Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
2024, Volume 30, Number 4, 843–850
DOI: 10.7546/nntdm.2024.30.4.843-850

Some new results on the largest cycle consisting of quadratic residues

Prabin Das[1] and Pinkimani Goswami[2]

[1] Department of Mathematics, University of Science and Technology Meghalaya
Baridua, India
e-mail: prabin1955@gmail.com

[2] Department of Mathematics, University of Science and Technology Meghalaya
Baridua, India
e-mail: pinkimanigoswami@yahoo.com

Received: 14 October 2023 **Revised:** 25 November 2024
Accepted: 10 December 2024 **Online First:** 11 December 2024

Abstract: The length of the largest cycle consisting of quadratic residues of a positive integer n is denoted by $L(n)$. In this paper, we have obtained a formula for finding $L(p)$, where p is a prime. Also, we attempt to characterize a prime number p in terms of the largest cycle consisting of quadratic residues of p.
Keywords: Quadratic residues, Fermat primes, Mersenne prime, Largest cycle, Legendre symbol.
2020 Mathematics Subject Classification: 11A07.

1 Introduction

In 2016, Haifeng Xu [2] introduced the notion of a cycle consisting of quadratic residues. It is defined as follows:

Definition 1.1. *If there exists a sequence of numbers* $\{x_i\}_{i=1}^{k}$ *such that*

$$\begin{cases} x_1^2 & \equiv x_2 \pmod{n} \\ x_2^2 & \equiv x_3 \pmod{n} \\ & \vdots \\ x_{k-1}^2 & \equiv x_k \pmod{n} \\ x_k^2 & \equiv x_1 \pmod{n} \end{cases}$$

then these k numbers form a cycle modulo n and the number k is defined as the cycle length.

It can be seen that for any integer $n > 1$ there exists a largest cycle modulo n and the length of such a cycle is denoted by $L(n)$.

Example 1.2. *For $n = 31$, we get $\{0\}$, $\{1\}$, $\{5, 25\}$, $\{2, 4, 16, 8\}$, $\{9, 19, 20, 28\}$ and $\{7, 18, 14, 10\}$ as possible cycles of lengths $1, 1, 2, 4, 4$ and 4, respectively. Here, we have 3 largest cycles having length 4, i.e., $L(31) = 4$.*

Example 1.3. *For $n = 49$, we get $\{0\}$, $\{1\}$,$\{18, 30\}$,$\{8, 15, 29\}$,$\{36, 22, 43\}$,$\{9, 32, 44, 25, 37, 46\}$, and $\{2, 4, 6, 11, 23, 39\}$ as possible cycles of lengths $1, 1, 2, 3, 3, 6$ and 6, respectively. Here, we have 2 largest cycles having length 6, i.e., $L(49) = 6$.*

Remark 1.4. *For any $n > 1$, we have*

$$0^2 \equiv 0 \pmod{n}$$

$$1^2 \equiv 1 \pmod{n}$$

These two cycles are named trivial cycles. Therefore it is clear $L(n) \geq 1$ for $n > 1$.

From Definition 1.1 it is easy to verify that for $i = 1, 2, \ldots, k$,

$$x_i^{2^k} \equiv x_i \pmod{n}$$

It is also clear that if $L(n) = k$, then k is the smallest power of 2 satisfying

$$x_j^{2^k} \equiv x_j \pmod{n}$$

where x_j is any element of any cycle of length k.

In this paper, we provide a general formula to compute $L(p)$, where p is prime and also characterize the prime p for the largest cycle consisting of quadratic residues. We organize our paper as follows:

In Section 2, an explicit formula is obtained to calculate $L(p)$, where p is prime. In Section 3, an attempt has been made to characterize the prime p for the length of the largest cycle consisting of quadratic residues.

We have followed David M. Burton [1] throughout the paper for all symbols and notations. Thus, $\gcd(m, n)$ and $\operatorname{lcm}(m, n)$ will mean the greatest common divisor and least common multiple of integers m and n, respectively, $\operatorname{ord}_n(a)$ will mean the order of an element a modulo n, QR_p will mean the set of all quadratic residues of p and $\phi(n)$ denote the number of positive integers not exceeding n that are relatively prime to n.

2 Main results

In this section, we provide a general formula to compute $L(p)$ for any prime p. If $p = 2$, then it can easily be computed as $L(p) = 1$. Therefore, we consider only odd primes and state our result in the form of a theorem as follows.

Theorem 2.1. *If p is any odd prime number and $L(p)$ is the length of a largest cycle consisting of quadratic residues modulo p, then*

$$L(p) = \begin{cases} \mathrm{ord}_{\frac{\phi(p)}{2}}(2), & \text{if } \frac{\phi(p)}{2} \text{ is odd} \\ \mathrm{ord}_{r^s}(2), & \text{if } \frac{\phi(p)}{2} \text{ is even and } \frac{\phi(p)}{2} = 2^t r^s, t \geq 1, s > 0 \text{ and } r \text{ is odd} \\ 1, & \text{if } \frac{\phi(p)}{2} \text{ is even and } \frac{\phi(p)}{2} = 2^t,\ t \geq 0 \end{cases}$$

Proof. Let p be an odd prime number. Assuming $L(p)$ to be the length of any largest cycle of quadratic residues of p, let $\{x_1, x_2, \ldots, x_{L(p)}\}$ form such a largest cycle.

Let g be a primitive root of p. Then there is a positive integer y such that $y \equiv g^2 \pmod p$ and $ord_p(y) = \frac{\phi(p)}{2} = \frac{p-1}{2}$. Now, for any $x_i \in QR_p$, $x_i \equiv y^{a_i} \pmod p$ with $1 \leq a_i \leq \frac{p-1}{2}$. By definition of the length of a cycle:

$$\begin{aligned} x_i^{2^{L(p)}-1} &\equiv 1 \pmod p \\ \Rightarrow (y^{a_i})^{2^{L(p)}-1} &\equiv 1 \pmod p \\ \Rightarrow y^{a_i(2^{L(p)}-1)} &\equiv 1 \pmod p \end{aligned}$$

So, $\frac{\phi(p)}{2} \mid a_i(2^{L(p)} - 1)$. Now, there are two cases:

Case I: Let $\frac{\phi(p)}{2}$ be odd.

If $\frac{\phi(p)}{2} \nmid 2^{L(p)} - 1$, then $\frac{\phi(p)}{2} \mid a_i$, i.e., $a_i = \frac{\phi(p)}{2} = \frac{p-1}{2}$, which implies $x_i \equiv y^{\frac{p-1}{2}} \equiv 1 \pmod p$. So, $L(p) = 1$.

If $\frac{\phi(p)}{2} \mid 2^{L(p)} - 1$, then $2^{L(p)} \equiv 1 \pmod{\frac{\phi(p)}{2}}$. This means that $\mathrm{ord}_{\frac{\phi(p)}{2}}(2) \leq L(p)$. Assuming $\mathrm{ord}_{\frac{\phi(p)}{2}}(2) = k$, we have $k \mid L(p)$ and $2^k - 1 \equiv 0 \pmod{\frac{\phi(p)}{2}}$ which implies $x_i^{2^k-1} \equiv 1 \pmod p$. But $L(p)$ is the smallest positive integer such that $x_i^{2^{L(p)}-1} \equiv 1 \pmod p$ for $i = 1, 2, \ldots, L(p)$. So, if $k < L(p)$, then $x_i^{2^k-1} \equiv 1 \pmod p$ contradicting the Definition 1.1. Therefore $k = L(p)$ i.e., $L(p) = \mathrm{ord}_{\frac{\phi(p)}{2}}(2)$.

Case II: Let $\frac{\phi(p)}{2}$ be even so that we can write $\frac{\phi(p)}{2} = 2^t r^s, t > 0, s \geq 0$ and r is an odd integer.

If $s = 0$, then $\frac{\phi(p)}{2} = 2^t$. Therefore, $\frac{\phi(p)}{2} \nmid 2^{L(p)} - 1$ and so $\frac{\phi(p)}{2} \mid a_i$. This means that $a_i = \frac{\phi(p)}{2}$ and, in view of $x_i \equiv y^{a_i} \pmod p$ we have $x_i \equiv 1 \pmod p$. Therefore, $L(p) = 1$.

Suppose $s \neq 0$, then $\frac{\phi(p)}{2} \mid a_i(2^{L(p)} - 1)$ implies $2^t r^s \mid a_i(2^{L(p)} - 1)$. Since $2^{L(p)} - 1$ is odd, we get $2^t \mid a_i$ and $r^s \mid 2^{L(p)} - 1$. Now, $r^s \mid 2^{L(p)} - 1$ implies $2^{L(p)} \equiv 1 \pmod{r^s}$. This means that $\mathrm{ord}_{r^s}(2) \leq L(p)$. Taking $\mathrm{ord}_{r^s}(2) = k_1$ we have $k_1 \leq L(p)$. But $k_1 < L(p)$ contradicts the Definition 1.1. Therefore $L(p) = k_1$, i.e., $L(p) = \mathrm{ord}_{r^s}(2)$.

Combining both cases, we have

$$L(p) = \begin{cases} \mathrm{ord}_{\frac{\phi(p)}{2}}(2), & \text{if } \frac{\phi(p)}{2} \text{ is odd} \\ \mathrm{ord}_{r^s}(2), & \text{if } \frac{\phi(p)}{2} \text{ is even, where } \frac{\phi(p)}{2} = 2^t r^s, t \geq 1, s > 0 \text{ and } r \text{ is odd} \\ 1, & \text{if } \frac{\phi(p)}{2} = 2^t, t \geq 0 \end{cases}$$

Thus the proof is complete. □

Corollary 2.2. For Fermat prime F_k, $\phi(F_k) = \phi(2^{2^k} + 1) = 2^{2^k}$ and $\frac{\phi(F_k)}{2} = 2^{2^k - 1}$. Therefore, by Theorem 2.1 $L(F_k) = 1$ which also gives Proposition 4.1 of [2].

Corollary 2.3. For safe prime $p = 2p_1 + 1$, where p_1 is also a prime, $\frac{\phi(p)}{2}$ is equal to 2 or an odd prime. In case of $\frac{\phi(p)}{2} = p_1 = 2$ we have $L(p) = 1$, i.e., $L(5) = 1$. If $\frac{\phi(p)}{2} = p_1 \neq 2$ and 2 is a primitive root modulo p_1, then $L(p) = \frac{p-3}{2}$. Thus Proposition 4.4 of [2] also follows from the preceding theorem.

Corollary 2.4. If p is a prime of the form $p = 2^k + 1$, where $k \geq 1$, then $\frac{\phi(p)}{2} = 2^{k-1}$, so $L(p) = 1$.

Note: It is easy to show that if $n = pq$ and $\gcd(L(p), L(q)) = 1$, then $L(n) = L(p)L(q)$, p and q being distinct primes.

3 Characterization of a prime associated with largest cycles of quadratic residues

In this section, we obtain a characterization of a prime p in terms of any largest cycle consisting of quadratic residues modulo the prime p.

Proposition 3.1. *For an odd prime p, $L(p) = 2$, if and only if p is of the form $2^k \cdot 3 + 1, k \geq 1$.*

Proof. Let us start by taking $p = 2^k \cdot 3 + 1, k \geq 1$. Then $\phi(p) = 2^k \cdot 3$ and thus, $L(p) = \mathrm{ord}_3(2) = 2$.

Conversely, let $L(p) = 2$.

Case I: If $\frac{\phi(p)}{2} > 1$ is an odd number, then either $\frac{\phi(p)}{2} \mid 2^{L(p)} - 1$ or $\frac{\phi(p)}{2} \nmid 2^{L(p)} - 1$. In case, $\frac{\phi(p)}{2} \nmid 2^{L(p)} - 1$ we have $L(p) = 1$, which contradicts our assumption. Therefore $\frac{\phi(p)}{2} \mid 2^{L(p)} - 1 = 3$. As $\frac{\phi(p)}{2} > 1$ we must have $\frac{\phi(p)}{2} = 3$, so that $p = 7 = 2 \cdot 3 + 1$ which is in the form $p = 2^k \cdot 3 + 1, k = 1$.

Case II: If $\frac{\phi(p)}{2}$ is an even number, then $\frac{\phi(p)}{2} = 2^t r^s, t \geq 1, s \geq 0$ and $r > 1$ is any odd number. The condition $s = 0$ can be ruled out since in that case, we shall have $L(p) = 1$ contradicting our assumption. Thus $\frac{\phi(p)}{2} = 2^t r^s, t \geq 1, s \geq 1$ and $r > 1$ is any odd number. By Theorem 2.1 $2 = L(p) = \mathrm{ord}_{r^s}(2)$, which implies $r^s = 3$. Therefore $\phi(p) = 2^{t+1} \cdot 3 = 2^k \cdot 3, k \geq 2$ i.e., $p = 2^k \cdot 3 + 1, k \geq 2$.

Combining the two cases we conclude that p is a prime number of the form $2^k \cdot 3 + 1, k \geq 1$ which completes the proof. □

Proposition 3.2. *For an odd prime p, $L(p) = 3$, if and only if p is of the form $2^k \cdot 7 + 1, k > 1$.*

Proof. We may start by assuming $p = 2^k \cdot 7 + 1, k \geq 1$. However, for $k = 1$, $p = 15$, which is not a prime number. So, we assume that $p = 2^k \cdot 7 + 1, k > 1$. Then $\phi(p) = 2^k \cdot 7$ and $L(p) = \text{ord}_7(2) = 3$.

Conversely, let $L(p) = 3$. If possible, let $\frac{\phi(p)}{2}$ be an odd number. Then either $\frac{\phi(p)}{2} \mid 2^{L(p)} - 1$ or $\frac{\phi(p)}{2} \nmid 2^{L(p)} - 1$. If $\frac{\phi(p)}{2} \nmid 2^{L(p)} - 1$, then $L(p) = 1$ contradicting our assumption. Hence $\frac{\phi(p)}{2} \mid 2^{L(p)} - 1$, which means that $\frac{\phi(p)}{2} = 1$ or 7. If $\frac{\phi(p)}{2} = 1$, then $L(p) = 1$ contradicting our assumption again. If $\frac{\phi(p)}{2} = 7$, then $\phi(p) = 14$, which admits of no solution for p. Therefore, $\frac{\phi(p)}{2}$ must be an even number so that we can express $\frac{\phi(p)}{2} = 2^t r^s, t \geq 1, s \geq 0$, where $r > 1$ is any odd number. However, following the argument as mentioned in Proposition 3.1, the integer $s = 0$ is ruled out. So, $\frac{\phi(p)}{2} = 2^t r^s, t \geq 1, s \geq 1$, and $r > 1$ is any odd number. Now $3 = L(p) = \text{ord}_{r^s}(2)$ implies $r^s = 7$. Therefore $\phi(p) = 2^{t+1} \cdot 7 = 2^k \cdot 7, k > 1$ i.e., p is a prime of the form $2^k \cdot 7 + 1, k > 1$. □

Proposition 3.3. *For an odd prime p, $L(p) = 4$, if and only if p is either of the form $2^k \cdot 5 + 1$ or $2^k \cdot 15 + 1$, where $k \geq 1$.*

Proof. Let p be either in the form $2^k \cdot 5 + 1$ or $2^k \cdot 15 + 1$, $k \geq 1$. If $p = 2^k \cdot 5 + 1, k \geq 1$, then $\frac{\phi(p)}{2} = 2^{k-1} \cdot 5, k \geq 1$. This gives $L(p) = \text{ord}_5(2) = 4$. Again, if $p = 2^k \cdot 15 + 1, k \geq 1$, then $\frac{\phi(p)}{2} = 2^{k-1} \cdot 15, k \geq 1$ which means that $L(p) = \text{ord}_{15}(2) = \text{lcm}(\text{ord}_3(2), \text{ord}_5(2)) = \text{lcm}(2, 4) = 4$.

Conversely, let $L(p) = 4$. If $\frac{\phi(p)}{2} > 1$ is an odd number, then either $\frac{\phi(p)}{2} \mid 2^{L(p)} - 1$ or $\frac{\phi(p)}{2} \nmid 2^{L(p)} - 1$. If $\frac{\phi(p)}{2} \nmid 2^{L(p)} - 1$, then $L(p) = 1$, which contradicts our assumption. Again, if $\frac{\phi(p)}{2} \mid 2^{L(p)} - 1$, then $\frac{\phi(p)}{2} = 3, 5$ or 15. For $\frac{\phi(p)}{2} = 3$, we have $L(p) = \text{ord}_3(2) = 2$ which contradicts our assumption. For $\frac{\phi(p)}{2} = 5$ and 15, we have $L(p) = \text{ord}_5(2)$ and $\text{ord}_{15}(2)$, respectively, and in both cases $L(p) = 4$. Thus, $p = 11 = 2 \cdot 5 + 1$ or $p = 31 = 2 \cdot 15 + 1$.

On the other hand, if $\frac{\phi(p)}{2}$ is an even number, then $\frac{\phi(p)}{2} = 2^t r^s, t \geq 1, s \geq 0$ where $r > 1$ is any odd number. However, following the argument as mentioned in Proposition 3.1, $s = 0$ is ruled out. So, $\frac{\phi(p)}{2} = 2^t r^s, t \geq 1, s \geq 1$, and $r > 1$ is any odd number. Then $4 = L(p) = \text{ord}_{r^s}(2)$, which implies $r^s = 3, 5, 15$. Here, only possible values of r^s are 5 and 15. Therefore p is a prime of the form $2^k \cdot 5 + 1$ or $2^k \cdot 15 + 1$ for $k \geq 1$. □

Proposition 3.4. *For an odd prime p, $L(p) = 5$, if and only if p is of the form $2^k \cdot 31 + 1$ where $k > 1$.*

Proof. We start by assuming $p = 2^k \cdot 31 + 1, k > 1$. Then $\frac{\phi(p)}{2} = 2^{k-1} \cdot 31$. So, $L(p) = \text{ord}_{31}(2) = 5$.

Conversely, let $L(p) = 5$. If $\frac{\phi(p)}{2} > 1$ is an odd number, then either $\frac{\phi(p)}{2} \mid 2^{L(p)} - 1$ or $\frac{\phi(p)}{2} \nmid 2^{L(p)} - 1$. If $\frac{\phi(p)}{2} \nmid 2^{L(p)} - 1$, then $L(p) = 1$, which contradicts our assumption. Again, if $\frac{\phi(p)}{2} \mid 2^{L(p)} - 1$, then $\frac{\phi(p)}{2} = 31$ which is not possible. Therefore $\frac{\phi(p)}{2}$ must be an even number so that we can take $\frac{\phi(p)}{2} = 2^t r^s, t \geq 1, s \geq 0$ where $r > 1$ is any odd number. However, following the argument as mentioned in Proposition 3.1, $s = 0$ is ruled out. So, $\frac{\phi(p)}{2} = 2^t r^s, t \geq 1, s \geq 1$, and $r > 1$ is any odd number. Therefore, $5 = L(p) = \text{ord}_{r^s}(2)$ which implies $r^s = 31$. Therefore p is a prime of the form $2^k \cdot 31 + 1, k > 1$. □

Proposition 3.5. *For an odd prime p, $L(p) = 6$, if and only if p is in one of the forms $2^k \cdot 9 + 1$, $2^k \cdot 21 + 1$ or $2^k \cdot 63 + 1$, where $k \geq 1$.*

Proof. Let p be in any one of the forms $2^k \cdot 9 + 1$, $2^k \cdot 21 + 1$ or $2^k \cdot 63 + 1$, $k \geq 1$. For $p = 2^k \cdot 9+1, k \geq 1$, $\frac{\phi(p)}{2} = 2^{k-1} \cdot 9, k \geq 1$. This gives $L(p) = \mathrm{ord}_9(2) = 6$. For $p = 2^k \cdot 21+1, k \geq 1$, $\frac{\phi(p)}{2} = 2^{k-1} \cdot 21, k \geq 1$ which gives $L(p) = \mathrm{ord}_{21}(2) = \mathrm{lcm}(\mathrm{ord}_3(2), \mathrm{ord}_7(2)) = \mathrm{lcm}(2, 3) = 6$. Finally, for $p = 2^k \cdot 63 + 1, k \geq 1$, $\frac{\phi(p)}{2} = 2^{k-1} \cdot 63, k \geq 1$ which gives $L(p) = \mathrm{ord}_{63}(2) = \mathrm{lcm}(\mathrm{ord}_7(2), \mathrm{ord}_9(2)) = \mathrm{lcm}(3, 6) = 6$.

Conversely, let $L(p) = 6$. If $\frac{\phi(p)}{2} > 1$ is an odd number, then either $\frac{\phi(p)}{2} \mid 2^{L(p)} - 1$ or $\frac{\phi(p)}{2} \nmid 2^{L(p)} - 1$. If $\frac{\phi(p)}{2} \nmid 2^{L(p)} - 1$, then $L(p) = 1$, which contradicts our assumption. Again, $\frac{\phi(p)}{2} \mid 2^{L(p)} - 1$ implies $\frac{\phi(p)}{2} = 3, 7, 9, 21$ or 63. Clearly, $\frac{\phi(p)}{2} \neq 3, 7$. Therefore $p = 19, 43$ or 127. Now, let $\frac{\phi(p)}{2}$ be an even number so that $\frac{\phi(p)}{2} = 2^t r^s, t \geq 1, s \geq 0$ where $r > 1$ is any odd number. However, following the argument as mentioned in Proposition 3.1, the integer $s = 0$ is ruled out. So, $\frac{\phi(p)}{2} = 2^t r^s, t \geq 1, s \geq 1$, where $r > 1$ is any odd number. Now, $6 = L(p) = \mathrm{ord}_{r^s}(2)$ which gives $r^s = 3, 7, 9, 21$ or 63. But $r^s = 3$ or 7 contradicts the assumption that $L(p) = 6$. Therefore, only possible values of r^s are $9, 21$ and 63. This shows that p is a prime of the form $2^k \cdot 9 + 1$ or $2^k \cdot 21 + 1$ or $2^k \cdot 63 + 1, k \geq 1$. □

The characterization of the prime number p in terms of the length of largest cycles with $L(p) = n$ where $n = 1, 2, 3, 4, 5$ and 6 motivates us to derive the same for any value of n. However, we are successful partially in our attempt which is contained in the following proposition.

Proposition 3.6. *For any odd prime p and any positive integer $n \geq 3$ with $L(p) = n$,*

(a) if $2^n - 1$ is prime, then n is a prime and p is of the form $2^k M_n + 1$, where $k \geq 2$, $M_n = 2^n - 1$ is a Mersenne prime, and

(b) if $2^n - 1$ is composite and n is a prime, then

$$p = \begin{cases} 2\Pi_{i=1}^{\ell} q_i + 1, & q_i \equiv \pm 1 \pmod 8,\ \ell \geq 1 & \text{if } \frac{\phi(p)}{2} \text{ is odd} \\ 2^t\Pi_{i=1}^{\ell} q_i + 1, & q_i \equiv \pm 1 \pmod 8,\ \ell \geq 1, t > 1 & \text{if } \frac{\phi(p)}{2} \text{ is even} \end{cases}$$

Proof. To start with, let us take $2^n - 1$ as prime. In this case n is also a prime number [1]. Now, let $\frac{\phi(p)}{2}$ be odd. Then either $\frac{\phi(p)}{2} \mid 2^{L(p)} - 1$ or $\frac{\phi(p)}{2} \nmid 2^{L(p)} - 1$. If $\frac{\phi(p)}{2} \nmid 2^{L(p)} - 1$, then $L(p) = 1$, which contradicts that $L(p) = n \geq 3$. Again, if $\frac{\phi(p)}{2} \mid 2^{L(p)} - 1$, then $\phi(p) = 2(2^n - 1)$ which imply $p = 2^{n+1} - 1$. But if $p = 2^{n+1} - 1$ is prime, then $n + 1$ is prime. This is not possible for any prime $n \geq 3$. So, $2(2^n - 1) + 1$ is composite and thus $\phi(p) = 2(2^n - 1)$ has no solution [1]. Therefore $\frac{\phi(p)}{2}$ must be even.

Let $\frac{\phi(p)}{2} = 2^t r^s, t \geq 1, s \geq 0$ and $r > 1$ is any odd number. Here, also $s = 0$ leads us to a contradictory value $L(p) = 1$ as $L(p) \geq 3$. Thus $\frac{\phi(p)}{2} = 2^t r^s, t \geq 1, s \geq 1$ and $r > 1$ is any odd number. Clearly, $r^s \mid 2^n - 1$ implies $2^n - 1 = r^s$ as $2^n - 1$ is prime. Therefore $p = 2^{t+1}(2^n - 1) + 1$. Thus, if $L(p) = n \geq 3$ and $2^n - 1$ is prime, then n must be an odd prime and p is of the form $2^k M_n + 1$, where $k \geq 2$ and $M_n = 2^n - 1$ is a Mersenne prime.

Next, let $2^n - 1$ be composite where n is a prime number. Then by [1], any prime divisor of $M_n = 2^n - 1$ is of the form $2kn + 1$ for some integer k. More precisely, prime divisor q of M_n is of the form $q \equiv \pm 1 \pmod 8$ [1]. It is also conjectured that $2^n - 1$ is square-free if n is prime. So, we consider $2^n - 1$ as a square-free number and hence it has at least two distinct prime factors. We start by taking exactly two distinct prime factors say q_1 and q_2 and then generalize the result for all possible distinct prime factors. Now, $q_1 = 2k_1 n + 1 \equiv \pm 1 \pmod 8$ and $q_2 = 2k_2 n + 1 \equiv \pm 1 \pmod 8$. Let $\frac{\phi(p)}{2} > 1$ be odd. Then $\frac{\phi(p)}{2} \mid 2^n - 1$ which implies $\frac{\phi(p)}{2} = q_1, q_2$, or $q_1 q_2$.

Without loss of generality, we may take $\frac{\phi(p)}{2} = q_1$, then $p = 2q_1 + 1, q_1 \equiv \pm 1 \pmod 8$ and $n = L(p) = \mathrm{ord}_{q_1}(2)$. As $q_1 \equiv \pm 1 \pmod 8$, so the Legendre symbol $\left(\frac{2}{q_1}\right) = 1$, i.e., 2 is quadratic residue of q_1, i.e., 2 is not a primitive root of q_1. Therefore, n must be a prime factor of $\frac{q_1 - 1}{2}$.

If $\frac{\phi(p)}{2} = q_1 q_2$, then $p = 2q_1 q_2 + 1, q_i \equiv \pm 1 \pmod 8$ and $n = L(p) = \mathrm{ord}_{q_1 q_2}(2) = \mathrm{lcm}(\mathrm{ord}_{q_1}(2), \mathrm{ord}_{q_2}(2))$. As n is prime, so either any one of $\mathrm{ord}_{q_1}(2)$ and $\mathrm{ord}_{q_2}(2)$ is equal to n while the other is 1 or $\mathrm{ord}_{q_1}(2) = \mathrm{ord}_{q_2}(2) = n$. Therefore by similar argument as mentioned in the preceding paragraph n must be prime factor of $\frac{q_1 - 1}{2}$ or $\frac{q_2 - 1}{2}$ or both, i.e., n must be a prime factor of $\Pi_{i=1}^{2} \frac{q_i - 1}{2}$. For more than two distinct prime factors of $2^n - 1$, we may argue similarly and arrive at a general expression for p namely, $p = 2\Pi_{i=0}^{\ell} q_i + 1$, where $q_i \equiv \pm 1 \pmod 8$ and $\ell \geq 1$ is the number of prime factors of $2^n - 1$.

Now, let $\frac{\phi(p)}{2}$ be even. In this case also we can similarly show that p must be a prime of the form $2^t \Pi_{i=0}^{\ell} q_i + 1$, where $q_i \equiv \pm 1 \pmod 8), \ell \geq 1$ and $t > 1$. □

Remark 3.7. *The question of deriving an expression for p when n and $2^n - 1$ are both composite remains open.*

4 Conclusion

In this paper, we have derived a general formula to compute $L(p)$, where p is prime. Under the same context we have also characterized p in terms of the largest cycle consisting of quadratic residues. In case of power digraphs [3] also we encounter with the problem of computing possible number of cycles. The present results easily help us to compute the length of largest cycles for power digraphs modulo n, where n is a prime. Similar computation of length of largest cycle for a power digraph modulo n where n is composite is yet to be solved in the context of the present study.

Acknowledgement

The authors would like to thank the anonymous referees for their valuable comments and suggestions that improved the quality of the paper.

References

[1] Burton, D. M. (2012). *Elementary Number Theory*. (7th ed.). TATA McGraw-Hill Edition.

[2] Xu, H., (2016). *The largest cycles consist by the quadratic residues and Fermat primes.* Preprint. arXiv:1601.06509v2[math.NT] 27 Jan 2016.

[3] Somer, L., & Křížek, M. (2004). On a connection of number theory with graph theory. *Czechoslovak Mathematical Journal*, 54(129), 465–485.