$$
$$\overline{34}, \overline{36}, \overline{37}, \overline{42}, \overline{45}, \overline{48}, \overline{49}, \overline{55}, \overline{58}, \overline{60}, \overline{64}.$$

As a corollary to Theorem 1, we shall give a proof of Korselt's criterion for Carmichael numbers as stated in the following corollary.

Corollary 1 (Korselt's criterion [2])**.** *A composite number n is a Carmichael number if and only if n is a product of distinct odd prime numbers and for any prime factor p of n, $p-1$ is a divisor of $n-1$.*

Proof. By definition, a composite number n is a Carmichael number if and only if for any integer a, $a^n \equiv a \pmod n$, i.e., $N(n) = n$. In particular, for any Carmichael number n, because $n \geq 4$ and $(-1)^n \equiv -1 \pmod n$, n must be odd.

Firstly, we assume that a composite number n is a Carmichael number. Let $n = p_1^{e_1} \cdots p_r^{e_r}$ be the prime factorization of n as in the statement of Theorem 1. Because n is odd, $p_i \neq 2$ for any $1 \leq i \leq r$, and the set

$$\left\{ \bar{a} \in (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times \ : \ \mathrm{ord}(\bar{a}) \,\middle|\, \left(p_i - 1, \frac{n}{p_i^{e_i}} - 1\right) \right\}$$

is a subset of the prime-to-p component of $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$, which is isomorphic to $(\mathbb{Z}/p_i\mathbb{Z})^\times$. Therefore, by definition,

$$N(n; p_i^{e_i}) \leq p_i - 1$$

for any $1 \leq i \leq r$. By Theorem 1 and the assumption that n is a Carmichael number, we see that

$$\prod_{i=1}^{r} p_i \leq \prod_{i=1}^{r} p_i^{e_i} = n = N(n) = \prod_{i=1}^{r} (N(n; p_i^{e_i}) + 1) \leq \prod_{i=1}^{r} p_i,$$

which implies that $e_i = 1$ and $N(n; p_i) = p_i - 1$ for any $1 \leq i \leq r$. Because $p_i \equiv 1 \pmod{p_i - 1}$, we see that

$$n - 1 \equiv \frac{n}{p_i} - 1 \equiv 0 \pmod{p_i - 1}$$

by the definition of $N(n; p_i)$. Therefore, n is a product of distinct odd prime numbers, and for any prime factor p of n, that $p - 1$ is a divisor of $n - 1$.

Conversely, we assume that n is a product of distinct odd prime numbers, and for any prime factor p of n, $p - 1$ is a divisor of $n - 1$. Because

$$0 \equiv n - 1 \equiv \frac{n}{p} - 1 \pmod{p - 1},$$

we see that

$$N(n; p) = p - 1,$$

which implies that

$$N(n) = \prod_{p|n} (N(n; p) + 1) = \prod_{p|n} p = n$$

by Theorem 1. Therefore, n is a Carmichael number and the corollary is proven. □

3. Non-existence of Integers n Such That $N(n) = n - 1$

In [1], the question of whether there exists any positive number n such that $N(n) = n - 1$ is raised. We answer this question in the following theorem.

Theorem 2. *There is no positive integer n such that $N(n) = n - 1$.*

Proof. Assume that there exists some positive integer n such that $N(n) = n - 1$. Because $N(1) = 1,\ N(2) = 2,\ N(3) = 3,\ N(4) = 2,\ N(5) = 5,\ N(6) = 4$, we may assume that $n \geq 7$.

The condition that $N(n) = n - 1$ implies that there exists only one integer $0 \leq b \leq n - 1$ such that

$$b^n \not\equiv b \pmod{n}. \tag{3}$$

If $2b \equiv b \pmod{n}$, then $b \equiv 0 \pmod{n}$, which contradicts (3). Therefore

$$2b \not\equiv b \pmod{n},$$

which implies that

$$(2b)^n \equiv 2b \pmod{n} \tag{4}$$

by (3). We now assume that n is odd. If $b \neq 2$, then $2^n \equiv 2 \pmod{n}$, which implies that

$$2b^n \equiv 2b \pmod{n}$$

by (4). This contradicts (3), as n is odd. Therefore, $b = 2$, i.e.,

$$2^n \not\equiv 2 \pmod{n} \tag{5}$$

by (3). Because $n \geq 7$, we see that

$$n - 2 \not\equiv 2 \pmod{n}, \quad 2(n-2) \not\equiv 2 \pmod{n},$$

which imply that

$$(n-2)^n \equiv n - 2 \pmod{n}, \quad 2^n(n-2)^n \equiv 2(n-2) \pmod{n},$$

respectively. These congruences contradict (5), as $(n, n-2) = 1$ by the assumption that n is odd. Therefore, n must be even.

Then we see that $(n-1)^n \equiv 1 \not\equiv n-1 \pmod{n}$, i.e., $b = n-1$. Therefore, for any integer $0 \leq a \leq n-2$, we have that $a^n \equiv a \pmod{n}$. In particular, for $a = \dfrac{n}{2} \pm 1$, we see that

$$\begin{aligned} \frac{n}{2} - 1 &\equiv \left(\frac{n}{2} - 1\right)^n \equiv \left(\frac{n}{2} - 1 - n\right)^n \equiv \left(-\frac{n}{2} - 1\right)^n \equiv \left(\frac{n}{2} + 1\right)^n \\ &\equiv \frac{n}{2} + 1 \pmod{n}, \end{aligned}$$

which implies a contradiction that $n = 2$. Thus, the proof is complete. □

Acknowledgement. The first author is very grateful to the second author, who is one of his students at the Soka University, for giving some interesting talks about results in [1], as well as his calculations of Carmichael indices in seminars held in 2022 at the Soka University. The authors thank Mr. Daisuke Matsukuma and his advisor, Professor Kyo Nishikawa, for making the graduation thesis [1] available for download on the internet. Moreover, we would like to thank Editage (www.editage.jp) for English language editing.

References

[1] D. Matsukuma, Gijisosuu to sosuuhantei test [Pseudoprimes and primality tests] (in Japanese), thesis, Aoyama Gakuin University, 2012. Available at `http://www.math.aoyama.ac.jp/~kyo/sotsuken/2012/matsukuma_sotsuron_2012.pdf`

[2] G. Tarry, I. Franel, A. Korselt and G. Vacca, Problème chinois, *L'intermédiaire des Mathématiciens* **6** (1899), 142-144.