there exist integers x, y.

$$x\,a \equiv 1 \mod n \quad \text{—} \quad \underline{a^{-1} \text{ exist.}}$$

$$\Leftrightarrow \quad xa = yn + 1$$

$$\Leftrightarrow \quad xa - yn = 1$$

$$\Leftrightarrow \quad \underline{\gcd(a, n) = 1}$$

Given a, n with $\gcd(a,n)=1$
can we find the x, y giving

$$xa + yn = 1 ?$$

$\underline{x \equiv a^{-1} \mod n.}$

Extended Euclidean Agorithm
Starting at end of the E. A.

$$10 = 90 - 2 \cdot 40$$

$$= 90 - 2 \cdot (310 - 3 \cdot 90) \qquad 40 = 310 - 3 \cdot 90$$

$$= 7 \cdot 90 - 2 \cdot 310 \qquad 90 = 710 - 2 \cdot 310$$

$$= 7 \cdot (710 - 2 \cdot 310) - 2 \cdot 310$$

$$= 7 \cdot 710 - 16 \cdot 310$$

We've found a x, y giving

$$x \cdot 710 + y \cdot 310 = \gcd(710, 310).$$