Elementary Number Theory

Atrajit Sarkar

November 13, 2025

Abstract

Hello

Contents

1 Primitive Roots

1.0.1 primitive roots of 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 $\{r + kp| \quad 0 < k < p\}$. 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.