Transition to Advanced Mathematics

Fall 2021

Practically Perfect Proof

Patrick May

December 31, 2021

Question 5.

Theorem 1. *If* $a \equiv b \pmod{n}$*, then* $\gcd(a,n) = \gcd(b,n)$.

Proof. Assume $a \equiv b \pmod{n}$. Let $g_{a,n} = \gcd(a,n)$ and $g_{b,n} = \gcd(b,n)$.

Then by definition, $n \mid (a-b)$.

Then $cn = a - b$ for some $c \in \mathbb{Z}$.

$$cn = a - b \tag{1}$$

$$\implies cn + b = a \tag{2}$$

$$\implies a - cn = b \tag{3}$$

By definition of gcd, $g_{b,n} \mid b$ and $g_{b,n} \mid n$.

Then $dg_{b,n} = n$ and $eg_{b,n} = b$ for some $d, e \in \mathbb{Z}$.

Starting with 2,

$$\begin{aligned} cn + b &= a \\ \implies cdg_{b,n} + eg_{b,n} &= a \\ \implies g_{b,n}(cd + e) &= a \end{aligned}$$

Since $(cd + e)$ is an integer by closure, $g_{b,n} \mid a$.

Similarly, $g_{a,n} \mid a$ and $g_{a,n} \mid n$.

Then $sg_{a,n} = n$ and $tg_{a,n} = a$ for some $s, t \in \mathbb{Z}$.

Starting with 3,

$$\begin{aligned} a - cn &= b \\ \implies tg_{a,n} - csg_{a,n} &= b \\ \implies g_{a,n}(t - cs) &= b \end{aligned}$$

Since $(t - cs)$ is an integer by closure, $g_{a,n} \mid b$.

Hence, $g_{b,n}$ is a common divisor of a and n. Thus we must have $g_{b,n} \le g_{a,n}$, since $g_{a,n}$ is the greatest common divisor of a and n.

Similarly, $g_{a,n}$ is a common divisor of b and n. Thus we must have $g_{a,n} \le g_{b,n}$, since $g_{b,n}$ is the greatest common divisor of b and n.

Therefore $g_{a,n} = g_{b,n}$.

$\square$