Primitive Roots of Unity (8)

Euler's Criterion

P = 2N+1 **odd** prime number, A integer

$$A^N \equiv \left(\frac{A}{P}\right) \pmod P$$

$1 \le B \le P-1$ **primitive root of unity**

$\Rightarrow B^K \pmod P$ $(1 \le K \le P-1)$ are distinct.

$(B^N)^2 \equiv 1$ (Fermat's Little Thm) $\Rightarrow B^N \equiv -1$

Hence B^K is QR $\Leftrightarrow$ K is even $\Leftrightarrow$ $(B^K)^N \equiv 1$.

Primitive Roots of Unity (9)

Multiplicativity of Legendre Symbols

P **odd** prime number, A, B integers

$$\left(\frac{AB}{P}\right) = \left(\frac{A}{P}\right)\left(\frac{B}{P}\right)$$

Proof

By **Euler's Criterion**, the left hand side is $(AB)^N$ (mod P), and the right hand side is $A^N \times B^N$ (mod P). Since $(AB)^N = A^N \times B^N$, we have the multiplicativity.