Taylor & Francis
Taylor & Francis Group

The American Mathematical Monthly

ISSN: 0002-9890 (Print) 1930-0972 (Online) Journal homepage: https://www.tandfonline.com/loi/uamm20

A Note on Gauss's Theorem on Primitive Roots

V. P. Ramesh, R. Thangadurai & R. Thatchaayini

NOTES

Edited by **Vadim Ponomarenko**

A Note on Gauss's Theorem on Primitive Roots

V. P. Ramesh, R. Thangadurai, and R. Thatchaayini

Abstract. In this note, we refine Gauss's famous theorem on the existence of primitive roots modulo p^ℓ for every odd prime number p and for every integer $\ell \geq 1$ and observe the following: For an odd prime number $p \geq 5$, at least half of the primitive roots modulo p are primitive roots modulo p^ℓ for every integer $\ell \geq 2$.

Throughout this note, $p \geq 5$ is an odd prime number and $\ell \geq 1$ is an integer. By a *primitive root* modulo p^ℓ, we mean *a generator* of the multiplicative group $\left(\mathbb{Z}/p^\ell\mathbb{Z}\right)^*$. For an element $g \in \left(\mathbb{Z}/p^\ell\mathbb{Z}\right)^*$, the *order of* g is denoted by $\mathrm{ord}_{p^\ell}(g)$ and defined to be the least positive integer m such that $g^m \equiv 1 \pmod{p^\ell}$. In particular, if g is a primitive root modulo p^ℓ, then $\mathrm{ord}_{p^\ell}(g) = p^{\ell-1}(p-1)$.

In 1801, while studying the periods of the unit fractions written in base 10, C. F. Gauss proved that *the multiplicative group* $(\mathbb{Z}/n\mathbb{Z})^*$ *is a cyclic group if and only if* $n = 2, 4, p^\ell$, *or* $2p^\ell$ *for any odd prime* p *and for any integer* $\ell \geq 1$ (see article 315 and page 379 of [4]). Indeed, in order to prove that the group $\left(\mathbb{Z}/p^\ell\mathbb{Z}\right)^*$ is cyclic, first he proved the same for $\ell = 1$ and then he proved the following theorem. We refer to Chapter 8 of [1].

Gauss's theorem. *For any odd prime number* p*, if* g *is a primitive root modulo* p*, then there exists an integer* m *such that* $g + mp$ *is a primitive root modulo* p^ℓ *for every integer* $\ell \geq 2$*. Moreover, if* a *is a primitive root modulo* p^2*, then* a *is a primitive root modulo* p^ℓ *for every integer* $\ell \geq 3$*.*

Since the total number of primitive roots modulo p is $\phi(p-1)$, where ϕ is the Euler phi function, we have the following natural question:

Question 1. *Among the* $\phi(p-1)$ *primitive roots modulo* p*, how many are actually a primitive root modulo* p^ℓ *for every integer* $\ell \geq 2$*? In other words, how many primitive roots modulo* p *satisfy Gauss's theorem with* $m = 0$*?*

In order to answer Question 1, by Gauss's theorem, it is enough to answer Question 1 for $\ell = 2$. That is, we need to compute the number of primitive roots modulo p that are primitive roots modulo p^2. Indeed, we have the following observation.

Theorem 1. *Let* p *be an odd prime number. Then at least* $\phi(p-1)/2$ *primitive roots modulo* p *are primitive roots modulo* p^ℓ *for every integer* $\ell \geq 2$*.*

doi.org/10.1080/00029890.2019.1550340
MSC: Primary 11A07, Secondary 11A41

In 1974, Cohen, Odoni, and Stothers [2], using analytic techniques, proved a stronger estimate than in Theorem 1, for all sufficiently large primes p. However, the proof of Theorem 1 is elementary and the result holds for all primes $p \geq 5$.

We recall the following two elementary group theory lemmas which are useful in proving Theorem 1.

Lemma 1. *For any element $a \in (\mathbb{Z}/p\mathbb{Z})^*$, we have*

$$ord_{p^2}(a) = ord_p(a) \text{ or } ord_{p^2}(a) = ord_p(a) \cdot p.$$

Proof. Let $\text{ord}_p(a) = r$ and $\text{ord}_{p^2}(a) = s$. Then, by definition, r divides s.

Since $a^r \equiv 1 \pmod{p}$, we can write $a^r = pu + 1$ for some integer u and hence we have $a^{rp} = (pu+1)^p \equiv 1 \pmod{p^2}$. Therefore, by definition, s divides rp. Since s divides rp and r divides s, we conclude that $s = r$ or $s = rp$, as desired. ∎

Lemma 2 (see [3]). *Let G be a finite cyclic group of order n. If an integer $d \geq 1$ divides n, then the number of elements of G of order d is precisely $\phi(d)$.*

Proof of Theorem 1. In order to prove Theorem 1, by Gauss's theorem, it is enough to prove the theorem for $\ell = 2$. By Lemma 1, it is enough to prove the following claim.

Claim. Among the $\phi(p-1)$ primitive roots g modulo p, there are at least $\phi(p-1)/2$ of them that satisfy $\text{ord}_{p^2}(g) \neq p - 1$.

Let $S = \{g \in (\mathbb{Z}/p\mathbb{Z})^* : \text{ord}_{p^2}(g) = p - 1 = \text{ord}_p(g)\}$ be a subset of $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^*$; we treat this set S as a subset of $\{1, 2, \ldots, p-1\}$. If possible, we assume that $|S| \geq 1 + (\phi(p-1)/2)$. Define another subset $T = p^2 - S = \{p^2 - g : g \in S\}$ of $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^*$, which is clearly a subset of $\{p^2 - p + 1, p^2 - p + 2, \ldots, p^2\}$. Hence, we get $T \cap S = \emptyset$ and

$$|T \cup S| = |T| + |S| \geq 2(1 + (\phi(p-1)/2)) > \phi(p-1) + 1. \tag{1}$$

To finish the proof of the claim, we shall prove that, for some integer t, there are at least $\phi(t) + 1$ elements $a \in \left(\mathbb{Z}/p^2\mathbb{Z}\right)^*$ with the property that $\text{ord}_{p^2}(a) = t$, which contradicts Lemma 2.

Let $b \in T$ be any element. Hence there exists $a \in S$ such that $b = p^2 - a$. First note that if $\text{ord}_{p^2}(b) = t < p - 1$, then t cannot be even. If so, then

$$1 \equiv b^t = (p^2 - a)^t \equiv (-1)^t a^t = a^t \pmod{p^2} \implies \text{ord}_{p^2}(a) \leq t < p - 1,$$

a contradiction. Hence, we assume that $\text{ord}_{p^2}(b) = t$ for some odd integer t. Also, since $t | p(p-1)$ and t is odd, we have $2t | p - 1$.

Case 1. $p \equiv 1 \pmod{4}$.

In this case, since 4 divides $(p-1)$ and t is odd, we get $2t < p - 1$. Therefore, we get

$$1 \equiv b^{2t} = (p^2 - a)^{2t} \equiv a^{2t} \pmod{p^2} \implies \text{ord}_{p^2}(a) \leq 2t < p - 1,$$

a contradiction. Thus, in this case, any element $b \in T$ has order $\text{ord}_{p^2}(b) = p - 1$. By (1), we see that the number of elements $c \in \left(\mathbb{Z}/p^2\mathbb{Z}\right)^*$ of order $p - 1$ is at least $|T \cup S| > \phi(p-1) + 1$, which proves the claim and hence the theorem in this case.

Case 2. $p \equiv 3 \pmod 4$.

Note that if $2t < p-1$, then we have $\text{ord}_{p^2}(a) \le 2t < p-1$, a contradiction. Hence, we assume that $2t = p-1$. We define the set $S^2 = \{a^2 : a \in S\}$. Note that $|S^2| = |S|$. Since $\max(S^2) \le (p-1)^2$ and $\min(T) \ge p^2 - p + 1 > (p-1)^2$, we conclude that $S^2 \cap T = \emptyset$. Thus, we get

$$|S^2 \cup T| = |S^2| + |T| > \phi(p-1) + 1 = \phi(t) + 1. \tag{2}$$

Note also that any element $b \in S^2$ is of order t. To see this, let $b \in S^2$ be any element. Then $b = a^2$ for some $a \in S$. Therefore,

$$\text{ord}_{p^2}(b) = \text{ord}_{p^2}(a^2) = (p-1)/2 = t.$$

Since any element of T is of order t, by (2), we get the number of elements of $(\mathbb{Z}/p^2\mathbb{Z})^*$ of order t is at least $\phi(t) + 1$, which contradicts Lemma 2. This proves the claim and hence the theorem. ■

ACKNOWLEDGMENTS. We thank the referees for carefully going through this manuscript and for the various suggestions to improve the presentation.

REFERENCES

[1] Burton, D. (2006). *Elementary Number Theory*, 6th ed. New Delhi: Tata McGraw-Hill.
[2] Cohen, S. D., Odoni, R. W. K., Stothers, W. W. (1974). On the least primitive root modulo p^2. *Bull. Lond. Math. Soc.* 6: 42–46.
[3] Gallian, J. A. (1999). *Contemporary Abstract Algebra*, 4th ed. New Delhi: Narosa Publishing House.
[4] Gauss, C. F. (1966). *Disquisitiones Arithmeticae*. (Arthur, A., Clarke, S. J., trans.) New Haven/London: Yale Univ. Press.

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

Harish-Chandra Research Institute, HBNI, Chhatnag Road, Jhunsi, Allahabad, India
thanga@hri.res.in

Department of Mathematics, Central University of Tamilnadu, Thiruvarur, India
thatchaarajacholan@gmail.com