Primitive Roots of Unity (4)

- (Recall) **Euler's Totient Function**

  ϕ**(N)** = the number of $1 \le K \le N$
  such that K and N are relatively prime

Theorem
There are ϕ**(P−1)** **primitive roots of unity**.

Examples

- (P=7) $\phi(6)=2$ (3,5 are prim roots)
- (P=11) $\phi(10)=4$ (2,6,7,8 are prim roots)

Primitive Roots of Unity (5)

- For each $1 \le A \le P-1$,
  take the **least K** ≥ 1 with $A^K \equiv 1 \pmod{P}$.
  K is the **order** of A (mod P).
- **ψ(K)** = # of elements A with order K
- **K divides P−1** because the sequence
  $A^K \pmod{P}$ $(K \ge 1)$ is cyclic and
  $A^{P-1} \equiv 1$ (by **Fermat's Little Thm**).
- We want: **$\psi(P-1) = \phi(P-1)$.**

Primitive Roots of Unity (6)

- It is enough to prove $\boldsymbol{\psi(K) = \phi(K)}$ for any K dividing P−1.
- This follows from the following 3 claims:

  (1) The sum of $\psi(K)$ is equal to P−1 (where K divides P−1). (**Obvious**)

  (2) The sum of $\phi(K)$ is equal to P−1 (where K divides P−1). (**Week 1**)

  (3) $\psi(K) = 0$ or $\phi(K)$.

Primitive Roots of Unity (7)

Proof of Claim (3): **$\psi(K) = 0$ or $\phi(K)$**.

Assume $\psi(K) \neq 0$. Take $1 \leq A \leq P-1$ with order K.

For each $1 \leq M \leq K$,

$$(A^M)^K \equiv A^{MK} \equiv (A^K)^M \equiv 1^M \equiv 1.$$

By **Lagrange's Theorem**, A^M $(1 \leq M \leq K)$ are the elements whose K-th powers are $\equiv 1$.

Among them, A^N ($1 \leq N \leq K$, **N and K are relatively prime**) are the elements with order K.

Hence **$\psi(K) = \phi(K)$**.