Elementary Number Theory

Atrajit Sarkar

November 14, 2025

Abstract

In this article I want to share some of my thoughts that I found interesting during my study on Elementary Number Theory by David M. Burton [DMB7] and other referrences that is included in the referrence section.

Contents

1 Finding Primitive Roots

1.1 Finding for p^2

We have primitive root of p, let that be r. Then $r^{p-1} \equiv 1 \mod p$. Now we have if $r^{p-1} \not\equiv 1 \mod p^2$ then r is the primitive root of p^2. Then we have total number of primitive roots are $\phi(\phi(p^2)) = (p-1)\phi(p-1)$. Our goal here is to find explicitly what are they.

Claim: If $r^{p-1} \equiv 1 \mod p^2$ then we have for $r' = r+kp \quad \forall k = 1(1)(p-1)$, $(r')^{p-1} \not\equiv 1 \mod p^2$ and hence we have in total $p-1$ many incongruent primitive roots of p^2 for each r with this property.

Claim: For $r^{p-1} \not\equiv 1 \mod p^2$ we already have it to be a primitive root. Then considering the set $\{r+kp \mid \quad 0 < k < p\}$. There exists exactly one elelemnt in this set such that $(r+kp)^{p-1} \equiv 1 \mod p^2$. Hence we get exactly $p-1$ primitive roots. So intotal $(p-1)\phi(p-1)$ many. And hence they are the exact primitive roots of p^2.

Now, we are going to find the exact form of k for which $(r+kp)^{p-1} \equiv 1 \mod p^2$ so that we can easily find out it and exclude it from primitive roots set.

Note that $r^{p-1} \not\equiv 1 \mod p^2$ in this case and $r^{p-1} \equiv 1 \mod p$ that means $r^{p-1} = 1 + pk_1 + p^2k_2$, where $p \nmid k_1$. $(r+kp)^{p-1} \equiv r^{p-1} + kp(p-1)r^{p-2} \equiv 1 + pk_1 - kpr^{p-2} \mod p^2$. Now, for $k \equiv k_1 r \mod p$, we have the desired result. Now, as k_1, r is unique for each r hence is k hence we exclude only one member.

1.2 Finding for p^k

Now we use the idea got in the above section. So, we have the following lemma.

Lemma 1.2.1. *If r is a primitive root of p^2 then $r^{p^{k-2}(p-1)} \not\equiv 1 \mod p^k$.*

and we have the following corollary

Corollary 1.2.2. *If r is a primitive root of p^2 then $(r+kp^2)^{p^{k-2}(p-1)} \not\equiv 1 \mod p^k$ for all $k = 1, \cdots p^{k-2} - 1$ and hence we have for each primitive root of p^2, p^{k-2} many primitive roots for p^k.*

Using lemma1.2.1 and corollary 1.2.2 we have total number of primitive roots for p^k is $p^{k-2}(p-1)\phi(p-1) = \phi(\phi(p^k))$. And hence these elemets are explicitly all the primitive roots of p^k.

1.3 Finding for $2p^k$

Lemma 1.3.1. *If r is a primitive root of p^k so is for $2p^k$.*

Using this lemma 1.3.1 and the fact that $\phi(2p^k) = \phi(p^k)$ we have all the pimitive roots of p^k are exactly the primitive roots of $2p^k$.

1.4 Summary

Now all together if we are given any composite number n and we are to find the primitive root of it we just need to check its form. Suppose $n = 2p^k$ then we find the primitive root of it in the followign steps:

1. First find one primtive root of p using trial and error method. Just we need to check all the devisors of $p-1$ upto $p-1/2$. After getting one such say r. Then we get the other primtive roots as $\{r^m \mid \quad gcd(m, p-1) = 1\}$.

2. Now we are going to find primitive roots of p^2. For that use the subsection 1.1.

3. Now we are going to find primitive roots of p^k. To do that use subsection 1.2. This step is easiest one after finding all the primitive roots of p^2.

4. Now finally these are explicitly the primitive roots of $2p^k \mod 2p^k$ by subsection 1.3.

References

[DMB7] D. M. Burton, *Elementary Number Theory*, 7th ed. 2011, pp. 147–163, Accessed on 2025-11-14. [Online]. Available: https://www.researchgate.net/profile/Issam_Kaddoura/post/Do-irrational-numbers-exist-in-nature/attachment/5f580f02f97a8800014574a2/AS%3A933631606403072%401599606529112/download/david-m-burton-elementary-number-theory-mcgraw-hill-education-2010.pdf.