IA Assignment 2

24 August 2020

MAM2000W 2IA KDSMIL001

1. By the fact that gcd(a, b)=1, we know that a and b are coprime. That means we can write them as their prime factorisations

$$a = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r},\ b = p_1^{b_1} p_2^{b_2} \dots p_r^{b_r}$$

where p_i are the prime numbers, $a_i, b_i \geq 0$, and

$$\begin{aligned} a_i \neq 0 &\implies b_i = 0 \\ b_i \neq 0 &\implies a_i = 0 \end{aligned}$$

What we mean by this is that any prime factor p_i of a with $a_i \geq 1$ is not a prime factor of b, and vice versa.
Now we can write c as its prime factorisation, as well as c^2:

$$c = p_1^{c_1} p_2^{c_2} \dots p_r^{c_r} \implies c^2 = p_1^{2c_1} p_2^{2c_2} \dots p_r^{2c_r}$$

But we are given that $c^2 = ab$, so we can write

$$c^2 = p_1^{a_1+b_1} p_2^{a_2+b_2} \dots p_r^{a_r+b_r}$$

and since a and b share no prime factors, all exponents in the equation above are either a_i or b_i (or 0) but never $a_i + b_i$. Thus we can write

$$a_i = 2c_i = 2m_i,\ b_i = 2c_i = 2n_i$$

for $m_i, n_i \in \mathbb{Z},\ m_i, n_i \geq 0$. Finally we can write

$$\begin{aligned} a = p_1^{2m_1} p_2^{2m_2} \dots p_r^{2m_r} &= (p_1^{m_1} p_2^{m_2} \dots p_r^{m_r})^2 = m^2 \\ b = p_1^{2n_1} p_2^{2n_2} \dots p_r^{2n_r} &= (p_1^{n_1} p_2^{n_2} \dots p_r^{n_r})^2 = n^2 \end{aligned}$$

for $m, n \in \mathbb{Z}^+$. Thus a and b are each squares.

$\square$