# Assignment - 3

Mithilaesh Jayakumar
G01206238

1) If $a$ and $b$ are relatively prime and $bc$ is a multiplicative of $a$, show that $c$ is a multiple of $a$.

Ans:- Assume that $a, b$ and $c$ are integers

We know that $a$ and $b$ are relatively prime

Therefore $gcd(a, b) = 1$

By the multiplicative inverse theorem,

$ma + nb = 1$ --- ① where $m$ and $n$ are integers

We know that $bc$ is a multiple of $a$

Therefore $a$ divides $bc$ and

$bc = ak$ — ② where $k$ is an integer

Take the ① and substitute it with multiplication of $c$ on both sides

$mac + nbc = c$

substitute $bc$ with $ak$ from ②

$mac + nak = c$

$a(mc + nk) = c$ — ③

substitute $mc + nk = q$

$aq = c$

where $q$ is an integer

Therefore, this shows that $a$ divides $c$ which implies that

$c$ is a multiple of $a$

2) In mod $n$ arithmetic, the quotient of two numbers $r$ and $m$ is a number $q$ such that $mq = r \bmod n$. Given $r, m, n$ how can you find $q$? How many $q$'s are there? Under what conditions is $q$ unique?

<u>Ans:</u> We know that $mq = r \bmod n$ — ①

Dividing ① by $\gcd(m,n)$ we get,

$$\frac{m * q}{\gcd(m,n)} = \frac{r \bmod n}{\gcd(m,n)}$$

$$= r/\gcd(m,n) \bmod n/\gcd(m,n)$$

As $mq = r \bmod n$, we know that $r = nk + mq$

Therefore several values of $q$ exist as $\gcd(m,n) \mid r$ holds

or there are no values of $q$.

We can get a unique value of $q$ for the condition

$\bmod (n/\gcd(m,n))$

3) In the final step of Euclid's algorithm for finding gcd (m, n) we get u and v such that $um + vn = 0$. Is $|um|$ (which $= |vn|$) the least common multiple of m and n?

<u>Ans:</u> yes, $|um|$ is the least common multiple of m and n

Let us prove this with an example,

consider two integers $m = 48$
$n = 16$

$gcd(m, n) = gcd(48, 16) = 16$

where $u * 48 + 16 * v = 0$

Now to find the values of u and v,

$16 * v = -48 * u$

$v = -3 * u$

Therefore $v = -3$ and $u = 1$

$|um| = |1 * 48| = 48$

$|vn| = |-3 * 16| = |-48| = 48$

$|um| = |vn|$

We need to prove that $|um| = LCM(48, 16)$

$LCM(48, 16) = 48$

$$\begin{array}{r|l} 16 & 48, 16 \\ \hline 3 & 3, 1 \\ \hline & 1, 1 \end{array}$$

Hence proved.

4) Is it possible for $\phi(n)$ to be bigger than $n$?

Ans: No, it is not possible for $\phi(n)$ to be bigger than $n$ because $\phi(n) = Z_n^*$ where $Z_n^*$ is defined as the set of mod $n$ integers that are relatively prime to $n$. $\phi(n)$ is defined as the number of elements in $Z_n^*$ and range of $\phi(n) = [0 \text{ to } n-1]$. Therefore $\phi(n)$ cannot be bigger than $n$.