



The Carmichael Function ?

* Sangeeta

Research Paper—Mathematics

3.1 THE CARMICHAEL FUNCTION?

It follows from Euler's theorem that if $(a, n) = 1$, there exists the smallest positive integer r such that $a^r \equiv 1 \pmod{n}$. The integer r thus obtained, is called the order of a modulo n . If $m > 1$, is an integer, then from 1.3.3(i), it follows easily that $a^m \equiv 1 \pmod{n}$ if and only if m is a multiple of r ; in particular r divides $\phi(n)$. If we choose $n = 2$, then for every odd integer a , $a^1 \equiv 1 \pmod{2}$, either order of a modulo 2 is always 1 = $\phi(2)$. For $n = 2$, there exists an integer a (a – any odd integer) such that order of a modulo 2 is $\phi(2) = 1$.

It is then natural to ask: given $n > 2$, does there always exist an integer a , $(a, n) = 1$ such that order of a modulo n is $\phi(n)$? The answer for the question is given in Theorem 1.3.7. In particular, if $n = pk$, p is odd prime and $k > 1$ is an integer such number always exists. We call it the primitive root modulo pk .

More precisely, the following assertions are equivalent: (i) a is a primitive root modulo p and $a^{p-1} \equiv 1 \pmod{p^2}$. (ii) a is a primitive root modulo p^2 . (iii) for every $k > 2$, a is a primitive root modulo p^k .

However, if n is divisible by $4p$ or pq when p and q are distinct odd primes, then there is no number a , $(a, n) = 1$ such that order of a modulo n is equal to $\phi(n)$. In particular, choose $a = 10$ and $p = 487$, then 10 is a primitive root modulo 487, but $10^{486} \not\equiv 1 \pmod{487^2}$, yields that 10 is not primitive root modulo 4872. Indeed, in 1910 R.D. Carmichael introduced a function λ and proved the following divisibility theorem: $a^{\lambda(n)} \equiv 1 \pmod{n}$, for $(a, n) = 1$. For integer $n > 1$ there always exist an integer a such that $(a, n) = 1$ and order of

a modulo n is equal to $\lambda(n)$. 3.1.1 Definition (The arithmetic function λ). Let $m > 1$ be any positive integer, defines:

- (i) $\lambda(1) = 1$
- (ii) $\lambda(m) = \phi(m)$, when $m = 2, 4, p^k, 2p^k$ where p is an odd prime and k a positive integer.
- (iii) $\lambda(m) = \frac{1}{2} \phi(m)$ when $m = 2^h$, $h > 2$
- (iv) For all remaining values of m where $m = \dots$, $h > 0$.
 $\lambda(m) = [\lambda(2^h), \lambda(p_1^{k_1}), \dots, \lambda(p_r^{k_r})]$, where $[\dots]$ denotes the least common multiple. Note that $\lambda(n)$ divides $\phi(n)$.

Therefore, $\lambda(n) < \phi(n)$, but $\lambda(n) = \phi(n)$ only for $n = 1, 2, 4, p^k, 2p^k$. Carmichael proved the following divisibility theorem.

3.1.2 Theorem. [36, p. 475] Let $m > 1$. There always exists an integer a co-prime to m such that $a^{\lambda(m)} \equiv 1 \pmod{m}$.

Proof. (i) Let $m = 2, 4, p^k, 2p^k$ and let $(a, m) = 1$. By definition $\lambda(m) = \phi(m)$. Hence $a^{\lambda(m)} \equiv 1 \pmod{m}$ by Fermat's theorem.

(ii) Let $m = 2^h$, $h > 2$, and let $(a, m) = 1$. Then by definition $\lambda(m) = \frac{1}{2} \phi(m)$. Therefore by theorem "If $m = 2^h$, $h > 2$ and $(a, m) = 1$, then $a^{(\phi(m))/2} \equiv 1 \pmod{m}$ we have $a^{\lambda(m)} \equiv 1 \pmod{m}$.

(iii) Let $m = 2^h p_1^{k_1} p_2^{k_2} \dots$ and let $(a, m) = 1$. Then by definition $\lambda(m) = [\lambda(2^h), \lambda(p_1^{k_1}), \dots, \lambda(p_r^{k_r})]$.

From (i) and (ii) we have

$$a^{\lambda(m)} \equiv 1 \pmod{2^h}$$

$$a^{\lambda(m)} \equiv 1 \pmod{p_i^{k_i}}$$

$$\dots$$

$$\dots$$

$$a^{\lambda(m)} \equiv 1 \pmod{m}$$

Then by (1.1.5 (x))

$[?(2h), ?() \dots, ?()]$

$a ? 1 \pmod{2h \dots}$ this implies

$a?(m) ? 1 \pmod{m}$.

3.1.3 Definition. If the congruence $a^{m-1} ? 1 \pmod{m}$ is satisfied for every a with $(a, m) = 1$, then m is called a number having Fermat Property. The existence of such numbers was first detected by the American mathematician Carmichael in 1809. The integers 561, 1105, 1729 and 2465 possess Fermat property.

3.1.4 Example. Show that 561 possess Fermat property. Solution. Let $561 = 3.11.17$ and $(a, 561) = 1$ gives $(a, 3) = (a, 11) = (a, 17) = 1$.

$a?(3) = a^2 ? 1 \pmod{3}$,

$a?(11) = a^{10} ? 1 \pmod{11}$,

$a?(17) = a^{16} ? 1 \pmod{17}$.

From this, we have

$a^{560} ? (a^2)^{280} ? 1 \pmod{3}$,

$a^{560} ? (a^{10})^{56} ? 1 \pmod{11}$,

$a^{560} ? (a^{16})^{35} ? 1 \pmod{17}$.

From this

$a^{560} ? 1 \pmod{561}$, where $(a, 561) = 1$.

Hence 561 possess Fermat property.

3.1.5 Theorem. Let $m ? 1 \pmod{?(m)}$. Then m has Fermat property.

Proof. Given

$m ? 1 \pmod{?(m)}$. Hence $?(m)$ divides $m-1$.

If a is any integer such that $(a, m) = 1$, then by Theorem 3.1.2.

$a?(m) ? 1 \pmod{m}$. This implies that

$a?(m).(m-1)/?(m) ? 1 \pmod{m}$, therefore,

therefore,

$a^{m-1} ? 1 \pmod{m}$

Hence m has Fermat property. 3.1.6 Theorem. If m is a product of distinct primes then, for all a , $a?(m)+1 ? a \pmod{m}$ (1) Proof. Let $m = ?p_i$. Then $(a, m) = 1$ gives $(a, p_i) = 1$, for each prime p_i .

By Fermat's theorem

$a^{p_i-1} ? 1 \pmod{p_i}$.

Then

$a^{n(p_i-1)} ? 1 \pmod{p_i}$.

Multiplying by a , we have

$a^{n(p_i-1)+1} ? a \pmod{p_i}$.

We infer that $a^{si} ? a \pmod{p_i}$ if $s_i ? 1 \pmod{p_i-1}$ (2) for all a such that $(a, p_i) = 1$. This congruence holds also when $(a, p_i) = p_i$, because then both sides of (2) are congruent to $0 \pmod{p_i}$. We choose a value of s such that $s ? s_i ? 1 \pmod{p_i-1}$ for every value of i , then we have $a^s ? a \pmod{p_i}$, for every prime p_i and for all a . By Chinese remainder theorem, $a^s ? a \pmod{m}$ provided that $s ? 1 \pmod{p_i-1}$ for every prime factor p_i of m . Since $?(m) = \text{L.C.M. } [p_i-1]$, therefore, if we choose $s = ?(m) + 1$ then it satisfies the condition $s ? 1 \pmod{p_i-1}$ for each i . So proves the result.

3.1.7 Remark. Since $?(m)$ is the least common multiple of all the p_i-1 , $?(m)+1$ is also the smallest value of $s > 1$ satisfying $s ? 1 \pmod{p_i-1}$ for all i . In general $a^s ? a \pmod{m}$ holds for all values of a if and only if $s ? 1 \pmod{?(m)}$. For particular values of a , as could be congruence to a for much smaller values of s than $?(m)+1$. Moreover, if m contains multiple prime factors, then (1) need not be true. For example $m = 12$ and $?(m) = 2$ and $2?(m)+1 = 2*2+1 = 5 \not\equiv 1 \pmod{12}$.

3.1.8 Theorem. If

$$?(x) = k \quad (1),$$

then (1) can not have two solutions of type pr , where p is a prime number and one another solution is given by $q = 1+pr-1 \pmod{p-1}$, if q is a prime.

Proof. Let if possible pr and qs are two solutions of (1), where p and q are distinct primes with $p < q$ (say). Hence

$$?(pr) = ?(qs)$$

This implies

$$pr-1 \pmod{p-1} = qs-1 \pmod{q-1} \quad (2)$$

If $r > 1$ then from (2) we get q divides $p-1$, which is a contradiction. So (1) can not have two prime power solutions. Hence $s = 1$ and from (2), we get that $q = 1+pr-1 \pmod{p-1}$ is another solution of (1).

3.1.9 Example. Find solutions of $?(x) = 6$, by using above theorem.

Solution. We know $?(32) = 6$ hence one solution of the form pr is 32 i.e. $p = 3$ and $r = 2$.

Then another solution q is given by

$$\begin{aligned} q &= 1 + pr - 1(r-1) \\ &= 1 + 3 \cdot 2 - 1(3-1) \\ &= 1 + 3(2) = 7 \\ \text{So } \phi(9) &= \phi(7) = 6. \end{aligned}$$

3.2 ON COMPOSITE NUMBER P WHICH SATISFY THE FERMAT CONGRUENCE $a^{P-1} \equiv 1 \pmod{P}$ AND MAXIMAL GENERALIZATION OF FERMAT'S THEOREM

By Fermat's Theorem 1.2.3 if p is a prime then for every integer a , with $(a, p) = 1$, $a^{p-1} \equiv 1 \pmod{p}$. This theorem is a tool for testing the primality of a given integer n . For, if it could be shown that the congruence $a^{n-1} \equiv 1 \pmod{n}$ fails to hold for some choice of a , then n is necessarily composite.

Let $n = 117$ and choose $a = 2$. We can show $2^{116} \not\equiv 1 \pmod{117}$ easily. Hence 117, must be composite.

J.H. Jeans [18] has discussed about the converse of Fermat's Theorem and asked that if a and n are integers such that $(a, n) = 1$, then is the relation $a^{n-1} \equiv 1 \pmod{n}$ true? Mr. E.B. Escott [10] has given a more direct proof of the same Theorem. The failure of the converse of Fermat's theorem has also been pointed out by Lucas [23] by means of an example. Lucas stated the converse in the form: If $ax-1$ is divisible by P for $x = P-1$, but for no other value of x which is divisor of $P-1$, then P is a prime number. In Theorem 3.2.3, we obtained the conditions for the integer P to be a solution of $a^{P-1} \equiv 1 \pmod{P}$.

3.2.1 Lemma. A necessary and sufficient condition on the integer P in order that the congruence $a^{P-1} \equiv 1 \pmod{P}$ shall be true for an integer a which is prime to P is that $P-1 \equiv 0 \pmod{\phi(P)}$.

Proof. First assume that

$$a^{P-1} \equiv 1 \pmod{P} \quad (1)$$

We assert that $\phi(P)$ divides $P-1$.

By Theorem 3.1.2

$$a^{\phi(P)} \equiv 1 \pmod{P} \quad (2)$$

and $\phi(P)$ is the least exponent such that (2) is true for every a prime

to P . So $\phi(P)$ divides $P-1$ from (1).

Converse: Let $\phi(P)$ divides $P-1$, then we have to prove that

$$a^{P-1} \equiv 1 \pmod{P} \quad (3)$$

Since $\phi(P)$ divides $P-1$, so $P-1 = \phi(P)k$, for some integer k .

It follows from (2), that

$$a^{\phi(P)} \equiv 1 \pmod{P}.$$

Then,

$$a^{\phi(P)k} \equiv 1^k \equiv 1 \pmod{P}$$

and we get that

$$a^{P-1} \equiv 1 \pmod{P}$$

Hence Proved.

3.2.2 Lemma . If a composite P satisfy the congruence

$$a^{P-1} \equiv 1 \pmod{P} \quad (1)$$

for every a which is prime to P , then P is the product of three or more different odd factors.

Proof. By Lemma 3.2.1, it follows that P and $\phi(P)$ are relatively prime. Hence, P does not contain a repeated prime factor; for if so, such a prime would be a factor both of P and $\phi(P)$, which is impossible.

We assert that P can not be a product of two prime factors. If possible let, $P = p_1 q_1$ and $p_1 > q_1$, it follows by lemma 3.2.1, that p_1 is an integer.

Since p_1 is greater than q_1 , so the second member of above equation is not an integer. Therefore, P can not be product of two prime factors. Hence, P is the product of three or more different odd prime factors. Further $\phi(P)$ is even since $\phi(m)$ is even when $m \geq 2$ and P is composite so that it is not 2. Hence (1) is not satisfied by an even number.

3.2.3 Theorem. There always exists values of composite P for which the congruence

$$a^{P-1} \equiv 1 \pmod{P} \quad (1)$$

is true when a is any integer prime to P .

Proof. We shall prove this theorem by finding number P of the form

$P = p_1 q_1 r_1$ where $p_1 < q_1 < r_1$ are primes and which satisfy the necessary and sufficient condition of Lemma 3.2.1. The numbers p_1, q_1, r_1 being primes, a necessary condition that $P = p_1 q_1 r_1$ will satisfy

$P-1 \equiv 0 \pmod{\phi(P)}$ is that each of the ex-

pression shall be an integer. Subtracting from these numbers in order the integers q_1r_1, r_1p_1, p_1q_1 we get (2)

must be an integer.

If $p_1 = 3$, then there is a single number 3.11.17 which satisfy (2), but this number fails to satisfy the condition in Lemma 3.2.1. For $p_1 = 5$ two solutions satisfying (2) and condition of Lemma 3.2.1 are 5.13.29. For $p_1 = 7$ we have four solutions 7.13.19, 7.13.31, 7.19.67 and 7.31.73.

Now we illustrate the method of finding solutions by carrying out the process in detail for the case $p_1 = 7$.

For $p_1 = 7$, first number in (2) is

In order that this shall be an integer it is necessary and sufficient that both q_1 and r_1 shall be of the form $6n+1$ or both of the form $6n-1$. From third number in (2) we see that

where m has one of the form $2, 3, \dots, 6$, since r_1 is greater than q_1 . This equation gives

(3)

Substituting this value of r_1 is second member of (2) we find = integer.

The values of q_1 which satisfy this relation are the following

For $m = 2, q_1 = 19$;

$m = 3, q = 13, 31$;

$m = 4, q = 23$;

$m = 5, q = 13, 73$;

$m = 6$, No value of q_1

If we substitute these values of q_1 in (3) and remember that r_1 must be prime we see that $q_1 = 23, 73$ both are impossible. The other values of q_1 in order gives the number

7.19.67, 7.13.31, 7.31.73, 7.13.19

are the only possible values of p which are of the form $7q_1r_1$. These satisfy the condition

$a^{p-1} \equiv 1 \pmod{P}$

In the similar way we may assume other values of P and determine all possible values of P .

Some other integers P having the property that the congruence

$a^{p-1} \equiv 1 \pmod{P}$

is true for every a which is prime to P :

5.13.17 13.37.241

5.17.29 13.37.97

7.13.19 13.37.61

7.13.31 31.61.271

7.19.67 31.61.211

7.31.73 31.61.631

13.61.397 37.73.109

and 13.37.73.457

Maximal generalization of Fermat's little theorem.

Let $n =$ be the prime factorization of n . Put $H(n) = \max \{ ?_1, ?_2, \dots, ?_k \}$

The following result by E. Lucas (1890) is known as maximal generalization of Fermat's little theorem.

3.2.4 Theorem. For all positive integer a and n , $(a, n) = 1$

$a^{?(n)} + H(n) \equiv aH(n) \pmod{n}$.

Proof : Let $r > s$.

Suppose that $ar \equiv as \pmod{n}$

Then

$ar - s \equiv 1 \pmod{n}$

By Theorem 3.1.2, $?(n)$ divides $r - s$ and $s > H(n)$.

Conversely suppose $?(n) < ?(n)$.

Then

$?(n) + H(n) < ?(n) + H(n) < n$ with simultaneous inequality if and only if n is prime or composite.

Then

$a^{?(n)} \equiv 1 \pmod{n}$

$an.a^{?(n)} \equiv an \pmod{n}$

$an \equiv an^{-(n)} \equiv 1 \pmod{n}$

(i)

Similarly

$a^{?(n)} \equiv 1 \pmod{n}$

$an.a^{?(n)} \equiv an \pmod{n}$

$an \equiv an^{-(n)} \equiv 1 \pmod{n}$

(ii)

From (i) and (ii)

$an \equiv an^{-(n)}$

$\equiv an^{-(n)} \pmod{n}$

or $a^{?(n)} + H(n) \equiv aH(n) \pmod{n}$