A Note on the Carmichael Function

Yimin Ge

Abstract

The well known *Euler's Theorem* states that $x^{\varphi(m)} \equiv 1 \pmod{m}$ for every positive integer m and every integer x coprime to m, where φ is the Euler's Totient Function.

However, with some exceptions, $\varphi(m)$ is usually not the least positive integer t so that $x^t \equiv 1 \pmod{m}$ holds for all integers x with $\gcd(x, m) = 1$ and can be "optimized" to the so-called *Carmichael Function* $\lambda(m)$.

Properties of this function keep appearing in Olympiad problems and can often be very useful. The purpose of this note is to state and prove some of these properties and to give some examples of how they can be applied in Olympiad problems.

Introduction

The following problem was given at the 3rd round of the 2006 Iranian National Olympiad:

Problem 1. *Let n be a positive integer and let d be the least positive integer, so that $a^d \equiv 1 \pmod{n}$ holds for every integer a with $\gcd(a, n) = 1$. Prove that there exists an integer b so that $\operatorname{ord}_n(b) = d$.*

We will see that this problem is a special case of a more general result, but before proving it, we shall cover some theory.

Definition 1. For a positive integer m and an integer x with $\gcd(x, m) = 1$, the *order* of x modulo m, denoted by $\operatorname{ord}_m(x)$, is the least positive integer t, so that $x^t \equiv 1 \pmod{m}$.

Euler's Theorem does not only imply that $\operatorname{ord}_m(x)$ exists but implies $\operatorname{ord}_m(x) \leq \varphi(m)$.

Lemma 1. *Let m be a positive integer and x be an integer coprime to m. Then $x^n \equiv 1 \pmod{m}$ if and only if $\operatorname{ord}_m(x) \mid n$. Furthermore, $x^{n_1} \equiv x^{n_2} \pmod{m}$ if and only if $\operatorname{ord}_m(x) \mid (n_1 - n_2)$.*

Proof. Let $d = \operatorname{ord}_m(x)$. It is clear that $d \mid n$ implies $x^n \equiv 1 \pmod{m}$. On the other hand, if $x^n \equiv 1 \pmod{m}$, then there exist integers q, r such that $n = qd + r$, $0 \leq r \leq d - 1$, and

$$x^n \equiv x^{qd+r} \equiv x^r \equiv 1 \pmod{m}.$$

But $0 \leq r \leq d - 1$, so $r = 0$. □

Definition 2. Let m be a positive integer. An integer g is called a *primitive root* modulo m if $\operatorname{ord}_m(g) = \varphi(m)$.

Primitive roots however do not exist for every positive integer m.

Lemma 2. *Let m be a positive integer greater than* 1. *Then primitive roots modulo m exist if and only if m has the form 2, 4, p^k or $2p^k$ where p is an odd prime number and k is a positive integer.*

This theorem is very well known, we skip the rather long proof of it (interested readers can find a proof in [2]).

The Carmichael Function

Definition 3. For a positive integer m, $\lambda(m)$ denotes the least positive integer t so that $x^t \equiv 1 \pmod{m}$ for all integers x with $\gcd(x, m) = 1$. $\lambda(m)$ is the so-called *Carmichael Function.*

Lemma 3. *Let m be a positive integer. Then $x^t \equiv 1 \pmod{m}$ holds for all integers x coprime to m if and only if $\lambda(m) \mid t$.*

The proof of Lemma 3 is similar to the proof of Lemma 1 and is left as an exercise to the reader.

Note that Euler's Theorem implies $\lambda(m) \leq \varphi(m)$.

It is clear that if m has primitive roots, then $\lambda(m) = \varphi(m)$. We will now find a formula for $\lambda(m)$.

Lemma 4. *Let $k \geq 3$ be an integer. Then $\lambda(2^k) = 2^{k-2}$.*

Proof. We first observe that $x^2 \equiv 1 \pmod{8}$ for all odd integers x.

Using induction, we can assume that $x^{2^{k-2}} \equiv 1 \pmod{2^k}$ for all odd x and some $k \geq 3$. Then either

$$x^{2^{k-2}} \equiv 1 \pmod{2^{k+1}} \quad \text{or} \quad x^{2^{k-2}} \equiv 1 + 2^k \pmod{2^{k+1}}.$$

We however have $x^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}$ in both cases, implying $\lambda(2^k) \leq 2^{k-2}$.

Now, let x be an odd integer so that $\operatorname{ord}_{16}(x) = 4$ (i.e. any integer congruent to 3 or 5 modulo 8). We clearly have $\operatorname{ord}_8(x) = 2$.

Using induction, we can assume that $\operatorname{ord}_{2^k}(x) = 2^{k-2}$ and $\operatorname{ord}_{2^{k+1}}(x) = 2^{k-1}$ for some $k \geq 3$. Then $x^{2^{k-2}} \equiv 1 \pmod{2^k}$ but $x^{2^{k-2}} \not\equiv 1 \pmod{2^{k+1}}$, implying

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

Hence, either

$$x^{2^{k-2}} \equiv 1 + 2^k \pmod{2^{k+2}} \quad \text{or} \quad x^{2^{k-2}} \equiv 1 + 2^k + 2^{k+1} \pmod{2^{k+2}}.$$

In both cases we have

$$x^{2^{k-1}} \equiv 1 + 2^{k+1} \not\equiv 1 \pmod{2^{k+2}}.$$

Thus $\operatorname{ord}_{2^{k+2}}(x) > 2^{k-1}$. On the other hand, $\operatorname{ord}_{2^{k+2}}(x) \mid \varphi(2^{k+2}) = 2^{k+1}$ by Lemma 1, so $\operatorname{ord}_{2^{k+2}}(x) \in \{2^k, 2^{k+1}\}$. But $\operatorname{ord}_{2^{k+2}}(x)$ cannot exceed $\lambda(2^{k+2})$ and we already know that $\lambda(2^{k+2}) \leq 2^k$. It follows that $\operatorname{ord}_{2^{k+2}}(x) = 2^k$ and thus $\lambda(2^{k+2}) = 2^k$. □

The proof of Lemma 4 also shows that

Lemma 5. *For any x congruent to 3 or 5 modulo 8, $\operatorname{ord}_{2^k}(x) = \lambda(2^k) = 2^{k-2}$ for all $k \geq 3$.*

Now, let a and b be two coprime positive integers and let $d_1 = \lambda(a)$, $d_2 = \lambda(b)$ and $d = \lambda(ab)$. Then $x^d \equiv 1 \pmod{ab}$ for any integer x coprime to ab, so

$$x^d \equiv 1 \pmod{a} \quad \text{and} \quad x^d \equiv 1 \pmod{b} \tag{1}$$

for all integers x coprime to ab. Now, from Lemma 3 it follows that $d_1 \mid d$ and $d_2 \mid d$ is a necessary and sufficient condition for (1) and since d is the least positive integer satisfying (1), it follows that $d = \operatorname{lcm}(d_1, d_2)$. We thus obtain

Lemma 6. *For any coprime positive integers a and b, $\lambda(ab) = \operatorname{lcm}(\lambda(a), \lambda(b))$.*

We see that Lemma 2, 4 and 6 already give a complete formula for $\lambda(m)$. We summarize:

Theorem 1. *Let m be a positive integer greater than 1. Then*

$$\lambda(m) = \begin{cases} \varphi(m) & \text{for } m = 2, 4, p^k, \text{ where } p \geq 3 \text{ is prime} \\ 2^{k-2} & \text{for } m = 2^k, \text{ where } k \geq 3 \\ \operatorname{lcm}(\lambda(p_1^{k_1}), \ldots, \lambda(p_r^{k_r})) & \text{for } m = \prod_{i=1}^{r} p_i^{k_i}, \text{ where } p_i \text{ are distinct} \\ & \text{prime numbers.} \end{cases}.$$

We can now return to the beginning of this note and solve Problem 1.

Lemma 7. *For any positive integer m, there exists an integer x so that $\operatorname{ord}_m(x) = \lambda(m)$.*

Proof. Let $m = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$ be the prime factorization of m and let x be a solution of the congruence system

$$x \equiv g_i \pmod{p_i^{k_i}} \quad \text{for } i = 1, \ldots, r,$$

where g_i are integers satisfying $\operatorname{ord}_{p_i^{k_i}}(x) = \lambda(p_i^{k_i})$ respectively (they exist by Lemma 2 and 5). Such an x exists by the Chinese Remainder Theorem.

Then by Lemma 1, $\lambda(p_i^{k_i}) = \operatorname{ord}_{p_i^{k_i}}(x) \mid \operatorname{ord}_m(x)$ for all $i = 1, \ldots, r$. Hence

$$\operatorname{ord}_m(x) \geq \operatorname{lcm}(\lambda(p_1^{k_1}), \ldots, \lambda(p_r^{k_r})) = \lambda(m).$$

But $\operatorname{ord}_m(x)$ cannot exceed $\lambda(m)$, so $\operatorname{ord}_m(x) = \lambda(m)$. □

However, Lemma 7 can be generalized to

Theorem 2. *Let m and d be positive integers. Then there exists an integer x with $\operatorname{ord}_m(x) = d$ if and only if $d \mid \lambda(m)$.*

Proof. If $\operatorname{ord}_m(x) = d$ for some x, then Lemma 1 implies $d \mid \lambda(m)$.

On the other hand, if $d \mid \lambda(m)$, let z be an integer with $\operatorname{ord}_m(z) = \lambda(m)$ (which exists by Lemma 7), $e = \lambda(m)/d$, and $x = z^e$. Then $\operatorname{ord}_m(x) = d$ because

$$x^d = z^{ed} = z^{\lambda(m)} \equiv 1 \pmod m$$

and $\operatorname{ord}_m(x) < d$ would imply $\operatorname{ord}_m(z) < ed = \lambda(m)$, a contradiction. □

The application of the properties of the Carmichael Function are, when possible, not always as obvious as it has been in Problem 1. The following problem illustrates another kind of usage:

Problem 2. *Prove that for any positive integer k, there is a positive integer n so that $2^k \mid 3^n + 5$.*

Solution. We will only discuss $k \geq 3$. The statement is true for $k = 3$, just take $n = 1$ (we need this for the purpose of induction).

It follows from Lemma 5 that $\operatorname{ord}_{2^k}(3) = \lambda(2^k) = 2^{k-2}$, so by Lemma 1, the numbers $3^1, 3^2, \ldots, 3^{2^{k-2}}$ all give different residues modulo 2^k. However, since

$$\operatorname{ord}_{2^{k+1}}(3) = \lambda(2^{k+1}) = 2^{k-1} > 2^{k-2} = \operatorname{ord}_{2^k}(3),$$

from Lemma 1 it follows that

$$3^{i+2^{k-2}} \equiv 3^i \pmod{2^k} \quad \text{but} \quad 3^{i+2^{k-2}} \not\equiv 3^i \pmod{2^{k+1}}$$

and thus

$$3^{i+2^{k-2}} \equiv 3^i + 2^k \pmod{2^{k+1}}.$$

Hence, if $3^i \equiv -5 \pmod{2^k}$, then either

$$3^i \equiv -5 \pmod{2^{k+1}} \quad \text{or} \quad 3^{i+2^{k-2}} \equiv -5 \pmod{2^{k+1}}.$$

□

References

[1] Mathlinks, *Order*,
`http://www.mathlinks.ro/Forum/viewtopic.php?t=108204`

[2] Mathlinks, *Primitive root*,
`http://www.mathlinks.ro/Forum/viewtopic.php?t=55473`

[3] Mathlinks, $(2^k) \mid (3^m + 5)$,
`http://www.mathlinks.ro/Forum/viewtopic.php?t=1912`

Yimin Ge: Vienna, Austria