

UNIQUE MODS IN AN LCM INTERVAL

SUSAM PAL

Created : August 4, 2008

Last Updated : January 11, 2009

Theorem. $i \equiv a \pmod{m}$ and $i \equiv b \pmod{n}$, where i, a, b, m and n are integers, $m > 0$ and $n > 0$. There is no such integer j , such that $j \neq i$, $|i - j| < lcm(m, n)$, $j \equiv a \pmod{m}$ and $j \equiv b \pmod{n}$, where $lcm(m, n)$ is the lowest common multiple of m and n .

Proof. Let us assume, there is a j , such that $j \neq i$, $|i - j| < lcm(m, n)$, $j \equiv a \pmod{m}$ and $j \equiv b \pmod{n}$.

i and j can be expressed as follows:

$$i = pm + a = qn + b, \text{ for some integers } p \text{ and } q.$$

$$j = rm + a = sn + b, \text{ for some integers } r \text{ and } s.$$

$$\text{So, } |i - j| = |p - r|m = |q - s|n.$$

Therefore, $|i - j|$ is a common multiple of m and n , such that it is less than $lcm(m, n)$. But this is a contradiction, since $lcm(m, n)$ is the lowest common multiple of m and n . Hence, we have a contradiction and we conclude that our assumption is wrong. \square