The Mathematics Student ISSN: 0025-5742
Vol. 94, Nos. 3-4, July - December (2025), 169–171

WHETHER THE ADDITIVE INVERSE OF A BAD PRIMITIVE ROOT OF P IS A PRIMITIVE ROOT OF P^2?

V. P. RAMESH AND DEVI, S.

(Received : 24 - 04 - 2025 ; Revised : 06 - 06 - 2025)

Abstract. In this article, for any odd prime p, we prove that the additive inverse of a bad primitive root of p is not bad only when $p \equiv 1 \pmod 4$, and for the case $p \equiv 3 \pmod 4$, we estimate a primitive root of p^ℓ from a bad primitive root of p.

1. Introduction

Let $a \in (\mathbb{Z}/n\mathbb{Z})^*$, if the order of a (denoted by $ord_n(a)$) is $\phi(n)$, we say that a is a *primitive root of* n [3]. For any odd prime p and a natural number ℓ, Gauss proved that, *if a is a primitive root of p, then there exists an integer m such that $a + mp$ is a primitive root of p^ℓ. Moreover, if a is a primitive root of p^2, then a is a primitive root of p^ℓ* (see [1, Chapter 8]). In the case $m = 0$ of Gauss's theorem, for any odd prime p, *a primitive root of p is said to be bad if it is not a primitive root of p^2* [2].

In 1974, Cohen et al. [2] analytically proved that *for each $\epsilon > 0$, there exists a constant $P(\epsilon)$ such that for any prime $p > P(\epsilon)$, the number of bad primitive roots of p is bounded above by $p^{\frac{1}{2}+\epsilon}$*. In 2023, Ramesh and Gowtham [4] proved that *the multiplicative inverse of a bad primitive root of p is not bad*.

A question that arises immediately is whether the additive inverse of a bad primitive root of p is also not bad. This is not always true and can be seen by examining the multiplicative group $(\mathbb{Z}/43\mathbb{Z})^*$. It is easy to verify that 19 is a bad primitive root of 43 since $ord_{43}(19) = 42 = ord_{43^2}(19)$,

2020 Mathematics Subject Classification: 11A07,11A41
Key words and phrases: primes, bad primitive root

but the additive inverse of 19, which is 24, is not even a primitive root of 43. We may still ask: Is there a modified statement that is true? In other words, we ask: Is the statement true if we restrict the primes to a suitable class? We observed that if $p \equiv 1 \pmod 4$, then the additive inverse of a bad primitive root of p is not bad. For the other class, namely, $p \equiv 3 \pmod 4$, we estimate a primitive root of p^2 from a bad primitive root of p. Indeed, we have the following observation.

Theorem 1.1. *Let p be an odd prime and ℓ be any natural number. Let a be a primitive root of p.*
(i) If $p \equiv 1 \pmod 4$, then a or $p-a$ is a primitive root of p^ℓ.
(ii) If $p \equiv 3 \pmod 4$, then a or $\lceil \frac{a^2}{p} \rceil p - a^2$ is a primitive root of p^ℓ.

Proof. In order to prove this result, by Gauss's theorem (see [1, Chapter 8]), it is enough to prove the result for $\ell = 2$. Let a be a primitive root of p, then necessarily $p-1 \mid ord_{p^2}(a)$. Thus, $ord_{p^2}(a) = p-1$ or $p(p-1)$.
Case 1. $p \equiv 1 \pmod 4$.

We claim that $ord_p(p-a) = p-1$. For if $ord_p(p-a) = k < p-1$, then, since $1 \equiv (p-a)^k \equiv (-a)^k \pmod p$, we have k is odd, whence $a^{2k} \equiv 1 \pmod p$. Now, since k is odd and $p \equiv 1 \pmod 4$, clearly $2k < p-1$, which is a contradiction to a being a primitive root of p. Thus, $ord_p(p-a) = p-1$.

Now to complete the proof, it is enough to show that if $ord_{p^2}(a) = p-1$, then $ord_{p^2}(p-a) = p(p-1)$ (or equivalently, $(p-a)^{p-1} \not\equiv 1 \pmod{p^2}$). Suppose that $(p-a)^{p-1} \equiv 1 \pmod{p^2}$. By the binomial theorem, $pa^{p-2} + a^{p-1} \equiv 1 \pmod{p^2}$, whence $pa^{p-2} \equiv 0 \pmod{p^2}$. Thus, $p \mid a^{p-2}$, a contradiction. Therefore, we have shown that $p-a$ is a primitive root of p^2, and hence $p-a$ is a primitive root of p^ℓ.
Case 2. $p \equiv 3 \pmod 4$.

We claim that $ord_p(\lceil \frac{a^2}{p} \rceil p - a^2) = p-1$. Clearly, $\frac{p-1}{2}$ is odd and $(\lceil \frac{a^2}{p} \rceil p - a^2)^{\frac{p-1}{2}} \equiv (-a^2)^{\frac{p-1}{2}} \equiv -1 \pmod p$, whence $ord_p(\lceil \frac{a^2}{p} \rceil p - a^2)$ is even, say k. Then, $1 \equiv (\lceil \frac{a^2}{p} \rceil p - a^2)^k \equiv a^{2k} \pmod p$, and since $k \neq \frac{p-1}{2}$, it follows that $ord_p(\lceil \frac{a^2}{p} \rceil p - a^2) = p-1$. Now, we must show that if $ord_{p^2}(a) = p-1$, then $ord_{p^2}(\lceil \frac{a^2}{p} \rceil p - a^2) = p(p-1)$. Indeed, as in the proof of case 1, a similar argument for $(\lceil \frac{a^2}{p} \rceil p - a^2)^{p-1} \equiv 1 \pmod{p^2}$ yields $\lceil \frac{a^2}{p} \rceil p a^{2(p-2)} \equiv 0 \pmod{p^2}$. Thus, $p \mid \lceil \frac{a^2}{p} \rceil$ or $p \mid a^{2(p-2)}$, which is a contradiction. This completes the proof. □

Corollary 1.2. *Let p be an odd prime and ℓ be any natural number. Let a be a bad primitive root of p. Then,*
(i) $p \equiv 1 \pmod 4$ if and only if $p - a$ is a primitive root of p^ℓ.
(ii) $p \equiv 3 \pmod 4$ if and only if $\lceil \frac{a^2}{p} \rceil p - a^2$ is a primitive root of p^ℓ.

Proof. The forward part follows from Theorem 1.1. Conversely, if $p - a$ is a primitive root of p^ℓ, then $a^{\frac{p-1}{2}} \equiv -1 \equiv (p-a)^{\frac{p-1}{2}} \equiv (-a)^{\frac{p-1}{2}} \pmod p$. Thus, $\frac{p-1}{2}$ is even, and hence $p \equiv 1 \pmod 4$. Similarly, if $\lceil \frac{a^2}{p} \rceil p - a^2$ is a primitive root of p^ℓ, then $-(a^2)^{\frac{p-1}{2}} \equiv -1 \equiv (\lceil \frac{a^2}{p} \rceil p - a^2)^{\frac{p-1}{2}} \equiv (-a^2)^{\frac{p-1}{2}} \pmod p$. Thus, $\frac{p-1}{2}$ is odd, and hence $p \equiv 3 \pmod 4$. □

Remark 1.3. It is easy to see from the proof of the above corollary, that the converse of (i) follows for a primitive root of p that is not necessarily bad and the converse of (ii) follows for any element of a multiplicative group modulo p which is not necessarily a bad primitive root of p.

Acknowledgement: We thank Professor R. Thangadurai and the reviewer of *The Mathematics Student* for various comments improving the presentation. This work was supported by the Department of Science and Technology (DST), Government of India, and the Institute of Mathematical Sciences, Chennai.

References

[1] Burton, D. M., *Elementary Number Theory*, 7th ed., McGraw-Hill, 2012.
[2] Cohen, S. D., Odoni, R. W. K., and Stothers, W. W., On the least primitive root modulo p^2, *Bulletin of the London Mathematical Society*, **6** (1974), 42-46.
[3] Gauss, C. F., *Disquisitiones Arithmeticae* (translated by Clarke A. A.), Yale University Press, 1966.
[4] Ramesh, V. P., and Gowtham, R., The inverse of a bad primitive root is not bad, *The American Mathematical Monthly*, **130**(10) (2023), 928.

V. P. Ramesh and Devi, S
Department of Mathematics
Central University of Tamil Nadu
Thiruvarur, Tamil Nadu - 610 005.
E-mail: vpramesh@gmail.com, devisphd22@students.cutn.ac.in