21-127 Homework 6

Christian Broms
Section J

Thursday 1st March, 2018

Complete the following problems. Fully justify each response.

1. Let $a, b \in \mathbb{Z}$. Prove that if d, d' are both gcds of a and b, then $d = \pm d'$.

   Proof. Since d, d' are both gcds of a and b, then by definition, $a|d'$, $b|d'$, $a|d$, $b|d$, so $d|d'$ and $d'|d$ because both are GCDs. When d, $d' = 0$, then the case is trivial and we can say $0 = \pm 0$, or if d or d' is zero then the other must also be 0 since both are gcds of a, b and again we say $0 = \pm 0$. In other cases, since $d|d'$ and $d'|d$ we know $|d| \leq |d'|$ and $|d'| \leq |d|$ when d, $d' \neq 0$. Therefore, $|d| = |d'|$. Because this relation is reliant on absolute value, inserting $-d'$ or d' will yield the same result. Thus, we conclude $d = \pm d'$. ■

2. Let $a, b \in \mathbb{Z}$, and let $d = \gcd(a, b)$. Prove that $\frac{a}{d}$ and $\frac{b}{d}$ are coprime.

   Proof. Because $d = \gcd(a, b)$, we know there exist $u, v \in \mathbb{Z}$ such that $d = au + bv$, and $\frac{au}{d} + \frac{bv}{d} = 1$. So, by Bezout's Lemma, we can say $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Thus, we have shown that $\gcd\left(\frac{a}{d}, \frac{b}{d}\right)$ is coprime. ■

3. Let $a, b \in \mathbb{Z}$. Prove that there exists a unique positive least common multiple of a and b. (Note: here you must prove both existence and uniqueness.)

   Proof. Existence. Let X be the set of common multiples of a and b, defined as $X = \{x \in \mathbb{N} \mid a|x, b|x\}$. We know $X \neq \emptyset$ because $|ab| \in X$.

Thus, by the well ordering principle, there is a smallest element in X. Let this smallest element be m, so $a|m$ and $b|m$. So let n be such that $a|n$ and $b|n$. We need to show that $m|n$ to fufill the second property of the LCM.

Then $n = qm + r$ so $n - qm = r$ with $0 \leq r < m$. Because $a|m$ and $a|m$ then $a|r$. The same is true for b, so $b|r$. Thus, $r = 0$, because if $r > 0$, then $r \in X$, though this is impossible because $r < m$ and we established that m is the smallest element in the set. Therefore, r must be 0, and we conclude that $n = qm$ or $m|n$ and hence the LCM exists.

Uniqueness. Assume that k and ℓ are both Least Common Multiples of a and b. Then, $a|\ell$ and $b|\ell$ and $a|k$ and $b|k$. In addition, we know that $k|\ell$ and $\ell|k$ because both are LCMs. Then, $|k| \leq |\ell|$ and $|\ell| \leq |k|$. Therefore, $|k| = |\ell|$, and it follows that there can only be one unique LCM. ■

4. Let $p \in \mathbb{Z}$. Prove that the following are equivalent

   (a) p is irreducible.

   (b) The only divisors of p are $\pm 1, \pm p$

   (c) p is prime (under the definition in Section 3.2, that p is prime whenever $p|ab \Rightarrow p|a \vee p|b$).

   Proof. (a⇒b). Let $a, b \in \mathbb{Z}$, and assume p is irreducible and $a|p$. Then $p = ab$. Because p is irreducible, then either a or $b = \pm 1$, that is either a or b is a unit. We can write a, b in terms of p, so if a is a unit then $b = \pm p$, and if b is a unit then $a = \pm p$. Thus, we conclude the only divisors of p are $\pm 1, \pm p$.

   (b⇒c). Assume the only divisors of p are $\pm 1, \pm p$. Then we can say $p = ab$. Without loss of generality, say $a = \pm 1$ and $b = \pm p$, though the order does not matter. Then, $p|ab \Rightarrow p|1$ or $p|p$. This fits the definition of a prime, so we conclude that p is a prime.

   (c⇒a). Assume p is prime. Then we can say $p|ab$ and $p|a$ or $p|b$ for some $a, b \in \mathbb{Z}$. First, consider the case when $p|a$. We can say $a = kp$ for $k \in \mathbb{Z}$. Then, $p = ab = kpb$ and $0 = p(1 - kb)$, which implies $0 = 1 - kb$, and $b = 1$, so b is a unit. Therefore, since b

is a unit, we know that p is irreducible. The same is true when considering $p|b$. ∎

5. Suppose $p_1, p_2, \ldots, p_r \in \mathbb{Z}$ are primes. Let $a = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, and let $b = p_1^{\ell_1} p_2^{\ell_2} \ldots p_r^{\ell_r}$, where $k_1, k_2, \ldots k_r, \ell_1, \ell_2, \ldots, \ell_r$ are nonnegative integers. Prove that $\gcd(a, b) = p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r}$, where $m_i = \min\{k_i, \ell_i\}$ for all $1 \leq i \leq r$.

   Proof. We can write a, b as the product of their GCD and some other integer $\alpha, \beta \in \mathbb{Z}$, such that $a = (p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r})\alpha$ and $b = (p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r})\beta$, where $p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r}$ is the GCD of a and b. Note, $\gcd(\alpha, \beta) = 1$ because the largest prime factors of a, b are contained within their GCD. Thus, we write $\alpha = p_1^{k_1 - m_1} p_2^{k_2 - m_2} \ldots p_r^{k_r - m_r}$ and $\beta = p_1^{\ell_1 - m_1} p_2^{\ell_2 - m_2} \ldots p_r^{\ell_r - m_r}$. Because $\gcd(\alpha, \beta) = 1$ we know that either $k_i - m_i = 0$ or $\ell_i - m_i = 0$. Rearranging, we have $k_i = m_i$ or $\ell_i = m_i$. Therefore, m_i must be the lesser of k_i and ℓ_i because $k_i - m_i, \ell_i - m_i \geq 0$. Hence, $m_i = \min\{k_i, \ell_i\}$, and we have shown $\gcd(a, b) = p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r}$, where $m_i = \min\{k_i, \ell_i\}$ for all $1 \leq i \leq r$.

   ∎

6. Prove that for all $n \geq 2$, there exists a prime in the set

$$\{k \in \mathbb{Z} \mid n \leq k \leq n!\}.$$

   (Hint: consider the divisors of $n! - 1$. Can they be in the set $\{1, 2, \ldots, n\}$?)

   Proof. We have $n \leq k \leq (n! - 1)$. There are two possiblities. In the first, $(n! - 1)$ is prime, and we can say $k = (n! - 1)$, where $n \leq k \leq (n! - 1)$. We then know that there exists a prime in the set $\{k \in \mathbb{Z} \mid n \leq k \leq n!\}$. In the second case, $(n! - 1)$ is not prime, and it has no factors between 2 and n. This is because by definition $n!$ has divisors 2 through n. Since $n!$ and $(n! - 1)$ are coprime, $(n! - 1)$ cannot have a common divisor. Because we can prime factorize $(n! - 1)$, and it has no factors between 2 and n, then the prime factors must be between n and $(n! - 1)$. Thus we know that there exists a prime in the set $\{k \in \mathbb{Z} \mid n \leq k \leq n!\}$. ∎