

Let e be a prime number and $p, q \in \mathbb{N}$. If $(p - 1) \bmod(e) \neq 0$ and $(q - 1) \bmod(e) \neq 0$ then $GCD(e, (p - 1)(q - 1)) = 1$.

Proof:

We will show this by assuming there exists a z such that $GCD(e, (p - 1)(q - 1)) = z > 1$, then by hypothesis we know that $e \leq z$ because the only integers that divide e are 1 and e . So the existence of z indicates that by the definition of GCD the following conditions must be true.

$$(a) z > 0$$

$$(b) z|e \text{ and } z|(p - 1)(q - 1)$$

$$(c) \text{ if } d|e \text{ and } d|(p - 1)(q - 1) \text{ then } d|z$$

Case1) $z > e$:

This contradicts the assumption that $z|e$ in condition (b) and hence it must be the case that $GCD(e, (p - 1)(q - 1)) = 1$.

Case 2) $z = e$:

$$(p - 1) \bmod(e) \neq 0 \rightarrow \exists n_1 \exists q_1 \ni (p - 1) = eq_1 + r_1 \text{ and } 0 < r_1 < e$$

$$(q - 1) \bmod(e) \neq 0 \rightarrow \exists n_2 \exists q_2 \ni (q - 1) = eq_2 + r_2 \text{ and } 0 < r_2 < e$$

$$(p - 1)(q - 1) = (eq_1 + r_1)(eq_2 + r_2)$$

$$(p - 1)(q - 1) = e(eq_1q_2 + q_1r_2 + q_2r_1) + r_1r_2 \text{ and } 0 < r_1r_2 < e^2$$

In the event $r_1r_2 < e$ then we have shown that $e \nmid (p - 1)(q - 1)$. In the case that $r_1r_2 > e$ then r_1r_2 then there exists integers c and r_3 such that r_1r_2 can be written as $r_1r_2 = r_3 + ce$ where $1 \leq c < e$ and $0 < r_3 < e$ which implies that we can write

$$(p - 1)(q - 1) = e(eq_1q_2 + q_1r_2 + q_2r_1 + c) + r_3 \rightarrow$$

$$e \nmid (p - 1)(q - 1)$$

It should be clear that $e \nmid r_1r_2$ when we consider the largest prime factor p_k of r_1 and the largest prime factor p_j of r_2 . Since $e|r_1r_2$ implies the existence of a natural number t such that $et = r_1r_2$ we know from the uniqueness of the prime factorization that e must be a factor of et and r_1r_2 , this is a contradiction because the largest prime number in the factorization of r_1r_2 is the maximum of (p_k, p_j) and $\max(p_k, p_j) < e$.

The result $e \nmid (p - 1)(q - 1)$ implies that $e = z \nmid (p - 1)(q - 1)$ and hence a contradiction of condition (b). We can then assume that $GCD(e, (p - 1)(q - 1)) = 1$.