

$$\text{ord}_p(a) = 2 \Leftrightarrow a \equiv -1 \pmod{p}$$

50

$$a \not\equiv 1 \pmod{p} \text{ و } a^2 \equiv 1 \pmod{p} \leftarrow \text{ord}_p(a) = 2 \text{ ليس } *$$

$$a \not\equiv 1 \pmod{p} \text{ و } p \mid (a^2 - 1) \Leftrightarrow$$

$$a \not\equiv 1 \pmod{p} \text{ و } p \mid (a-1)(a+1) \Leftrightarrow$$

$$p \mid (a-1) \text{ و } p \mid (a+1) \text{ الآن}$$

$$p \nmid a-1 \text{ و } a \not\equiv 1 \pmod{p} \text{ و } p \nmid a+1$$

$$a \equiv -1 \pmod{p} \Leftrightarrow p \mid a+1 \Leftrightarrow$$

$$(a \equiv -1 \pmod{p} \text{ و } a^2 \equiv 1 \pmod{p}) \Leftrightarrow a \equiv -1 \pmod{p} \text{ ليس } *$$

$$a \not\equiv 1 \pmod{p} \text{ و } a \equiv -1 \pmod{p}$$

$$1 \equiv -1 \pmod{p} \Leftrightarrow a \equiv 1 \pmod{p} \text{ و } a \equiv -1 \pmod{p}$$

$$2 \equiv 0 \pmod{p} \Leftrightarrow$$

$$p \mid 2 \text{ و } p=2 \text{ و } p \text{ زوج}$$

$$a \not\equiv 1 \pmod{p} \text{ و } a^2 \equiv 1 \pmod{p} \Leftrightarrow$$

$$\text{ord}_p(a) = 2 \Leftrightarrow$$

$$\text{ord}_n(b) = k_2 \text{ و } \text{ord}_n(a) = k_1 \text{ و } a, b \text{ نس$$

$$b^{k_2} \equiv 1 \pmod{n} \text{ و } a^{k_1} \equiv 1 \pmod{n} \Leftrightarrow$$

$$(ab)^{k_1} \equiv 1^{k_1} \pmod{n} \Leftrightarrow ab \equiv 1 \pmod{n} \text{ الآن}$$

$$a^{k_1} b^{k_1} \equiv 1 \pmod{n} \Leftrightarrow$$

$$b^{k_1} \equiv 1 \pmod{n} \Leftrightarrow$$

$$k_2 \leq k_1 \Leftrightarrow$$

$$k_1 \leq k_2 \text{ و } (ab)^{k_2} \equiv 1 \pmod{n} \text{ و } k_1 \leq k_2$$

$$n-1 \mid \phi(n) \Leftrightarrow \text{ord}_n(a) \mid \phi(n) \text{ و } \text{ord}_n(a) = n-1 \text{ و } a \text{ نس$$

$$n-1 \leq \phi(n) \Leftrightarrow$$

$$\phi(n) = n-1 \Leftrightarrow \phi(n) \leq n-1 \text{ و } \phi(n) = n-1$$

$$n \text{ و } n \text{ أولي}$$