Outline of the proof of:

φ is multiplicative
i.e. if $\gcd(n,m)=1$ then $\varphi(nm)=\varphi(n)\varphi(m)$

- Preliminary fact (a variant of the Division Algorithm)
  - given $d>0$, then $\forall n\ \exists!$ pair $\hat{q}, \hat{r}$ s.t.
    $n = \hat{q}d + \hat{r}$ where $1 \le \hat{r} \le d$

- Let $E(t) = \{k \in [t] \mid \gcd(k,t)=1\}$
  - then $|E(nm)| = \varphi(nm)$, $|E(n)| = \varphi(n)$ and $|E(m)| = \varphi(m)$

- Note that $|E(n) \times E(m)| = |E(n)|\,|E(m)|$ so that the result follows if we establish a bijection from $E(nm)$ to $E(n) \times E(m)$

- The bijection is defined as follows:
  - if $x \in E(nm)$ write

$$x = \hat{q}_n n + r_n \qquad 1 \le r_n \le n$$

and $$x = \hat{q}_m m + r_m \qquad 1 \le r_m \le m$$

Then

$$x \longrightarrow (r_n, r_m) \text{ is a function}$$

Details: $\gcd(n, r_n) = \gcd(m, r_m) = 1$

- 1-1 ness: Suppose $x_1 \longrightarrow (r_n^1, r_m^1)$ and $x_2 \longrightarrow (r_n^2, r_m^2)$ where $x_1 \ge x_2$. Assume $(r_n^1, r_m^1) = (r_n^2, r_m^2)$ and prove that $nm \mid x_1 - x_2$ where $0 \le x_1 - x_2 \le nm-1$

<u>ontoness</u>: Since $\gcd(n,m)=1$ $\exists$ w, z s.t

$$nw + mz = 1 \quad (\dagger)$$

- Suppose $(r,s) \in E(n) \times E(m)$. Multiply both sides of $(\dagger)$ by $r-s$ and manipulate to get an expression

$$\hat{x} = tn + r = um + s$$

where t and u are integers and $\gcd(\hat{x}, nm) = 1$

- Since $\hat{x}$ may not be in the range $1 \rightarrow nm$ write

$$\hat{x} = l(nm) + x \quad \text{where} \quad \gcd(x, nm) = 1$$

and $1 \leq x \leq nm$.

- Then solve for x to get

$$x = \hat{t}n + r = \hat{u}m + s$$

which by the Preliminary fact is unique.

Thus

$$x \longrightarrow (r,s)$$

and ontoness is established