

- (ii) There are p^d natural numbers which are less than, or equal to, p^d . Of these, the ones which are not coprime to p^d are exactly those which have a factor p :

$$pi, \quad i \in \{1, 2, \dots, p^{d-1}\}.$$

There are p^{d-1} such natural numbers. So $\varphi(p^d) = p^d - p^{d-1}$.

- (iii) If $m = 1$ or $n = 1$ (or both), then the result clearly holds.

Suppose that $m, n > 1$. Write $1, 2, \dots, mn$ in an $n \times m$ array

$$\begin{array}{cccccc} 1 & 2 & 3 & \cdots & m \\ m+1 & m+2 & m+3 & \cdots & 2m \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (n-1)m+1 & (n-1)m+2 & (n-1)m+3 & \cdots & mn \end{array}$$

These integers are a CSR modulo mn .

We have that $\varphi(mn)$ of these integers are coprime to mn . Furthermore, an integer is coprime to mn if, and only if, it is coprime to both m and n . The n columns correspond to the congruence classes modulo m . Also, $\varphi(m)$ of the columns consist of integers which are coprime to m .

The remaining $n - \varphi(m)$ columns consist of integers i with $(i, m) > 1$. Pick a column $c, m+c, \dots, (n-1)m+c$ of integers which are coprime to m . Since $0, 1, \dots, n-1$ is a CSR modulo n and $(n, m) = 1$, by Corollary 12.14 we have that $0, m, \dots, (n-1)m$ is a CSR modulo n . Hence $c, m+c, \dots, (n-1)m+c$ is a CSR modulo n .

Hence $\varphi(n)$ of the integers in the column $c, m+c, \dots, (n-1)m+c$ are coprime to n . Since there are $\varphi(m)$ such columns of integers which are coprime to m , there are $\varphi(m)\varphi(n)$ integers which are coprime to both m and n . Hence $\varphi(mn) = \varphi(m)\varphi(n)$.

- (iv) This follows from (ii) and (iii).

□