A. **Applying Lagrange's Theorem.** We give a corollary of Lagrange's theorem.

Corollary. Let p be **prime** and

The congruence $x^d - 1 \equiv 0 \mod p$ has exactly

Proof. By Fermat's theorem, the congruence

$x^{p-1} - 1 \equiv 0 \mod p$

is satisfied by the $p - 1$ incongruent integers:

The factorization coming from the geometric sum formula

general factorization $\to t^k - 1 =$

and the asumption that

yield

$x^{p-1} - 1 =$

Therefore each of the $p - 1$ solutions $[1 \dots p - 1]$ of $x^{p-1} - 1 \equiv 0 \mod p$ satisfies

By Lagrange's Theorem, the two congruences respectively have

But the sum of these quantities must attain value:

This is only possible if the number of solutions in each case attains its:

□

B. **Existence of Primitive Roots.** We show that every prime has a primitive root.

Theorem. Let p a prime. Then p has a primitive root.

Proof. The possible orders of integers modulo p are

We will prove the following lemma, which is stronger than the theorem.

Lemma. For each $d \mid p-1$, there are exactly

Proof. Let $\psi(d)$ denote the number of incongruent order d integers.

Thus our aim is to show, for each $d \mid p-1$, that:

We use strong induction on d.

Base Case. Let $d = 1$. Up to congruence modulo p, the only order 1 integer is:

So: $\psi(1) =$

Strong Inductive Assumption. Let divisor $d \mid p-1$ be given.

assume $\rightarrow$ ψ agrees with ϕ at all divisors d' of $p-1$ such that:

Inductive Step.

goal $\rightarrow$

By the theorem from the last page, the congruence

$x^d - 1 \equiv 0 \mod p$

has exactly d incongruent solutions, namely the integers whose order is

Therefore

$d = [\text{number of mod } p \text{ roots of } x^d - 1] =$

By induction, ψ matches ϕ on those divisors d' less than d, and thus

$\cdots =$

Next we use that $\phi * \mathbb{1} = \mathrm{id}$ to obtain

$\cdots =$

In sum we have shown:

□

Example 1. Let p be an odd prime and let r be a primitive root of p. Prove that

$r^{(p-1)/2} \equiv -1 \mod p$

Thus, if further $p \equiv 1 \mod 4$, then the solutions to $x^2 \equiv -1 \mod p$ are:

Demonstrate this when $p = 13$, which has 2 as a a primitive root.

Solution. We show $x = r^{(p-1)/2}$ satisfies the congruence

$x^2 - 1 \equiv 0 \mod p$

But factoring $x^2 - 1 \equiv 0 \mod p$ yields

and then because p is prime, either

But solution $x = r^{(p-1)/2}$ is not congrurent to 1 modulo p, because otherwise

So solution $x = r^{(p-1)/2}$ must be:

We give the roots of -1 in the case of $p = 13$, using primitive root $r = 2$.

and we confirm

□

Powers of Two. We show powers of two generally don't have primitive roots.

Theorem. The only positive powers of 2 that have primitive roots are 2 and 4.

Proof. Evidently 1 is a primitive root of 2, and 3 is a primitive root of 4.

The theorem will then follow from the lemma below, as the lemma would imply

Lemma. Let $k \geqslant 3$ be an integer and a be odd. Then

Proof. Note that $\phi(2^k)/2 =$

So we need to address the congruence

goal $\rightarrow$

We use induction on $k \geqslant 3$.

Base Case. If $k = 3$ then

Inductive Assumption. Let integer $k \geqslant 3$ be given.

assume $\rightarrow$

Inductive Step.

goal $\rightarrow$

Using difference of squares

The first factor is divisible by 2 because:

By induction, the second factor is divisible by:

Hence the product:

which completes the proof.

□