International Journal of Pure and Applied Mathematics

Volume 19 No. 4 2005, 421-433

ON THE CONGRUENCES $a^{\phi(n)+L} \equiv a(\bmod n)$ AND $a^{n+L} \equiv a(\bmod n)$

A.N. El-Kassar

Department of Mathematics
Faculty of Science
Beirut Arab University Tarik El-Jedidah
P.O. Box 11-5020, Beirut, LEBANON
e-mail: ak1@bau.edu.lb

Abstract: Fermat's Theorem states that if n is prime, then $a^n \equiv a(\mathrm{mod}n)$ holds for every integer a. Euler's Theorem states that the congruence $a^{\phi(n)} \equiv 1(\mathrm{mod}n)$, and hence $a^{\phi(n)+1} \equiv a(\mathrm{mod}n)$, holds for every integer a relatively prime to n, where $\phi(n)$ is Euler phi- function. If the condition that a and n are relatively prime is dropped, then the last congruence holds for every integer a iff n is a product of distinct primes. The congruences $a^{\phi(n)+L} \equiv a(\mathrm{mod}n)$ and $a^{n+L} \equiv a(\mathrm{mod}n)$ are examined. Given L, the values of n for which the congruence $a^{\phi(n)+L} \equiv a(\mathrm{mod}n)$ ($a^{n+L} \equiv a(\mathrm{mod}n)$) holds for every integer a are characterized. In addition, properties of solutions are studied. The two congruences are extended to finite commutative rings with identity. For a fixed L, a characterization of all finite commutative rings with identity R for which $a^{\varphi(R)+L} = a$ ($a^{r+L} = a$) for every $a \in R$ is given, where r is the order of R and $\varphi(R)$ is the order of its group of units.

AMS Subject Classification: 11A25, 11U60
Key Words: congruences, Euler's Theorem, finite commutative rings

1. Introduction

Fermat's Theorem states that if p is a prime integer, then the congruence $a^{p-1} \equiv 1 \ (\mathrm{mod}p)$ holds for every integer a relatively prime to p. The result can be extended to all integers so that $a^p \equiv a(\mathrm{mod}p)$ holds for all a.

Received: October 15, 2004

Euler's generalization of Fermat's Little Theorem states that the congruence $a^{\phi(n)} \equiv 1(\text{mod}n)$ holds for every integer a relatively prime to n, where $\phi(n)$ is the Euler phi-function. This can be stated as: if $(a, n) = 1$, then

$$a^{\phi(n)+1} \equiv a(\text{mod}n), \tag{1.1}$$

where (a, n) denotes the greatest common divisor of a and n. It is clear that the last congruence is not always valid. Harger and Smith [9] showed exactly when the congruence 1.1 is valid. They also proved that if the condition $(a, n) = 1$ is dropped, then $a^{\phi(n)+1} \equiv a(\text{mod}n)$ holds for every integer a iff n is square free (a product of distinct primes).

The converse of Fermat's Theorem is not true. That is, if $a^{n-1} \equiv 1 \ (\text{mod}n)$ holds for every integer a with $(a, n) = 1$, then n is not necessarily prime. A composite integer n is called a Carmichael number (C-number) if $a^{n-1} \equiv 1 \ (\text{mod}n)$ holds for every integer a relatively prime to n. Equivalently, n is a C-number iff

$$a^n \equiv a \ \ (\text{mod}n) \tag{1.2}$$

holds for every integer a with $(a, n) = 1$. In 1910, Carmichael [4] showed that the composite integer $561(= 3.11.17)$ is a C-number. In 1912, Carmichael [5] began an in-depth study of such numbers. Alford et al [1], some eighty years later, proved that there are infinitely many Carmichael numbers.

Many generalizations and related notions to Carmichael numbers can be found in the literatures. In 1932, Lehmer [11] considered the two equations $k\phi(n) = n-1$ and $k\phi(n) = n+1$, referred to as Lehmer's equations. Composite solutions to Lehmer's equation $k\phi(n) = n-1$, if there are any, see [2] and [12], are Carmichael numbers. The class of numbers that generalize the solutions of Lehmer's other equation $k\phi(n) = n+1$, in the sense that Carmichael numbers generalize the solutions of $k\phi(n) = n-1$, are called L-numbers, see [6]. That is, an L-number is a composite number n satisfying $a^{n+1} \equiv 1(\text{mod}n)$ for any integer a with $(a, n) = 1$. Hence, the congruence

$$a^{n+2} \equiv a \ \ (\text{mod}n) \tag{1.3}$$

holds for every integer a with $(a, n) = 1$ iff n is an L-number. In [10], Korselt noted that an integer n is C-number if and only if $n = p_1p_2...p_i$ is square free and $p_j - 1$ divides $n-1$ for every prime divisor p_j of n. The analogue criteria for L-numbers states that an integer n is an L-number if and only if $n = p_1p_2...p_i$ is square free and each $p_j - 1$ divides $n + 1$.

The ring theoretic problems of determining all finite rings with identity R of order $|R|$ such that the order of the group of units of R divides $|R| \pm 1$

were initiated by Beslin and Ligh [3]. These ring theoretic problems generalize Lehmer's equations. Note that if we take R to be $\mathbf{Z}_n$, the ring of integers modulo n, the ring theoretic problems reduce to Lehmer's equations. In [6], the author considered the problems of determining all finite rings (C-rings) with identity R of order r such that $a^{r-1} = 1$ for every invertible element a. Such rings generalize the notion of Carmichael numbers. The problem of determining all finite rings (L-rings) with identity R of order r such that $a^{r+1} = 1$ for every invertible element a of R, which generalize the L-numbers, was also considered in [6]. These two problems incorporate the solutions of the two ring theoretic problems considered by Beslin and Ligh.

In [7], a new class of integers that generalize Carmichael numbers, L-numbers, solutions of Lehmer's equations, and the ring theoretic problems was introduced.

The purpose of this paper is to study the congruences

$$a^{\phi(n)+L} \equiv a \pmod{n} \tag{1.4}$$

and

$$a^{n+L} \equiv a \pmod{n}, \tag{1.5}$$

as well as their generalizations to finite commutative rings with identity. The generalized problems are as follows. For a fixed L, find all finite commutative rings with identity R for which $a^{\varphi(R)+L} = a$ ($a^{r+L} = a$) for every $a \in R$, where r is the order of R and $\varphi(R)$ is the order of its group of units. Note that if R is $\mathbf{Z}_n$ the two ring theoretic problems reduce to the congruences 1.4 and 1.5.

2. The Congruence $a^{\phi(n)+L} \equiv a(\mathrm{mod} n)$

Throughout the following, let n be a positive integer with prime power factorization $p_1^{\alpha_1}.p_2^{\alpha_2}...p_i^{\alpha_i}$ so that $n \geq 2$. A divisor d of n is a unitary divisor iff $\left(d, \frac{n}{d}\right) = 1$. Some of the properties of unitary divisors are given in the following lemma.

Lemma 1. *Let n be a positive integer, a is an integer, and let $d = (a, n)$.*

a) n is a square free iff every divisor d of n is unitary.

b) n is a square free iff every prime divisor p of n is unitary.

c) $\left(a, \frac{n}{d}\right) = \left(d, \frac{n}{d}\right)$.

d) $\left(a, \frac{n}{d}\right) = 1$ iff d is a unitary divisor of n.

e) If n is a square free, then $\left(a, \frac{n}{d}\right) = 1$.

Proof. Parts (a) and (b) follow from the fact that the unitary divisors of an integer $n = p_1^{\alpha_1}.p_2^{\alpha_2}...p_i^{\alpha_i}$ are of the form $d = p_1^{\beta_1}.p_2^{\beta_2}...p_i^{\beta_i}$, where $\beta_j = 0$ or $\beta_j = \alpha_j$, $1 \leq j \leq i$. If $d = (a, n)$, then $\left(d, \frac{n}{d}\right) = \left((a, n), \frac{n}{d}\right) = \left(a, (n, \frac{n}{d})\right) = \left(a, \frac{n}{d}\right)$. Parts (d) and (e) follow from (c). □

In the following theorem we give conditions on an integer a so that a power of a is congruent to a modulo n.

Theorem 1. *Let n and a be fixed integers with $n > 1$. The following are equivalent:*

a) The congruence $a^{\phi(n)+1} \equiv a \pmod{n}$ holds.

b) $a^m \equiv a \pmod{n}$ for some fixed integer $m > 1$.

c) $d = (a, n)$ is a unitary divisor of n.

Proof. It is clear that (a) implies (b). Now suppose that there is an integer $m > 1$ with $a^m \equiv a \pmod{n}$. Dividing by d, we get $a^{m-1} \cdot \frac{a}{d} \equiv \frac{a}{d} \pmod{\frac{n}{d}}$. Since $\left(\frac{a}{d}, \frac{n}{d}\right) = 1$, the last congruence gives $a^{m-1} \equiv 1 \pmod{\frac{n}{d}}$. Therefore, $(a, \frac{n}{d}) = 1$ and by Lemma 1, $(d, \frac{n}{d}) = (a, \frac{n}{d}) = 1$ so that d is unitary divisor of n. Thus (b) implies (c).

Now suppose that d is a unitary divisor of n. Then, $1 = (d, \frac{n}{d}) = (a, \frac{n}{d})$. By Euler's Theorem,

$$a^{\phi\left(\frac{n}{d}\right)} \equiv 1 \pmod{\frac{n}{d}}.$$

Since $\phi\left(\frac{n}{d}\right)$ divides $\phi(n)$, the last congruence gives that $a^{\phi(n)} \equiv 1 \pmod{\frac{n}{d}}$ and hence $a^{\phi(n)+1} \equiv a \pmod{\frac{n}{d}}$. Now $a^{\phi(n)+1} \equiv a \pmod{d}$ since d divides a. But d is unitary so that $(d, \frac{n}{d}) = 1$. Therefore, the last two congruences can be combined to give $a^{\phi(n)+1} \equiv a \pmod{n}$. □

An immediate consequence of Theorem 1 is that n is square free whenever the congruence $a^m \equiv a \pmod{n}$ holds for every integer a, where m is a fixed integer greater then 1. To see this, we let p be any prime divisor of n. Then, $p^m \equiv p \pmod{n}$ and by Theorem 1, $\left(p, \frac{n}{p}\right) = 1$. Hence every prime divisor of n is unitary; and from Lemma 1, we have that n is square free.

Corollary 1. *Let n be a positive integer and let $m > 1$. If $a^m \equiv a \pmod{n}$ holds for every integer a, then n is a square free.*

Now we consider the problem of determining all integers n for which the congruence $a^{\phi(n)+L} \equiv a \ (\mathrm{mod}n)$ holds for every integer a. According to Corollary 1, we only need to consider square free integers n.

Theorem 2. *Let $n = p_1.p_2...p_i$ be a square free positive integer and let $L \geq 1$. The congruence $a^{\phi(n)+L} \equiv a \ (\mathrm{mod}n)$ holds for every integer a iff $\mathrm{lcm}(p_1 - 1, p_2 - 1, ..., p_i - 1)$ divides $L - 1$.*

Proof. Let $n = p_1.p_2...p_i$ be square free and let $L \geq 1$. Suppose that for every integer a, the congruence $a^{\phi(n)+L} \equiv a \ (\mathrm{mod}n)$ holds. Given an integer a with $(a, n) = d$, we have that $\left(a, \frac{n}{d}\right) = 1$ and hence $a^{\phi\left(\frac{n}{d}\right)} \equiv 1 \ (\mathrm{mod}\frac{n}{d})$. Since $\phi\left(\frac{n}{d}\right)$ divides $\phi(n)$, $a^{\phi(n)} \equiv 1 \ (\mathrm{mod}\frac{n}{d})$ holds and

$$a^{\phi(n)+L} \equiv a^L(\mathrm{mod}\frac{n}{d}).$$

From the fact that d divides a, we have

$$a^{\phi(n)+L} \equiv a^L(\mathrm{mod}d).$$

But n is square free, so $\left(d, \frac{n}{d}\right) = 1$ and the above two congruences can be combined to give

$$a^{\phi(n)+L} \equiv a^L(\mathrm{mod}n).$$

Since $a^{\phi(n)+L} \equiv a \ \ (\mathrm{mod}n)$, $a^L \equiv a \ \ (\mathrm{mod}n)$ must be valid for every a. Hence, $a^{L-1} \equiv 1 \ \ (\mathrm{mod}n)$ holds whenever $(a, n) = 1$ and the congruence $a^{L-1} \equiv 1 \ (\mathrm{mod}p_j)$ holds for each $p_j, 1 \leq j \leq i$. In particular, $\omega^{L-1} \equiv 1 \ \ (\mathrm{mod}p_j)$ holds for every primitive root ω of p_j. Therefore, $p_j - 1$, which is the order of ω modulo p_j, divides $L - 1$ for every $j, 1 \leq j \leq i$, and thus

$$\mathrm{lcm}(p_1 - 1, p_2 - 1, ..., p_i - 1) \text{ divides } L - 1.$$

Conversely, suppose that $\mathrm{lcm}(p_1 - 1, p_2 - 1, ..., p_i - 1)$ divides $L - 1$. Then, $p_j - 1$ divides $L - 1$ for every $j, 1 \leq j \leq i$. If a is an integer with $(a, p_j) = 1$, then $a^{L-1} \equiv 1 \ \ (\mathrm{mod}p_j)$. Since $p_j - 1$ divides both $L - 1$ and $\phi(n)$, $a^{\phi(n)+L} \equiv a^{\phi(n)}a^{L-1}a \equiv a \ \ (\mathrm{mod}p_j)$. Now if $(a, p_j) \neq 1$, then $0 \equiv a^{\phi(n)+L} \equiv a \ (\mathrm{mod}p_j)$. Therefore, $a^{\phi(n)+L} \equiv a \ (\mathrm{mod}p_j)$ holds for every $p_j, 1 \leq j \leq i$, and the result follows from the fact that n is square free. □

Corollary 2. *Let n be a positive number. Then, $a^{\phi(n)+1} \equiv a(\mathrm{mod}n)$ holds for every integer a iff n is a product of distinct primes.*

Next we consider the congruence $a^{\phi(n)+L} \equiv a(\mathrm{mod}n)$ for $L < 0$; which is the same as dealing with the congruence $a^{\phi(n)-L} \equiv a \pmod{n}$ for $L > 0$. Note that if $L > \phi(n)$, then $a^{\phi(n)-L}$ is not defined for all a. Also, if $L + 1 = \phi(n)$, where n is not necessarily square free, then $a^{\phi(n)-L} \equiv a(\mathrm{mod}n)$ for every a. So we consider the problem only when $\phi(n) > L$. In the following theorem we characterize the solutions n for which $a^{\phi(n)-L} \equiv a(\mathrm{mod}n)$ holds for every a, where $L > 0$. The proof is similar to that of Theorem 1 and will be omitted.

Theorem 3. *Let L be a positive integer. The congruence $a^{\phi(n)-L} \equiv a \pmod{n}$ holds for every integer a iff $\phi(n) = L + 1$ or $n = p_1.p_2...p_i$ with $\mathrm{lcm}(p_1 - 1, p_2 - 1, ..., p_i - 1)$ divides $L + 1$.*

We close this section with the following theorem listing some properties of the solutions.

Theorem 4. *Suppose that the congruence $a^{\phi(n)+L} \equiv a \pmod{n}$ holds for every integer a. Then:*

a) The congruence is satisfied by a finite number of solutions n.

b) If $L = -1$ then $n = 2, 3, 4$ or 6.

c) If $L = 3$ then $n = 2, 3,$ or 6.

d) If $L = -3$ then $n = 5, 8, 10, 12, 15,$ or 30.

e) If L is even, then $n = 2$.

f) If n is square free and $L-1$ divides $L'-1$ then $a^{\phi(n)+L'} \equiv a \pmod{n}$ holds for every integer a.

Proof. Part (a) follows from Theorem 2 and Theorem 3 along with the fact that $\phi(n) = L - 1$ is satisfied by a finite number of values of n. For part (b), suppose that $a^{\phi(n)-1} \equiv a(\mathrm{mod}n)$ holds for every a. When $(a, n) = 1$, we have that $a^2 \equiv a^{\phi(n)} \equiv 1(\mathrm{mod}n)$. This implies that the possible values of n are $2, 3, 4, 6,$ and 8. The value $n = 8$ is dismissed since $2^{\phi(8)-1} \equiv 2^3 \equiv 0(\mathrm{mod}8)$. When $L = 3$, we have from Theorem 2 that $n = p_1.p_2...p_i$ and $p_j - 1$ divides $L-1 = 2$. Then, $p_j = 2$ or 3; and hence, the solutions are $n = 2, 3,$ or 6. For the case $L = -3$, we have that either $\phi(n) = 4$ or $n = p_1.p_2...p_i$, where $p_j - 1$ divides $L+1 = 4$. Now $\phi(n) = 4$ implies that $n = 5, 8,$ or 12; and $p_j - 1 \mid L+1 = 4$ gives that $p_j = 2, 3,$ or 5. Hence, the possible solutions are $n = 2, 3, 4, 5, 6, 10, 15,$ or 30. The values $n = 2, 3$ and 6 are dismissed since $\phi(n) + L$ must be positive. Finally, parts (e) and (f) follow from Theorem 2 and Theorem 3. □

3. The Congruence $a^{n+L} \equiv a(\mathrm{mod}n)$

Now we consider the problem of determining the integers n for which the congruence $a^{n+L} \equiv a(\mathrm{mod}n)$ holds for all integers a.

Theorem 5. *Let n be a positive number and $L \geq 1-n$. Then, $a^{n+L} \equiv a(\mathrm{mod}n)$ holds for every integer a if and only if $n = 1-L$ or $n = p_1.p_2...p_i$ with $p_j - 1$ divides $n + L - 1$.*

Proof. It is clear that $a^{n+L} \equiv a(\mathrm{mod}n)$ holds for every integer a whenever $n = 1 - L$. So we consider the case when $n + L > 1$. Suppose that $a^{n+L} \equiv a(\mathrm{mod}n)$ holds for every integer a. Since $n + L > 1$, Lemma 2 gives that $n = p_1.p_2...p_i$. For each $p_j, 1 \leq j \leq i$,

$$a^{n+L} \equiv a(\mathrm{mod}p_j),$$

holds for every integer a. In particular, the last congruence holds for every primitive root ω of p_j. Since $(\omega, p_j) = 1$,

$$\omega^{n+L-1} \equiv 1(\mathrm{mod}p_j).$$

Therefore, $p_j - 1$, divides $n + L - 1$ for every $j, 1 \leq j \leq i$.

Conversely, suppose that $n = p_1.p_2...p_i$ with $p_j - 1$ divides $n + L - 1$. Then, $p_j - 1$ divides $\frac{n}{p_j} + L - 1$, say $\frac{n}{p_j} + L - 1 = k(\ p_j - 1)$. By Fermat's Theorem, we have that

$$a^{n+L} = \left(a^{\frac{n}{p_j}}\right)^{p_j}.a^L = a^{\frac{n}{p_j}}.a^L = a^{\frac{n}{p_j}+L-1}.\ a = a^{k\ (p_j-1)}\ .a$$
$$= a^{k\ (p_j-1)+1}\ \equiv a(\mathrm{mod}p_j)\,.$$

Since n is square free, it follows that $a^{n+L} \equiv a(\mathrm{mod}n)$. □

We close this section with the following theorem listing some properties of the solutions.

Theorem 6. *Let n be a positive number. Then:*

a) $a^n \equiv a(\mathrm{mod}n)$ holds for every integer a if and only if n is a C-number.

b) $a^{n+2} \equiv a(\mathrm{mod}n)$ holds for every integer a if and only if n is a L-number.

c) If $a^{n+L} \equiv a(\mathrm{mod}n)$ holds for every integer a and $p = n + L$ is prime, then $a^{N+L} \equiv a(\mathrm{mod}N)$ holds for every integer a, where $N = np$.

d) The congruence $a^{n-1} \equiv a\ (\mathrm{mod}n)$ holds for every integer a whenever $n = 2p$ or $n = 2pq$, where p and q are odd primes with $q = 2p - 1$.

Proof. Using Korselt criteria and its L-numbers analogue along with Theorem 5, we obtain (a) and (b). Let $N = np$, where $n = p_1.p_2...p_i$ and $p = n+L$ is prime. Since $p-1 = \frac{N}{p}+L-1$, $(p-1)|\frac{N}{p}+L-1$. Also, $(p_j-1)|(n+L-1) = p-1$ and $Np+L-1 = (n+1)(p-1)$ implies that $(p_j-1)|\ Np+L-1$. By Theorem 5, we have part (c). Finally, (d) follows from (c). □

4. Ring-Theoretic Generalization

Let R be a finite commutative ring with identity, $r = |R|$ its order, $U(R)$ its group of units, and $\varphi(R) = |U(R)|$ is the order of the group of units. Throughout the following we assume that R is a nontrivial finite commutative ring with identity so that $r > 1$, the identity element and the zero elements are distinct, and $\varphi(R) < r$. Note that when $R = \mathbf{Z}_n$, $r = |R| = |\mathbf{Z}_n| = n$, $U(R) = U(\mathbf{Z}_n) = U_n$ and $\varphi(R) = \varphi(\mathbf{Z}_n) = \phi(n)$ is Euler's phi-function. If R is a field, say $R = GF(p^\alpha)$, the Galois field of order p^α, then $U(R)$ is cyclic and isomorphic to $\mathbf{Z}_{p^\alpha-1}$ and $\varphi(R) = p^\alpha - 1$. If R is a direct sum, say $R = R_1 \oplus R_2 \oplus ... \oplus R_i$, then $U(R)$ is isomorphic to $U(R_1) \times U(R_2) \times ... \times U(R_i)$ and $\varphi(R) = \varphi(R_1)\varphi(R_2)...\varphi(R_i)$. When R is the direct sum of fields, $R = F_1 \oplus F_2 \oplus .... \oplus F_i$, where $F_j = GF(p_j^{\alpha_j})$, $r = |R| = p_1^{\alpha_1}.p_2^{\alpha_2}...p_i^{\alpha i}$, the group of units $U(R)$ is isomorphic to $\mathbf{Z}_{p_1^{\alpha_1}-1} \times \mathbf{Z}_{p_2^{\alpha_2}-1} \times ... \times \mathbf{Z}_{p_i^{\alpha_i}-1}$ and $\varphi(R) = (p_1^{\alpha_1} - 1).(p_2^{\alpha_2} - 1)...(p_i^{\alpha_i} - 1)$.

Recall that a ring R is called a C-ring if and only if $a^{r-1} = 1$, $\forall a \in U(R)$; and R is an L-ring if and only if $a^{r+1} = 1, \forall a \in U(R)$. The characterizations of C-rings and L-rings obtained in [6] are stated in the following theorem.

Theorem 7. *Every C-ring and every L-ring is a direct sum of fields. Moreover, if* $R = GF(p_1^{\alpha_1}) \oplus GF(p_2^{\alpha_2}) \oplus ... \oplus GF(p_i^{\alpha_i})$, *then:*

a) R is a C-ring iff each $p_j^{\alpha_j} - 1$ *divides* $r-1$ *iff each* $p_j^{\alpha_j} - 1$ *divides* $\frac{r}{p_j^{\alpha_j}} - 1$;

b) R is an L-ring iff each $p_j^{\alpha_j} - 1$ *divides* $r+1$ *iff each* $p_j^{\alpha_j} - 1$ *divides* $\frac{r}{p_j^{\alpha_j}} + 1$.

In the following we generalize the two congruences $a^{n+L} \equiv a(\mathrm{mod} n)$ and $a^{\phi(n)+L} \equiv a(\mathrm{mod} n)$ to finite commutative rings with identity; namely, we consider the following problems.

Problem 1. Find all finite commutative rings with identity R such that $a^{\varphi(R)+L} = a$ holds for every $a \in R$.

Problem 2. Find all finite commutative rings with identity R such that $a^{r+L} = a$ holds for every $a \in R$.

Complete characterization of solutions to both problems will be obtained. Note that if R is any ring with $L = 1 - \varphi(R)$, then R satisfies Problem 1. Also, if R is any ring with $L = 1 - r$, then R satisfies Problem 2. Except for these cases, any ring satisfying either problem must be a direct sum of fields. This will be shown next.

Lemma 2. *If for some $m > 1, a^m = a$ for every $a \in R$, then R is a direct sum of fields.*

Proof. Suppose that there is $m > 1$ such that $a^m = a$ for every $a \in R$. Let a be a nilpotent element of R so that $a^k = 0$ for some $k > 1$. If $k \leq m$, then $a = a^m = a^k a^{m-k} = 0$. If $k > m$, write k as $qm + l$, where $0 \leq l < m$ and $q \geq 1$. Then $q + l < qm + l = k$. Now, $0 = a^k = a^{qm+l} = (a^m)^q . a^l = a^{q+l} = a^{k_1}$, where $k_1 = q + l < k$. If $k_1 \leq m$, then $a = 0$. Otherwise, write k_1 as $q_1 m + l_1$, where $0 \leq l_1 < m$ and $q_1 \geq 1$, so that $q_1 + l_1 < q_1 m + l_1 = k_1$ and $0 = a^{k_1} = a^{q_1 m + l_1} = a^{q_1 + l_1} = a^{k_2}$, where $k_2 = q_1 + l_1 < k_1$. If $k_2 \leq m$, then $a = 0$. Otherwise find $k_3 < k_2 < k_1 < k$, and so on. This process cannot continue indefinitely and eventually we have some $k_j \leq m$ so that $a = 0$. Thus R has no nonzero nilpotent elements and R is a direct sum of fields. □

Corollary 3. *Let R be a finite commutative ring with identity.*

a) If $a^{\varphi(R)+L} = a$ holds for every $a \in R$, then either $L = 1 - \varphi(R)$ or R is a direct sum of fields.

b) If $a^{r+L} = a$ holds for every $a \in R$, then either $L = 1 - r$ or R is a direct sum of fields.

Proof. Suppose that $a^{\varphi(R)+L} = a$ holds for every $a \in R$. If $\varphi(R) + L > 1$, then Lemma 2 gives that R is a direct sum of fields. If $\varphi(R) + L = 0$, then $a^{\varphi(R)+L} = a$ for every $a \in R$ implies that R is a trivial ring. Now, $\varphi(R) + L < 0$ is impossible since in this case $a^{\varphi(R)+L}$ is not defined for all a. The only remaining case is that $\varphi(R) + L = 1$ and hence we have part (a). A similar argument can be used to show part (b). □

In the following lemma we give some properties concerning direct sum of fields. These results are needed for the classification of solutions of Problem 1 and Problem 2.

Lemma 3. *Let $R = F_1 \oplus F_2 \oplus .... \oplus F_i$ be a direct sum of fields with $F_j = GF(p_j^{\alpha_j}), 1 \leq j \leq i$. Then:*

a) $a_j^{p_j^{\alpha_j}} = a_j, \forall\ a_j \in F_j$.

b) $a_j^{k(p_j^{\alpha_j}-1)+1} = a_j$, $\forall\ a_j \in F_j$ *and* $k \geq 0$.

c) $\forall\ a \in R$, $a^s = a^t$ *whenever* $s \equiv t\ (\mathrm{mod}\varphi(R))$.

d) $\forall\ a \in R, a^{\varphi(R)+1} = a$.

Proof. Suppose that $a_j \in F_j = GF(p_j^{\alpha_j})$. If $a_j = 0$, then $a_j^{p_j^{\alpha_j}} = 0 = a_j$. If $a_j \neq 0$, then $a_j \in U(F_j) = F_j^* \cong \mathbf{Z}_{p_j^{\alpha_j}-1}$ so that $a_j^{p_j^{\alpha_j}-1} = e_j$, where e_j is the identity of F_j. Multiplying by a_j, we get $a_j^{p_j^{\alpha_j}} = a_j$ and hence we have (a). For part (b), $a_j^{k(p_j^{\alpha_j}-1)+1} = a_j$ holds when $a_j = 0$; and when $a_j \neq 0$, $a_j^{p_j^{\alpha_j}-1} = e_j$ gives that $a_j^{k(p_j^{\alpha_j}-1)+1} = a_j$. Now suppose that $s \equiv t(\mathrm{mod}\varphi(R))$. Then $s = t + k\varphi(R) = t + k(p_1^{\alpha_1} - 1).(p_2^{\alpha_2} - 1)...(p_i^{\alpha_i} - 1)$ for some k. For every $a = (a_1, a_2, ..., a_i)$ in R, we have

$$\begin{aligned} a^s &= a^{t+k(p_1^{\alpha_1}-1).(p_2^{\alpha_2}-1)...(p_i^{\alpha_i}-1)} \\ &= \left(a_1^{k_1\left(p_1^{\alpha_1}-1\right)+t}, a_2^{k_2\left(p_2^{\alpha_2}-1\right)+t}, ..., a_i^{k_i\left(p_i^{\alpha_i}-1\right)+t}\right), \end{aligned}$$

where $k_j = k \prod_{h=1,h\neq j}^{i}(p_h^{\alpha_h} - 1)$. If $a_j = 0$, then $a_j^{k_j\left(p_j^{\alpha_j}-1\right)+t} = 0 = a_j^t$. If $a_j \neq 0$, then $a_j^{k_j\left(p_j^{\alpha_j}-1\right)+t} = a_j^{k_j\left(p_j^{\alpha_j}-1\right)+1}.a_j^{t-1}$. From part (b), $a_j^{k_j\left(p_j^{\alpha_j}-1\right)+1} = a_j$ so that $a_j^{k_j\left(p_j^{\alpha_j}-1\right)+t} = a_j.a_j^{t-1} = a_j^t$. Hence,

$$\begin{aligned} a^s &= \left(a_1^{k_1\left(p_1^{\alpha_1}-1\right)+t}, a_2^{k_2\left(p_2^{\alpha_2}-1\right)+t}, ..., a_i^{k_i\left(p_i^{\alpha_i}-1\right)+t}\right) \\ &= \left(a_1^t, a_2^t, ..., a_i^t\right) \\ &= a^t. \end{aligned}$$

Part (d) follows from (c). □

Theorem 8. *Let* $R = GF(p_1^{\alpha_1}) \oplus GF(p_2^{\alpha_2}) \oplus ... \oplus GF(p_i^{\alpha_i})$ *and let* $L > 0$. *Then,* $a^{\varphi(R)+L} = a$ *for every* $a \in R$ *iff* $LCM(\ p_1^{\alpha_1} - 1, p_2^{\alpha_2} - 1, ..., p_i^{\alpha_i} - 1)$ *divides* $L - 1$.

Proof. Let $R = GF(p_1^{\alpha_1}) \oplus GF(p_2^{\alpha_2}) \oplus ... \oplus GF(p_i^{\alpha_i})$ and let $L > 0$. Suppose that $a^{\varphi(R)+L} = a$. By Lemma 3 (c), $a^{\varphi(R)+L} = a^L$. Hence, $a_j^L = a_j$, $\forall\ a_j \in F_j$ and thus $a_j^{L-1} = e_j$, $\forall\ a_j \in F_j^*$. In particular, $\omega_j^{L-1} = e_j$, for every generator ω_j of the cyclic group $F_j^* \cong \mathbf{Z}_{p_j^{\alpha_j}-1}$. Therefore, the order of ω_j in $F_j^*, p_j^{\alpha_j} - 1$, divides $L - 1$ for $\forall j, 1 \leq j \leq i$. □

In a similar manner we prove the following theorem.

Theorem 9. *Let $R = GF(p_1^{\alpha_1}) \oplus GF(p_2^{\alpha_2}) \oplus ... \oplus GF(p_i^{\alpha_i})$ and let $L < \varphi(R)$. Then, $a^{\varphi(R)-L} = a$ for every $a \in R$ iff $LCM(\ p_1^{\alpha_1} - 1, p_2^{\alpha_2} - 1, ..., p_i^{\alpha_i} - 1)$ divides $L + 1$.*

In the following theorem, we characterize all solutions to Problem 1 for $L = 0, 1$.

Theorem 10. *Let R be a finite commutative ring with identity. Then:*

a) $a^{\phi(R)} = a$ for every $a \in R$ iff $R = \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus ... \oplus \mathbf{Z}_2$.

b) $a^{\phi(R)+1} = a$ for every $a \in R$ iff $R = GF(p_1^{\alpha_1}) \oplus GF(p_2^{\alpha_2}) \oplus ... \oplus GF(p_i^{\alpha_i})$.

Proof. Let $R = GF(p_1^{\alpha_1}) \oplus GF(p_2^{\alpha_2}) \oplus ... \oplus GF(p_i^{\alpha_i})$ and suppose that $a^{\phi(R)} = a$ for every $a \in R$. This implies that $a^{\phi(R)} = a$ for every $a \in U(R)$. Using Euler's Theorem, we have that $e = a$ for every $a \in U(R)$ and $U(R) = \{e\}$. Thus R is a boolean ring of the form $R = \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus ... \oplus \mathbf{Z}_2$. Part (b) follows from Theorem 8. □

Next we consider Problem 2. A characterization of solutions is given in the following theorem. Note that if $r + L = 1$, then $a^{r+L} = a$ holds for every a. If $r + L < 1$, then $a^{r+L} = a$ is not defined for all a. So we consider the problem when $r + L > 1$ and, from Lemma 2, R is a direct sum of fields.

Theorem 11. *Let $R = GF(p_1^{\alpha_1}) \oplus GF(p_2^{\alpha_2}) \oplus ... \oplus GF(p_i^{\alpha_i})$, $r = \mid R \mid = p_1^{\alpha_1}.p_2^{\alpha_2}...p_i^{\alpha i}$ and let $L > 1 - r$. Then $a^{r+L} = a$ holds for every integer a in R if and only if $p_j^{\alpha_j} - 1$ divides $r + L - 1$ if and only if $p_j^{\alpha_j} - 1$ divides $\dfrac{r}{p_j^{\alpha_j}} + L - 1$.*

Proof. Suppose that $a^{r+L} = a$ for every $a \in R$, where $R = GF(p_1^{\alpha_1}) \oplus GF(p_2^{\alpha_2}) \oplus ... \oplus GF(p_i^{\alpha_i})$ and $L > 1 - r$. If $a = (a_1, a_2, ...a_i)$, then $\left(a_1^{r+L}, a_2^{r+L}, ...a_i^{r+L}\right) = (a_1, a_2, ...a_i)$ and hence $a_j^{r+L} = a_j$ for $1 \leq j \leq i$. From Lemma 3 (c), we have that $r + L \equiv 1\,(\mathrm{mod}\varphi(F_j))$. This implies that $r + L \equiv 1\left(\mathrm{mod} p_j^{\alpha_j} - 1\right)$. Hence, $p_j^{\alpha_j} - 1$ divides $r + L - 1$.

Conversely, suppose that $p_j^{\alpha_j}-1$ divides $r+L-1$, then $r+L \equiv 1 \,(\mathrm{mod}\varphi\,(F_j))$ and by Lemma 3 (c), we have $a_j^{r+L} = a_j$. Hence,

$$a^{r+L} = \left(a_1^{r+L}, a_2^{r+L}, ..., a_i^{r+L}\right) = (a_1, a_2, ..., a_i) = a.$$

Finally, it is easy to see that $p_j^{\alpha_j} - 1 \mid r + L - 1$ and $p_j^{\alpha_j} - 1 | \frac{r}{p_j^{\alpha_j}} + L - 1$ are equivalent. □

We close this section by proving that solutions to Problem 1 and Problem 2 are precisely the C-rings and L-rings, respectively.

Theorem 12. *Let $R = GF(p_1^{\alpha_1}) \oplus GF(p_2^{\alpha_2}) \oplus ... \oplus GF(p_i^{\alpha_i})$ and let $r = \mid R \mid$. Then:*

a) $a^r = a$ holds for every integer a in R if and only if R is a C-ring.

b) $a^{r+2} = a$ holds for every integer a in R if and only if R is a L-ring.

Proof. If $a^r = a$ holds for every integer a in R, then clearly R is a C-ring. Now suppose that R is a C-ring. From 7, $p_j^{\alpha_j} - 1$ divides $r - 1$, and from theorem 11, $a^r = a$ holds for every integer a in R. Part (b) is shown in a similar manner. □

5. Conclusion

Two congruences generalizing Fermat's Theorem and Euler's Theorem were considered. Complete characterization of all integers n satisfying $a^{\varphi(n)+L} \equiv a(\mathrm{mod}n)$ and all integers n satisfying $a^{n+L} \equiv a(\mathrm{mod}n)$ were obtained. The result of Harger and Smith [9] and the characterization of L-numbers and C-numbers [6] are special cases of the results obtained in this paper. Also, the two congruences were extended to finite commutative rings with identity. For future work, computational aspects of the two congruences and their ring theoretic generalizations will be investigated.

References

[1] W.R. Alford, A. Granville, C. Pomerance, There are infinitely many Carmichael's numbers, *Ann. of Math.* (1994), 103-122.

[2] R. Alter, Can $\phi(n)$ divides $n-1$ properly? *Amer. Math. Monthly*, **80** (1973), 192-193.

[3] S. Beslin, S. Ligh, Lehmer's equations and finite rings with identity, *Comm. in Algebra*, **18**, No. 9 (1990), 3123-314.

[4] R.D. Carmichael, Note on a new number theory function, *Bull. Amer. Math. Soc.*, **16** (1910), 232-238.

[5] R.D. Carmichael, On composite numbers P which satisfy $a^{P-1} \equiv 1(\mathrm{mod}P)$, *Amer. Math. Monthly*, **19** (1912), 22-27.

[6] A.N. El-Kassar, Extending Carmichael's numbers and L-numbers to finite rings with identity, *Int. J. Appl. Math. 1*, No. 3 (1999), 333-343.

[7] A.N. El-Kassar, Generalizations of Carmichael's numbers, In: *Proceedings of the International Conference on Scientific Computations*, Lebanese American University, Beirut Lebanon (1999), 127-139.

[8] A.N. El-Kassar, A generalization of Lehmer's equations, In: *Proceedings of the International Conference on Scientific Computations*, Lebanese American University, Beirut Lebanon (1999), 141-151.

[9] R.T. Harger, R.M. Smith, A generalization of Fermat's Little Theorem, *Inter. J. Math. Ed. Sci. Tech.*, **31**, No. 3 (2000), 476-477.

[10] A. Korselt, Problem chinois, *L'intermdiare des Mathematiciens*, **6** (1899), 142-143.

[11] D.H. Lehmer, On Euler's totient function, *Bull. Amer. Math. Soc.*, **38** (1932), 745-751.

[12] C. Pomerance, On composite n for which $\phi(n)|n-1$, II, *Pacific J. Math.*, **69** (1977), 177-186.