CISC102 - Discrete Math I

July 2018

Assignment 3 - Problem 7

Sam Huang (10175794)

Part A

Prove that

$$GCD(m*a, m*b) = m*GCD(a,b)$$

Direct proof, starting from the LHS:

Let $u = GCD(m*a, m*b)$

*u can be expressed as u = ax + by for integers x and y, given Theorem 11.13 from the textbook, which states that if d is the smallest positive integer of the form a*x+b*y, then d = GCD(a,b)*

$u = (m*a)*x + (m*b)*y$

Therefore, u is a sum of multiples of m

$m|u$

Therefore, u is a multiple of m

$u = p*m$, for some integer p

Substitute $u = p*m$ *in* $u = (m*a)*x + (m*b)*y$

$p*m = (m*a)*x + (m*b)*y$

To prove the equality $u = GCD(m*a, m*b) = m*GCD(a,b) = m*p$, we need to show that $p = d = GCD(a,b)$

To prove $p = d$, we need to show that $p \geq d$ and $d \geq p$

To show $p \geq d$:

Theorem 11.13 tells us that d is the smallest positive integer which can be expressed as an linear combination of a and b where a and b are integers.

We know that

$\rightarrow p * m = (m * a) * x + (m * b) * y$

Divide out m

$\rightarrow p = a * x + b * y$

Since p is another such linear expression of a and b, d cannot be greater than p. Therefore, $p \geq d$

To show $d \geq p$:

$d = ax + by$

Multiply both sides by m

$\rightarrow m * d = (m * a) * x + (m * b) * y$

Since u is the smallest positive integer of the form $a * x + b * y$ for $a = m * a$ and $b = m * b$, then $m * d \geq u$

$\rightarrow m * d \geq p * m$

$\rightarrow d \geq p$

Now we have shown that $p \geq d$ and $d \geq p$, we know that $p = d$.

We can substitute $p = d$ back into the equality we need to prove

$u = GCD(m * a, m * b) = m * GCD(a, b) = m * p = m * d = m * GCD(a, b)$

Therefore, we have proven that the theorem

$$GCD(m * a, m * b) = m * GCD(a, b)$$

is true. ■

Part B

Prove that

If $GCD(a, m) = d$ and $GCD(b, m) = 1$, then $GCD(a * b, m) = d$

Direct proof

Given $GCD(a, m) = d$, we know that: $d|a$ and $d|m$

Therefore,

$a = x * d$, $m = y * d$, $b = z * d + r$

for integers x,y,z

Multiplying a and b, we get

$a * b = x * d * (z * d + r)$

Expand RHS

$\rightarrow a * b = x * d * z * d + r * x * d$

Let some integers $n_1 = x * d * z$ and $n_2 = r * x$

$\rightarrow a * b = n_1 * d + n_2 * d$

$\rightarrow a * b = d * (n_1 + n_2)$

We see that $a * b$ is the sum of multiples of d, therefore $d|(a * b)$

We now know:

$d|(a * b)$,

$d|a$ and $d \nmid b$,

$d|m$ and $GCD(b, m) = 1$, which means b and m are relatively prime

Therefore, $GCD(a * b, m) = d$. We have proven that the theorem is true. ■