Nicole Robles

CYEN 489 – 001

Proof Homework 1

Conjecture 1:

$$\gcd(a, b) * lcm(a, b) = a * b$$

Proof 1:

Let $d = \gcd(a, b)$ *(eq. 1)*

$a = p_1 * d,\ b = p_2 * d$ *(eq.2)* where $p_1, p_2 \in \mathbb{Z}^+$ and $\gcd(p_1, p_2) = 1$

There exists a number $\alpha = p_1 * p_2 * d = p_2 * (p_1 * d)$. *(eq. 3)*

Suppose there exists a $\beta < \alpha$ such that β is a multiple of both a and b. This means $a|\beta \ and \ b|\beta$. So, for some $t_1, t_2 \in \mathbb{Z}^+$,

$\beta = a * t_1$ *(eq. 4)* and $\beta = b * t_2$ *(eq. 5)*, so substituting the values for a and b from eq. 2, we get

$\beta = (d * p_1) * t_1$ *(eq. 6)* and $\beta = (d * p_2) * t_2$ *(eq. 7)*.

By eq. 6 and eq. 7, $\beta = d * p_1 * t_1 = d * p_2 * t_2$ and thus

$p_1 * t_1 = p_2 * t_2$, $\gcd(p_1, p_2) = 1$ *(eq. 8)*.

Since $\gcd(p_1, p_2) = 1$, then all factors of p_2 must be found within t_1, which means that $p_2|t_1$, so

$t_1 = p_2 * s_1$ *(eq. 9)*, for some $s_1 \in \mathbb{Z}^+$.

Similarly, since $\gcd(p_1, p_2) = 1$, all factors of p_1 must be found within t_2, which means that $p_1|t_2$, so

$t_2 = p_1 * s_2$ *(eq. 10)*.

We can then substitute eq. 9 into eq. 6 to get a modification of eq. 3,

$\beta = d * p_1 * t_1 = d * p_1 * p_2 * s_1 = \alpha * s_1$ *(eq. 10)*.

This contradicts $\beta < \alpha$ and so, α must be the least common multiple of a and b.