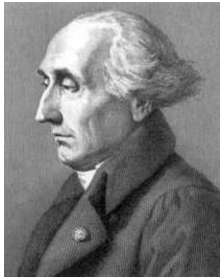
Primitive Roots of Unity (1)

- **Primitive roots of unity** play an important role in modular arithmetic. They were studied by Euler, Lambert, and Lagrange. Gauss first rigorously proved their existence.

Leonhard Euler (1707-1783)

Johann Heinrich Lambert (1728-1777)

Joseph-Louis Lagrange (1736-1813)



https://en.wikipedia.org/wiki/Johann_Heinrich_Lambert
https://en.wikipedia.org/wiki/Joseph-Louis_Lagrange

Primitive Roots of Unity (2)

Definition

An integer A ($1 \le A \le P-1$) is a **primitive root of unity (mod P)** if

$$A^K \not\equiv 1 \pmod{P} \quad \text{for } 1 \le K \le P-2.$$

Example (P=7)

- **3**, $3^2 \equiv$ **2**, $3^3 \equiv$ **6**, $3^4 \equiv$ **4**, $3^5 \equiv$ **5**, $3^6 \equiv$ **1**

  $\Rightarrow$ 3 is a primitive root of unity (mod 7)
- **2**, $2^2 \equiv$ **4**, $2^3 \equiv$ **1**

  $\Rightarrow$ 2 is **not** a primitive root of unity (mod 7)

Primitive Roots of Unity (3)

$A \pmod 7$	0	1	2	**3**	4	**5**	6
$A^2 \pmod 7$	0	1	4	**2**	2	**4**	1
$A^3 \pmod 7$	0	1	1	**6**	1	**6**	6
$A^4 \pmod 7$	0	1	2	**4**	4	**2**	1
$A^5 \pmod 7$	0	1	4	**5**	2	**3**	6
$A^6 \pmod 7$	0	1	1	**1**	1	**1**	1

$$A^K \pmod 7 \text{ for } K = 1, 2, \ldots, 6$$

- **3,5 primitive roots of unity** (mod 7)
- 1,2,4,6 not primitive roots of unity