



A NOTE ON GAUSS'S THEOREM ON THE PRIMITIVE ROOTS MODULO p^ℓ

V. P. Ramesh

Department of Mathematics, Central University of Tamil Nadu, Thiruvarur, India
vpramesh@gmail.com

S. Sivakumar

Department of Mathematics, Central University of Tamil Nadu, Thiruvarur, India
sivakumar235781@gmail.com

Received: 2/24/26, Accepted: 8/20/26, Published: 10/7/26

Abstract

We prove that if a is coprime to an odd prime p , there exists a unique m modulo p such that $\text{ord}_{p^2}(a + mp) = \text{ord}_p(a)$. We also provide an explicit characterization of the primitive roots of p^ℓ with respect to the primitive roots of p .

1. Introduction and Main Results

Throughout this article, p is an odd prime, $\ell \geq 1$ is an integer, and $\text{ord}_n(a)$ denotes the order of a in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$. Any generator of $(\mathbb{Z}/n\mathbb{Z})^*$ is called a *primitive root* of n .

In 1801, Gauss [4] proved that the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic if and only if $n = 2, 4, p^\ell$, or $2p^\ell$ for an odd prime p . Further, he proved that if g is a primitive root of p and p^2 , then g is a primitive root of p^ℓ for all $\ell > 2$. Gauss formulated a method to look for primitive roots of p^ℓ from the primitive roots of p , and he observed the following result.

Theorem 1 (see Chapter 8 of [1]). *For any odd prime p , if g is a primitive root of p , then there exists k such that $g + kp$ is a primitive root of p^2 and hence a primitive root of p^ℓ for all $\ell \geq 2$.*

The primitive roots of p that are not primitive roots of p^2 are referred to as the *bad primitive roots* of p (see Cohen et al. [2]). In 2019, Ramesh et al. [5] proved that for any odd prime p , the number of bad primitive roots of p is less than $\frac{1}{2}\phi(p-1)$.

While studying Gauss's theorem (Theorem 1), a question that arises immediately is the following, which generalizes the concept of bad primitive roots.

Question 1. For a given primitive root g of p , does there exist k for which $g + kp$ is not a primitive root of p^2 and hence, not a primitive root of p^ℓ for all $\ell > 1$?

More generally, we wish to consider Question 1 for every element of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$. Indeed, we have the following observation, which states that for any $a \in (\mathbb{Z}/p\mathbb{Z})^*$ there exists a unique k modulo p such that the order of $(a + kp)$ modulo p^2 is equal to the order of a modulo p .

Theorem 2. *Let p be an odd prime and let a be an integer such that $(a, p) = 1$. Then, there exists a unique m modulo p such that $\text{ord}_{p^2}(a + mp) = \text{ord}_p(a)$. That is, for every $\mathcal{P}_a$, there exists a unique $x \in \mathcal{P}_a$ such that $\text{ord}_{p^2}(x) = \text{ord}_p(x)$, where $\mathcal{P}_a = \{x \in (\mathbb{Z}/p^2\mathbb{Z})^* : x \equiv a \pmod{p}\}$.*

In the special case of Theorem 2, in which g is a primitive root of p , we have a unique k modulo p such that $g + kp$ is not a primitive root of p^2 (see Corollary 1). Clearly, if $k = 0$, then g is a bad primitive root of p .

Corollary 1. *Let g be a primitive root of p . Then there exists a unique m modulo p such that $g + mp$ is not a primitive root of p^2 . That is, there exists a unique $x \in \mathcal{P}_g$, such that $\text{ord}_{p^2}(x) = p - 1$.*

Further, if g is a primitive root of p , then $g + kp$ is a primitive root of p^2 for any k except the unique k modulo p given by Corollary 1. In 1975, Robbins [6] showed that if g is a primitive root of p , then $g^p - gp$ is a primitive root of p^2 . We ask the next question.

Question 2. Is it possible to formulate a description of the primitive roots of p^2 from the primitive roots of p ?

The answer is provided by the following theorem, which is a generalization of Robbins's result [6] and also a consequence of Theorem 2.

Theorem 3. *Let p be an odd prime, g be a primitive root of p , and $k \not\equiv 0 \pmod{p}$. Then, $g^p + kp \pmod{p^2}$ is a primitive root of p^ℓ for all $\ell > 1$.*

2. Preliminaries

To begin with, we recall the following elementary facts.

Lemma 1 (see Lemma 1 of [5]). *For any element $a \in (\mathbb{Z}/p^2\mathbb{Z})^*$, we have*

$$\text{ord}_{p^2}(a + kp) = \text{ord}_p(a) \text{ or } p \cdot \text{ord}_p(a).$$

Lemma 2 (see Theorem 7 of Chapter 2.3 of [3]). *Let G be a finite cyclic group of order n and let $\ell | n$. Then, the number of elements of G of order ℓ is exactly equal to $\phi(\ell)$.*

3. Proofs of Theorems

Before we prove our main results, we need a relation on $(\mathbb{Z}/p^2\mathbb{Z})^*$ as follows: for any $a, b \in (\mathbb{Z}/p^2\mathbb{Z})^*$, we define the relation $\sim$ as $a \sim b$ if $a \equiv b \pmod{p}$. It is easy to see that $\sim$ is an equivalence relation and induces the partition $\mathcal{P} = \{\mathcal{P}_a : a = 1, 2, \dots, p-1\}$, where $\mathcal{P}_a = \{a + kp \pmod{p^2} : k = 0, 1, \dots, p-1\}$, illustrated in Figure 1. It is easy to see that for any $b \in \mathcal{P}_a$, it follows from Lemma 1 that $\text{ord}_{p^2}(b) = \text{ord}_p(a)$ or $p \cdot \text{ord}_p(a)$.

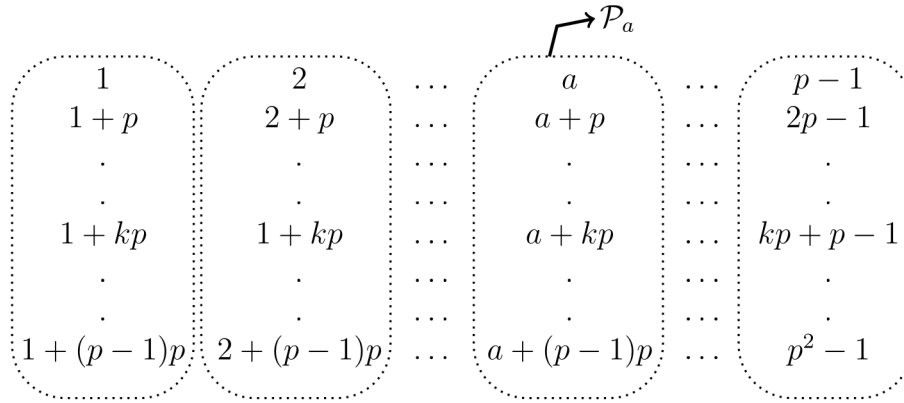


Figure 1: The partition $\mathcal{P}$ of $(\mathbb{Z}/p^2\mathbb{Z})^*$ induced by the equivalence relation $\sim$.

We now proceed to show that for any homomorphism f on $(\mathbb{Z}/p^2\mathbb{Z})^*$, if $a \sim b$ then $f(a) \sim f(b)$, that is, $f(\mathcal{P}_a) \subseteq \mathcal{P}_{f(a)}$. Further, we present a condition on f so that $f(\mathcal{P}_a) = \mathcal{P}_{f(a)}$, and f behaves like an automorphism by preserving the order of elements of $\mathcal{P}_a$. There are, nevertheless, advantages in such an equivalence relation, for we may be able to make observations on the order of elements of $\mathcal{P}_a$.

Now, let $f : (\mathbb{Z}/p^2\mathbb{Z})^* \rightarrow (\mathbb{Z}/p^2\mathbb{Z})^*$ be a homomorphism, and let g be a primitive root of p^2 . Then, $f(g) = g^n \pmod{p^2}$ for some unique $0 \leq n < \phi(p^2)$. Now, for any $x \in (\mathbb{Z}/p^2\mathbb{Z})^*$, there exists $m \in \mathbb{Z}$ such that $x \equiv g^m \pmod{p^2}$ and hence $f(x) = f(g^m) = f(g)^m = g^{mn} \pmod{p^2} \equiv x^n \pmod{p^2}$. Therefore, for every homomorphism f on $(\mathbb{Z}/p^2\mathbb{Z})^*$, there exists a unique $0 \leq n < \phi(p^2)$ such that $f(x) = x^n \pmod{p^2}$ for all $x \in (\mathbb{Z}/p^2\mathbb{Z})^*$. In addition, for any integer $0 \leq n < \phi(p^2)$, the function $f(x) = x^n \pmod{p^2}$ is a homomorphism on $(\mathbb{Z}/p^2\mathbb{Z})^*$, and there are exactly $\phi(p^2)$ of them.

Lemma 3. *Let p be an odd prime, $f : (\mathbb{Z}/p^2\mathbb{Z})^* \rightarrow (\mathbb{Z}/p^2\mathbb{Z})^*$ be a homomorphism, and $a \in (\mathbb{Z}/p^2\mathbb{Z})^*$. Then $f(\mathcal{P}_a) \subseteq \mathcal{P}_{f(a)}$.*

Proof. Let $f : (\mathbb{Z}/p^2\mathbb{Z})^* \rightarrow (\mathbb{Z}/p^2\mathbb{Z})^*$ be a homomorphism and let $a, b \in (\mathbb{Z}/p^2\mathbb{Z})^*$ such that $a \sim b$. Then, by the above paragraph, $f(x) = x^n \pmod{p^2}$ for some

unique $0 \leq n < \phi(p^2)$. Thus,

$$\begin{aligned} f(a) - f(b) &\equiv (a^n - b^n) \pmod{p^2} \\ &\equiv (a - b) \left(\sum_{i=0}^{n-1} a^i b^{n-1-i} \right) \pmod{p^2} \\ &\equiv 0 \pmod{p} \quad (\text{since } p|a - b). \end{aligned}$$

Hence, $f(a) \sim f(b)$, or equivalently, $f(\mathcal{P}_a) \subseteq \mathcal{P}_{f(a)}$. $\square$

Lemma 4. *Let p be an odd prime and $a \in (\mathbb{Z}/p^2\mathbb{Z})^*$. Let f be a homomorphism on $(\mathbb{Z}/p^2\mathbb{Z})^*$ defined by $f(x) = x^n \pmod{p^2}$, for some n coprime to both p and $\text{ord}_{p^2}(a)$. Then, f restricted to $\mathcal{P}_a$ is one-to-one (that is, $f(\mathcal{P}_a) = \mathcal{P}_{f(a)}$), and for any $b \sim a$, we have $\text{ord}_{p^2}(f(b)) = \text{ord}_{p^2}(b)$.*

Proof. Let $x, y \in \mathcal{P}_a$ and let $f(x) = f(y)$. Then it follows from the definition of f that

$$0 \equiv (x^n - y^n) \pmod{p^2} \equiv (x - y) \sum_{r=0}^{n-1} x^{n-1-r} y^r \pmod{p^2}.$$

Since $x \equiv y \equiv a \pmod{p}$ and $(n, p) = 1$, it follows that

$$\sum_{r=0}^{n-1} x^{n-1-r} y^r \equiv \sum_{r=0}^{n-1} a^{n-1} \equiv na^{n-1} \not\equiv 0 \pmod{p}.$$

Thus, $x - y \equiv 0 \pmod{p^2}$, and since $0 < x < p^2$ and $0 < y < p^2$, it follows that $x = y$. Therefore, $f|_{\mathcal{P}_a}$ is one-to-one.

Next, we show that if $b \sim a$, then $\text{ord}_{p^2}(f(b)) = \text{ord}_{p^2}(b)$. Letting $b \sim a$, it then follows from Lemma 1 that $\text{ord}_{p^2}(a) = \text{ord}_p(a)$ or $p \cdot \text{ord}_p(a)$, and also that $\text{ord}_{p^2}(b) = \text{ord}_p(a)$ or $p \cdot \text{ord}_p(a)$. Now, since $(\text{ord}_{p^2}(a), n) = 1$ and $(n, p) = 1$, it follows that $(\text{ord}_p(a), n) = 1$. Hence, $(\text{ord}_{p^2}(b), n) = 1$, which implies that $\text{ord}_{p^2}(b^n) = \text{ord}_{p^2}(b)$. That is, $\text{ord}_{p^2}(f(b)) = \text{ord}_{p^2}(b)$. $\square$

We now proceed to prove our main results via these lemmas.

Proof of Theorem 2. Let g be a primitive root of p^2 . Then, clearly, g is a primitive root of p . Let $\mathcal{P}_a \in \mathcal{P}$ and $\text{ord}_p(a) = \ell|p - 1$. By Lemma 2,

$$|\{b \in (\mathbb{Z}/p\mathbb{Z})^* : \text{ord}_p(b) = \ell\}| = \phi(\ell).$$

Hence, let $a_1, a_2, \dots, a_{\phi(\ell)}$ be the distinct elements of $(\mathbb{Z}/p\mathbb{Z})^*$ such that $\text{ord}_p(a_i) = \ell$. It is easy to see that for any $i \neq j$, we have $a_i \not\equiv a_j \pmod{p}$, and hence

$\mathcal{P}_{a_1}, \mathcal{P}_{a_2}, \dots, \mathcal{P}_{a_{\phi(\ell)}}$ are distinct partition elements of $\mathcal{P}$. Moreover, by Lemma 1 it follows that $\text{ord}_{p^2}(b) = \ell$ or ℓp , for any $b \in \mathcal{P}_{a_i}$. By Lemma 2, we have

$$|\{b \in (\mathbb{Z}/p^2\mathbb{Z})^* : \text{ord}_{p^2}(b) = \ell \text{ or } \ell p\}| = p\phi(\ell) \text{ and } \left| \bigcup_{i=1}^{\phi(\ell)} \mathcal{P}_{a_i} \right| = p\phi(\ell).$$

Thus, all the elements of $(\mathbb{Z}/p^2\mathbb{Z})^*$ of order ℓ or ℓp , are in $\bigcup_{i=1}^{\phi(\ell)} \mathcal{P}_{a_i}$.

Now it is enough to prove that for every $\mathcal{P}_{a_i}$, there exists a unique $x \in \mathcal{P}_{a_i}$ such that $\text{ord}_{p^2}(x) = \text{ord}_p(x) = \ell$. By Lemma 2, the total number of elements of order ℓ in $(\mathbb{Z}/p^2\mathbb{Z})^*$ is $\phi(\ell) < p$, and since $|\mathcal{P}_{a_i}| = p$, the partition $\mathcal{P}_{a_i}$ contains at least one element b_i of order ℓp , whence there exists t_i such that $b_i \equiv g^{t_i \frac{p-1}{\ell}} \pmod{p^2}$ and $(t_i, \ell p) = 1$. Thus, for any t_i and t_j , there exists n_{ij} coprime to ℓp such that $t_i n_{ij} \equiv t_j \pmod{\ell p}$. We define a function $f_{ij} : (\mathbb{Z}/p^2\mathbb{Z})^* \rightarrow (\mathbb{Z}/p^2\mathbb{Z})^*$ as follows: $f_{ij}(x) = x^{n_{ij}} \pmod{p^2}$. It is clear from our earlier remark that f_{ij} is a homomorphism and

$$f_{ij}(b_i) = b_i^{n_{ij}} \pmod{p^2} \equiv g^{t_i n_{ij} \frac{p-1}{\ell}} \equiv g^{t_j \frac{p-1}{\ell}} \equiv b_j \pmod{p^2}.$$

Further, it follows from Lemma 4 that $f_{ij}|_{\mathcal{P}_{a_i}}$ is a one-to-one function onto $\mathcal{P}_{a_j}$ preserving the order of elements. But since there are exactly $\phi(\ell)$ elements of order ℓ in $(\mathbb{Z}/p^2\mathbb{Z})^*$ and by Lemma 1, it follows that every $\mathcal{P}_{a_i}$ has exactly one element x_i such that $\text{ord}_{p^2}(x_i) = \ell = \text{ord}_p(x_i)$. $\square$

It is interesting to note that for any primitive root $1 < g < p$ of p , if the corresponding unique $m \pmod{p} \neq 0$, then g is also a primitive root of p^2 , hence p^ℓ for all $\ell > 1$. We now proceed to prove Theorem 3.

Proof of Theorem 3. Let $\text{ord}_p(g) = p-1$. Then by Theorem 2, there exists a unique m modulo p such that $\text{ord}_{p^2}(g + mp) = \text{ord}_p(g) = p-1$. Since $g^p \equiv g \pmod{p}$, we have $g^p \in \mathcal{P}_g$, that is, $g^p \equiv g + kp \pmod{p^2}$ for some integer k such that $0 \leq k \leq p-1$. Now, by Lemma 1, $\text{ord}_{p^2}(g^p) = p-1$ or $p(p-1)$. Since $(g^p)^{p-1} \equiv 1 \pmod{p^2}$, then necessarily $\text{ord}_{p^2}(g^p) = p-1$. This implies that $g^p \equiv g + mp \pmod{p^2}$ for the unique m modulo p , and hence $g^p + kp \not\equiv g + mp \pmod{p^2}$ for all $k \not\equiv 0 \pmod{p}$. Hence, $g^p + kp \pmod{p^2}$ is a primitive root of p^2 for all $k \not\equiv 0 \pmod{p}$, and we have therefore proved that, $g^p + kp \pmod{p^2}$ is a primitive root of p^ℓ for all $\ell > 1$. $\square$

In fact, the converse of Theorem 3 is also true. More generally, let p be an odd prime, and ℓ be a positive integer. Then, h is a primitive root of p^ℓ if and only if there exists a primitive root g of p and $k \not\equiv 0 \pmod{p}$ such that $h = g^p + kp$.

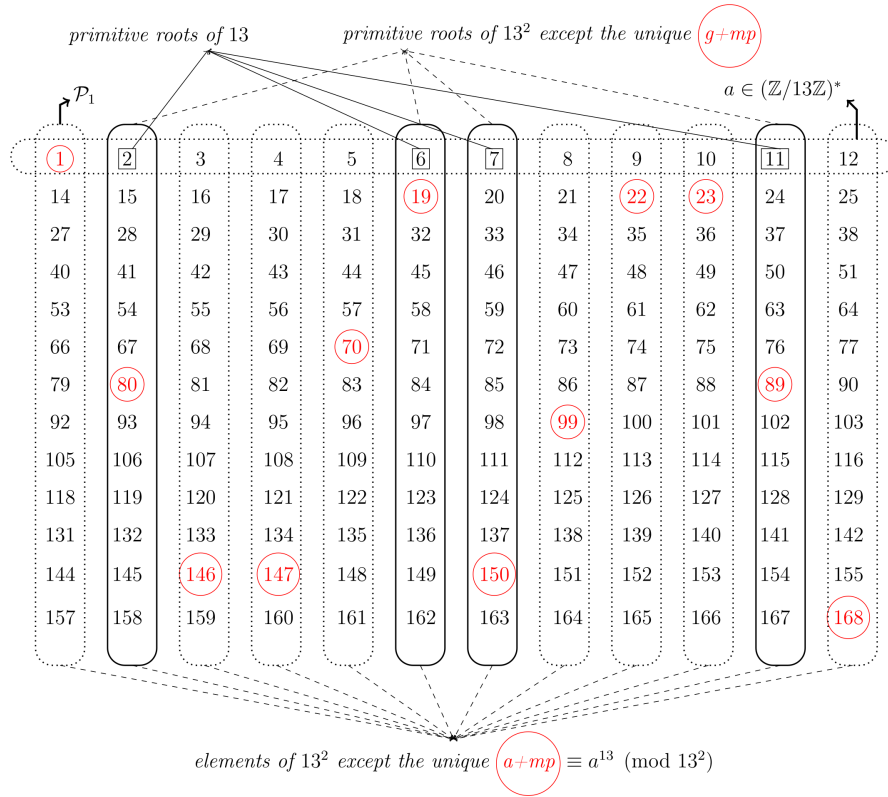
Acknowledgements. The authors gratefully acknowledge the referee's careful reading of the manuscript and also for the various comments improving the presentation. This work was supported by the Anusandhan National Research Foundation (MTR\2023\001373) and the Institute of Mathematical Sciences, Chennai.

References

- [1] D. M. Burton, *Elementary Number Theory*, 6th ed., McGraw-Hill, Boston, MA, 2006.
- [2] S. D. Cohen, R. W. Odoni, and W. W. Stothers, On the least primitive root modulo p^2 , *Bull. London Math. Soc.* **6** (1) (1974), 42–46.
- [3] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004.
- [4] C. F. Gauss, *Disquisitiones Arithmeticae*, Gerhard Fleischer, Leipzig, 1801.
- [5] V. P. Ramesh, R. Thangadurai, and R. Thatchaayini, A note on Gauss's theorem on primitive roots, *Amer. Math. Monthly* **126** (3) (2019), 252–254.
- [6] N. Robbins, Calculating a primitive root $\pmod{p^e}$, *Math. Gaz.* **59** (409) (1975), 195.

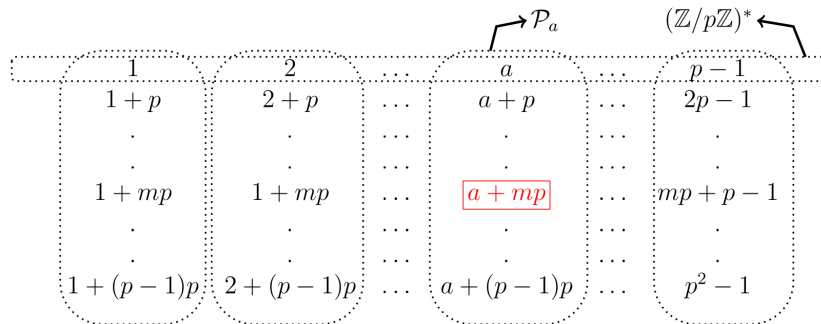
A. Appendix- Graphical Illustration of Theorem 2

Numerically



For all $a \in (\mathbb{Z}/13\mathbb{Z})^*$, there exists a unique $m \pmod{13}$ such that $ord_{13^2}(a + 13m) = ord_{13}(a)$.

Abstractly



For all $a \in (\mathbb{Z}/p\mathbb{Z})^*$, there exists a unique $m \pmod{p}$ such that $ord_{p^2}(a + mp) = ord_p(a)$.