MATH 335 Homework 2

Chris Camano: ccamano@sfsu.edu

September 7, 2022

1. Produce a clear and clean proof of the following statement you have discovered in class: Let a and b two positive integers. Then $ab = \gcd(a,b)\text{lcm}(a,b)$.

   Proof. Let a and b be expressed in their corresponding prime decompositions:

   $$a = \prod_{i=1}^{k} p_i^{\alpha_i}$$

   $$b = \prod_{i=1}^{k} p_i^{\beta_i}$$

   where $p_1, ..., p_k$ are distinct prime numbers and $\alpha_1, ..., \alpha_k$ and $\beta_1, ..., \beta_k$ are integer exponents.

   Likewise define the gcd(a,b) and lcm(a,b) by their prime decomposition formulas:

   $$gcd(a,b) = \prod_{i=1}^{k} p_i^{\max\{\alpha_i,\beta_i\}}$$

   $$lcm(a,b) = \prod_{i=1}^{k} p_i^{\min\{\alpha_i,\beta_i\}}$$

   with these definitions we can re-express $gcd(a,b)lcm(a,b)$ as the following:

   $$\prod_{i=1}^{k} p_i^{\max\{\alpha_i,\beta_i\}} \prod_{i=1}^{k} p_i^{\min\{\alpha_i,\beta_i\}}$$
   $$\prod_{i=1}^{k} p_i^{\max\{\alpha_i,\beta_i\}} p_i^{\min\{\alpha_i,\beta_i\}}$$
   $$\prod_{i=1}^{k} p_i^{\max\{\alpha_i,\beta_i\}+\min\{\alpha_i,\beta_i\}}$$

   however since there are only two numbers being considered for each prime exponent if one is the max the other must be the min and vice versa, in other words:

   $$\max\{\alpha_i,\beta_i\} + \min\{\alpha_i,\beta_i\} = \alpha_i + \beta_i$$

returning to our previous expression with this new identity:

$$\prod_{i=1}^{k} p_i^{\alpha_i+\beta_i}$$
$$\prod_{i=1}^{k} p_i^{\alpha_i} p_i^{\beta_i}$$
$$\prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=1}^{k} p_i^{\beta_i}$$
$$ab$$

thus it has been shown that using the prime decomposition definitions of gcd and lcm that

$$ab = \gcd(a,b)\mathrm{lcm}(a,b)$$

□

2. We learned that if two integers a and b are relatively prime, then there exist integers t and u such that $at + bu = 1$. Prove the converse: if there are integers t and u such that $at + bu = 1$ then a and b are relatively prime.

   Proof. Let the gcd of a and b be denoted as the letter g:

   $$\gcd(a,b) = g$$

   By the definition of g for any linear combination of the form:

   $$ax + by, x, y \in \mathbb{Z}$$

   $g|ax + by$ therefore $g|at + bu$ which is equivilant to stating that $g|1$. The only factors of 1 are -1,1 therefore since g is the greatest common factor this implies that g must be equal to 1.

   □

3. Let a and b be integers with $b > 0$. Using division algorithm, write $a = bq + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < b$. Show that $\gcd(a,b) = \gcd(b,r)$.

   Proof. Let d=gcd(a,b). By the definition of gcd $d|a$ and $d|b$ and for all e such that e is a common divisor of a and b $e|d$.
   Likewise to prove that the $d = gcd(b,r)$ we must first show $d|b$ and $d|r$ and then demonstrate that for other common multiples of b and r that d is greater.
   By definition of d $d|b$, to prove that $d|r$ consider the following algebraic manipulation:

   $$a = qb + r \quad 0 \leq r < b$$

   $$r = a - qb$$

   which implies that proving $d|r$ is equivilant to proving $d|a - qb$.
   Since $d|a$ and $d|b$ we can re express the term $a - qb$ as follows:

   $$a - qb = dk + qdl, \quad k, l \in \mathbb{Z}$$

$$a - qb = d(k + ql)$$

so it is shown that $d|a - qb$ and concequently that $d|r$.
This gives us the notion that d is at the least a common divisor of b and r, we now need to show that it is the greatest common divisor.

Suppose for some integer e, $e|b$ and $e|r$, by the definition of gcd this implies that e divides any linear combination of b and r. Consider the following linear combination:

$$qb + r(1)$$

then $e|qb + r \mapsto c|a$. so c is a common divisor of a and b. d is the greatest common divsor of a and b by the original definition. This means that if e were larger than d that we would arive at a contradiction, therefore e must be less than or equal to d which proves that for some common divisor e of b and r that $e|d$

This means that d=gcd(b,r) and d=gcd(a,b) by definition so we arrive to the final conclusion that:

$$gcd(b,r) = gcd(a,b)$$

□

4. Show that for all positive integers $n > 2$, $\phi(n)$ is an even number.

Proof. To approach this proof let us first recall the two following properties of the Euler Totient function:

(a) if p is a prime number then $\phi(p^k) = p^k - p^{k-1}$

(b) for all n$\mathbb{Z}$

$$\phi(n) = \prod_{i=1}^{k} \phi(p_i^{\alpha_i}) = \prod_{i=0}^{k} p_i^{\alpha_i - 1}(p_i - 1)$$

To prove that for all $n > 2$ that $\phi(n)$ is even we must consider the operation we are preforming when given an arbitrary integer n. We apply the phi function to each of the prime factors of n. In this operation there are two possible occurences. The first is that the chosen prime factor is odd and the other is that it is even.
Consider the case where $p_i = 2k + 1, k \in \mathbb{Z}$ by definition 2 we have the following:

$$\begin{aligned}
&\phi(p_i^{\alpha_i}) = p_i^{\alpha_i - 1}(p_i - 1) \\
&p_i^{\alpha_i - 1}(p_i - 1) = (2k+1)^{\alpha_i}(2k + 1 - 1) \\
&(2k+1)^{\alpha_i} 2k
\end{aligned}$$

So it has been shown that for an odd prime factor p_i that $2|p_i$.
Now consider the case when the chosen prime factor is even and there do not exist odd prime factors. This only occurs when the single prime factor is 2. Using property one we can show:

$$\phi(2^k) = 2^k - 2^{k-1} = 2(2^{k-1} - 2^{k-2})$$

Thus we have shown that in any event the euler totient function returns an even value for $n > 2$. □

5. Prove that if d divides n then $\phi(d)$ divides $\phi(n)$.

Proof. if $d|n$ then n can be expressed as an integer multiple of d:

$$n = dk, k \in \mathbb{Z}$$

$$\begin{aligned} &n = n \\ &\phi(n) = \phi(n) \\ &\phi(dk) = \phi(n) \\ &\phi(d)\phi(k) = \phi(n) \quad \text{multiplicative propery of phi function} \end{aligned}$$

for all integer inputs phi returns another integer thus $\phi(k) \in \mathbb{Z}$ let $\phi(k) = k^*$ then:

$$\phi(d)k^* = \phi(n) \tag{1}$$

so it is clear then that $\phi(n)$ is equal to $\phi(d)$ times some integer. Since $\phi(n)$ can be expressed as $\phi(d)$ times another integer this implies

$$\phi(d)|\phi(n)$$

□