A NECESSARY AND SUFFICIENT CONDITION FOR 2 TO BE A PRIMITIVE ROOT OF $2p + 1$

V. P. RAMESH, R. THANGADURAI, M. MAKESHWARI AND SASWATI SINHA

V. P. Ramesh, M. Makeshwari, Saswati Sinha
Department of Mathematics,
Central University of Tamil Nadu,
Thiruvarur, Tamilnadu - 610 005

R. Thangadurai,
Harish-Chandra Research Institute, HBNI
Chhatnag Road, Jhunsi
Allahabad - 211019

For Correspondence:
V. P. Ramesh, (Corresponding Author)
Department of Mathematics,
Central University of Tamil Nadu,
Thiruvarur, Tamilnadu - 610 005
Email: vpramesh@gmail.com

ABSTRACT. Let p be an odd prime such that $2p+1$ is a prime or prime power. Then, in this article, we prove that 2 is a primitive root of $2p+1$ if and only if $p \equiv 1 \pmod{4}$.

Key words: Primitive root, Sophie Germain prime, permutation and orbits of permutation.

AMS subject classification: 11A07, 11A41 and 20F05.

1. Introduction

Gauss proved that the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic if and only if $n = 2, 4, p^k$ or $2p^k$ for all odd primes p and for all positive integers k. For such integers n, the generators are called *primitive roots* of n. Indeed, while studying the periods of rational numbers of the form $1/p$ for a prime $p \neq 2$ or 5, Gauss proved the above result and he conjectured that 10 *is a primitive root of p for infinitely many primes p*. Later E. Artin generalized this conjecture and gave a heuristic argument for a quantitative form of this conjecture and nowadays, it is well-known as *Artin's primitive root conjecture* [4]. Due to these conjectures there are many efforts leading to discoveries around primitive roots of n, to list a few [1, 4, 5, 6].

We will first set up some notations. For any $x \in \mathbb{R}$, $[x]$ denotes the *greatest integer function* i.e., the largest integer less than or equal to x. A prime p is said to be a *Sophie Germain prime* [2] if $2p + 1$ is also a prime. It is expected that there is an infinitude of such primes. Let σ be an element of the symmetric group S_n. It is easy to observe that the following relation is an equivalence relation. For $i, j \in \{1, 2, 3, \ldots, n\}$, we say $i \sim j$ if there exists $k \in \mathbb{Z}$ such that $\sigma^k(i) = j$. The equivalence classes of this relation are called orbits of σ. Furthermore, $\sigma \in S_n$ is said to be a *cycle* of length ℓ, if one of its orbits has ℓ elements and rest of them have only one element.

In this article, we prove the following results.

Theorem 1.1. *Let p be an odd prime such that $2p + 1$ is a prime or prime power. Then 2 is a primitive root of $2p + 1$ if and only if $p \equiv 1 \pmod 4$.*

Lemma 1.2. *Let p be an odd prime such that $2p + 1 = q^k$ for some prime q and some integer $k \geq 2$. Then $q = 3$, k is a prime number and $p \equiv 1 \pmod 4$.*

Lemma 1.3. *For any natural number k, we have*

$$\left[\frac{2^{\phi(3^k)}}{3^k}\right] \equiv 1 \pmod 3,$$

where ϕ is the Euler's totient function.

Corollary 1.4. *For any natural number ℓ,*

$$\left[\frac{2^{\phi(3^\ell)}}{3^\ell}\right] \textit{ divides } \left[\frac{2^{\phi(3^{\ell+1})}}{3^{\ell+1}}\right].$$

From Gauss we know that *"For a prime p, if a is a primitive root of p and p^2, then a is a primitive root of p^ℓ for all $\ell \geq 3$"*. We consider a special case of this statement, namely for $a = 2$, $p = 3$ and in this article we present the following result which is a stronger result for this special case.

Lemma 1.5. *For any $k \in \mathbb{N}$, 2 is a primitive root of 3^k.*

Though, Lemma 1.5 can be proved using the above result of Gauss, in this article we have invoked Lemma 1.3 to give a self-contained proof of this lemma. It is to be noted that these lemmas are useful while proving Theorem 1.1.

In 1969, D. J. Aulicino and Morris Goldfeld [1] have studied the permutation $(n!)$ defined as $(n!) = \prod_{k=0}^{n-1} (1, 2, \ldots, (n-k))$, i.e., the product of first n cycles. They observed a connection between a primitive root of $2n+1$ and the permutation $(n!)$ having only one orbit (which is called as a *transitive permutation*) and proved that *for any natural number n, the permutation $(n!)$ is transitive if and only if $2n + 1$ is a prime for which 2 is a primitive root* [1]. Therefore, we have the following natural corollary from Theorem 1.1.

Corollary 1.6. *Let p be an odd prime. Then the permutation $(p!)$ is transitive if and only if $2p + 1$ is prime and $p \equiv 1 \pmod 4$.*

We performed a few computations with primes up to 3×10^6 and observed that about 4.515% of primes in the above range are such that $2p+1$ is also prime with 2 as a primitive root. Furthermore, the primes $13, 1093$ and 797161 are the only primes in the above range for which 2 is a primitive root and $2p + 1$ is not prime. It is easy to observe that for the above listed primes, $2p + 1$ is an odd power of 3, namely $27 = 3^3, 2187 = 3^7$ and $1594323 = 3^{13}$. We have also estimated that for the prime $p = 695759652988215296899222525183588718147845154 7013$, $2p + 1 = 3^{103}$ with 2 as a primitive root. It is worth mentioning here that the powers of 3 in the representations of $2p + 1$ are also primes.

We state the following lemma (see Theorem 2 of [3]) which will be used while proving Theorem 1.1.

Lemma 1.7. *Let p be an odd prime such that $2p + 1$ is also a prime. Then, we have*

(1) $2p + 1$ *divides* $2^p - 1$, *if* $p \equiv 3 \pmod 4$*;*
(2) $2p + 1$ *divides* $2^p + 1$, *if* $p \equiv 1 \pmod 4$.

2. PROOFS OF LEMMAS 1.2, 1.3 AND 1.5

Let p be an odd prime such that $2p+1=q^k$ for some prime q and for some integer $k \geq 2$. Clearly, $q \geq 3$. Therefore,

$$2p = q^k - 1 = (q-1)(1+q+q^2+\cdots+q^{k-1}).$$

Since $q \geq 3$, by the unique factorization in integers, we conclude that $2 = q-1$ and $p = 1+q+q^2+\cdots+q^{k-1}$. Thus, we get

$$q = 3 \text{ and } p = 1+3+3^2+\cdots+3^{k-1}.$$

Since $3^{2m} \equiv 1 \pmod 4$ and $3^{2m+1} \equiv -1 \pmod 4$, we see that k must be an odd integer. For otherwise, we get $p \equiv 0 \pmod 4$, a contradiction to p being prime. Since k is an odd integer, we get $p \equiv 1 \pmod 4$.

Now, suppose k is not prime, equivalently $k = mn$ for some $1 < m, n < k$, then $3^m - 1$ and $3^n - 1$ are factors of $3^k - 1$ since

$$3^k - 1 = (3^m - 1)(1 + 3^m + 3^{2m} + \cdots + 3^{(n-1)m})$$

which is a contradiction. □

Now we prove Lemma 1.3 by induction on k. When $k = 1$, it is clearly true. We shall assume the result for $k = \ell$ and we prove for $\ell + 1$. Since $2^{\phi(3^\ell)} \equiv 1 \pmod{3^\ell}$, we get

$$2^{\phi(3^\ell)} = \left[\frac{2^{\phi(3^\ell)}}{3^\ell}\right] 3^\ell + 1. \tag{2.1}$$

Taking the 3-rd power both sides and since $3 \cdot \phi(3^\ell) = \phi(3^{\ell+1})$ we get

$$2^{\phi(3^{\ell+1})} = \left[\frac{2^{\phi(3^\ell)}}{3^\ell}\right]^3 3^{3\ell} + \left[\frac{2^{\phi(3^\ell)}}{3^\ell}\right]^2 3^{2\ell+1} + \left[\frac{2^{\phi(3^\ell)}}{3^\ell}\right] 3^{\ell+1} + 1.$$

On simplification, we get,

$$\left[\frac{2^{\phi(3^{\ell+1})}}{3^{\ell+1}}\right] = \left[\frac{2^{\phi(3^\ell)}}{3^\ell}\right] \left(\left[\frac{2^{\phi(3^\ell)}}{3^\ell}\right]^2 3^{2\ell-1} + \left[\frac{2^{\phi(3^\ell)}}{3^\ell}\right] 3^\ell + 1 \right).$$

And, by induction hypothesis, the lemma follows. □

Now, we prove Lemma 1.5 by induction on k. Since 2 is a primitive root of 3, we shall assume that 2 is a primitive root of 3^ℓ for some integer $\ell \geq 2$ and we prove that 2 is a primitive root of $3^{\ell+1}$.

Let the order of 2 modulo $3^{\ell+1}$ be d. Then, $d \mid \phi(3^{\ell+1}) = 2 \cdot 3^{\ell}$. Since 2 is a primitive root of 3^{ℓ}, we get $\phi(3^{\ell}) \mid d$ and therefore it is clear that $d = 2 \cdot 3^{\ell-1}$ or $2 \cdot 3^{\ell}$. By Lemma 1.3, we see that

$$3 \nmid \left[\frac{2^{\phi(3^{\ell})}}{3^{\ell}}\right] \iff 3^{\ell+1} \nmid 2^{2\cdot 3^{\ell-1}} - 1 \text{ (from (2.1))}.$$

Hence, we get $d \neq 2 \cdot 3^{\ell-1}$ and $d = 2 \cdot 3^{\ell}$. And therefore 2 is a primitive root of $3^{\ell+1}$. □

3. Proof of Theorem 1.1

Let p be an odd prime such that $2p + 1 = q^k$ for some odd prime q and for some natural number k.

Case 1. $k = 1$, i.e. both p and $2p + 1$ are primes.

Let us assume that 2 be a primitive root of $2p + 1$ and we prove that $p \equiv 1 \pmod 4$. Suppose, $p \not\equiv 1 \pmod 4$, then $2^p \equiv 1 \mod 2p + 1$ from Lemma 1.7 which is a contradiction to 2 being a primitive root of $2p+1$. Conversely, if $p \equiv 1 \pmod 4$, then again from Lemma 1.7, we have $2^p \equiv -1 \mod 2p + 1$ which implies $2^p \not\equiv 1 \mod 2p + 1$ and hence 2 is a primitive root of $2p + 1$.

Case 2. $k > 1$, i.e. $2p + 1 = q^k$ for some odd prime q and for some natural number $k \geq 2$.

Now, by Lemma 1.2, we conclude that $q = 3$, k is an odd integer and $p \equiv 1 \pmod 4$. Conversely, from Lemma 1.5, it follows that 2 is a primitive root of $2p + 1$. □

Acknowledgment: We thank M. Ram Murty for carefully going through this manuscript and also for various comments improving the presentation and results. We also thank the reviewers of *JRMS* and *The Mathematics Students* for various comments improving the presentation.

References

[1] Aulicino, D. J., and Goldfeld, M., A New Relation Between Primitive Roots and Permutations, *The American Mathematical Monthly*, **76** (1969), no. 6, 664–666.

[2] Burton, D., *Elementary Number Theory*, 7th ed. Tata McGraw-Hill, 2012.

[3] Jaroma, J. H. and Reddy, K. N., Classical and alternative approaches to the Mersenne and Fermat numbers, *The American Mathematical Monthly*, **114** (2007), no. 8, 677–687.

[4] Ram Murty, M., Artin's conjecture for primitive roots, *The Mathematical Intelligencer*, **10** (1988), 59–67.

[5] Ramesh, V. P., Thangadurai, R. and Thatchaayini, R., A Note on Gauss's Theorem on Primitive Roots, *The American Mathematical Monthly*, **126** (2019), no. 3, 252–254.

[6] Yuan, Y. and Wenpeng, Z., On the distribution of primitive roots modulo a prime, *Publicationes Mathematicae Debrecen*, **61** (2002), no. 3-4, 383–391.