$(a,b)=1$

φ é multiplicativa $(a,b)=1 \Rightarrow \varphi(ab)=\varphi(a)\varphi(b)$

Suponha $(a,b)=1$

$1 \quad 2 \quad 3 \ldots \quad m-1 \quad m$

$m+1 \quad m+2 \quad m+3 \ldots \quad m+(m-1) \quad 2m$

$(n-1)(m+1) \quad (n-1)(m+2) \qquad\qquad m \cdot n$

Eficiência de Euclides: o que acontece depois de 2 passos

Euclid (a,b)

$(p-1)! \equiv -1 \pmod{p} \overset{?}{\iff} p$ Primo

p Primo $\overset{?}{\Rightarrow} (p-1)! \equiv -1 \pmod{p}$

Suponha [illegible] p Primo

temos que $(p-1)! = (p-2)! \cdot (p-1)$

Logo $(p-1)! \equiv (p-2)! \cdot (p-1) \pmod{p}$

Voltando um Passo $[(p-2)!]_p \overset{?}{\equiv} 1$

Logo $(p-1)! \equiv (p-1) \pmod{p}$

$\equiv (-1) \pmod{p}$

$(p-1)! \equiv -1 \pmod{p} \overset{?}{\Rightarrow} p$ primo

Suponha $(n-1)! \equiv -1 \pmod{n}$

$a^p \equiv a \pmod{p} \Rightarrow p$ primo

$2^{344} \equiv 2 \pmod{344}$

$344 = 11 \cdot 31$

Logo 344 composto

$2^{561} \equiv 2 \pmod{561}$

$561 = 11 \cdot 3 \cdot 17$

$(a, bc) = 1$

$(a, bc) = 1 \Rightarrow (a,b) = 1 \;\&\; (a,c) = 1$

$(a, bc) = 1 \Leftarrow (a,b) = 1 \;\&\; (a,c) = 1$

Suponha $(a, bc) = 1$

$(a, bc) = (a,b) \cdot (a,c)$

$(a,b) = 1 \;\&\; (a,c) = 1 \Rightarrow (a,bc) = 1$

$(a,b) = 1$

$(a,c) = 1$

Suponha $(a,b) = 1 \;\&\; (a,c) = 1$

Divisão de Euclides

$qm + r$

$(qm + r, m) \overset{?}{=} (r, m)$

$a = qm + r \quad (a, m) = (r, m)$