

Online Quiz 5

1. Let p, q be prime number; Let $n > 1$.

Assume $p|n$ and $q|n$

WTS: $pq|n$.

Since $p|n$, gives $\exists k_1 \in \mathbb{Z}$ s.t. $n = p \cdot k_1$ (from defⁿ of divisibility).

Since $q|n$, gives $\exists k_2 \in \mathbb{Z}$ s.t. $n = q \cdot k_2$, gives $p \cdot k_1 = q \cdot k_2$; Since $p \neq q$, gives $k_1 \neq k_2$.

Since p, q are prime, $p \neq q$, gives $\exists a \in \mathbb{Z}$ s.t. $k_1 = a \cdot q$, which $p \cdot a \cdot q = q \cdot k_2$.

(Also, $\exists b \in \mathbb{Z}$ s.t. $k_2 = b \cdot p$, which $p \cdot k_1 = q \cdot b \cdot p$).

Since $q \cdot k_2 = n$, gives $n = p \cdot a \cdot q = a \cdot (p \cdot q)$, which $pq|n$.

2. Let $a \equiv r \pmod{p}$, $a \equiv r \pmod{q}$.

WTS: $a \equiv r \pmod{pq}$.

According to the definition, $\exists k_1 \in \mathbb{Z}$ s.t. $a = r + k_1 p$; $\exists k_2 \in \mathbb{Z}$ s.t. $a = r + k_2 q$, gives

$$r + k_1 p = r + k_2 q, \text{ according to the cancellation rules:} \\ \Rightarrow k_1 p = k_2 q.$$

Similar to Q1, $\exists b \in \mathbb{Z}$ s.t. $k_1 = b \cdot q$ which $p \cdot b \cdot q = q \cdot k_2$.

Since $a = r + k_2 q = r + b \cdot (p \cdot q)$, which $a \equiv r \pmod{p \cdot q}$.

3. Let $n \equiv 14 \pmod{17}$; $n \equiv 14 \pmod{19}$; $n \equiv 14 \pmod{23}$, gives.

$$\text{From Q2, gives } n \equiv 14 \pmod{323}; n \equiv 14 \pmod{391}; n \equiv 14 \pmod{437}.$$

\downarrow
 17×19

\downarrow
 17×23

\downarrow
 19×23

Thus, the possible combination from 4000 to 11000 of $n \equiv 14 \pmod{323}$ are:

$$n = 14 + 323 \times 13 = 4213; 4536; 4859; \dots; 7443; 7766; \dots; 10986; 11309$$

$$n = 14 + 391 \times 11 = 4315; 4706; 5097; \dots; 7443; 7834; \dots; 10962; 11353$$

$$n = 14 + 437 \times 10 = 4384; 4821; 5258; \dots; 7443; 7880; \dots; 10939; 11376$$

Therefore $n = 7443$ is the only such number n according to Q2.