# **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 ≤ B ≤ P-1 **primitive root of unity** ⇒ B<sup>K</sup> (mod P) (1 ≤ K ≤ P-1) are distinct. (B<sup>N</sup>)<sup>2</sup> ≡ 1 (Fermat's Little Thm) ⇒ B<sup>N</sup> ≡ -1 Hence B<sup>K</sup> is QR ⇔ K is even ⇔ (B<sup>K</sup>)<sup>N</sup> ≡ 1. 2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199

## **Primitive Roots of Unity (9)**

### **Multiplicativity of Legendre Symbols**

P odd prime number, A, B integers

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

#### **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.