Math 3110 Assignment 6 Solutions

(1a)[5 pts] Prove that for any integers a and b which are not both 0, we have $\gcd(a,b) = \gcd(-a,b)$. Hint: let $d = \gcd(a,b)$. Now use the Characterization of the GCD Theorem to show that $d = \gcd(-a,b)$.

Proof. Let a and b be integers which are not both zero, and let $d = \gcd(a,b)$. Then we know from the Char. of the GCD Thm. that

1. $d > 0$,
2. $d|a$ and $d|b$, and
3. for all $c \in \mathbb{Z}$: if $c|a$ and $c|b$, then $c|d$.

To show that $d = \gcd(-a,b)$, we simply need to check that d satisfies all of the above conditions with a replaced with $-a$. Condition 1. is immediate, since it doesn't involve a. As for 2., since $d|a$ and $d|b$, by the Divisibility Theorem, $d|-a$ (and $d|b$), and so the second condition is satisfied. Now for 3. Assume that c is an integer for which $c|-a$ and $c|b$. The by the Divisibility Theorem, $c|a$ and $c|b$. Now by 3. above, we see that $c|d$. This proves all three conditions and shows that $d = \gcd(-a,b)$. □

(1b)[5 pts] Use (1) to prove that for any integers a and b which are not both 0, we have $\gcd(a,b) = \gcd(a,-b)$. Hint: for any integers x and y which are not both 0, we have $\gcd(x,y) = \gcd(y,x)$. Your proof should be very short; do NOT just rewrite the proof of (1) here but for b.

Proof. Let a and b be integers which are not both 0. Then $\gcd(a,b) = \gcd(b,a)$ (by the hint, which I told you that you didn't have to prove). By (1a), $\gcd(b,a) = \gcd(-b,a)$. Now by the hint again, $\gcd(-b,a) = \gcd(a,-b)$. This shows that $\gcd(a,b) = \gcd(a,-b)$. □

(1c)[5 pts] Use the above to prove that for any integers a and b which are not both 0, we have $\gcd(a,b) = \gcd(-a,-b)$.

Proof. Let a and b be integers which are not both 0. By (1a), $\gcd(a,b) = \gcd(-a,b)$. Now by (1b), $\gcd(-a,b) = \gcd(-a,-b)$. □

(2a)[2 pts - completion] Prove that for any integers a and b which are both nonzero, we have $\text{lcm}(a,b) = \text{lcm}(-a,b)$. Hint: let $m = \text{lcm}(a,b)$. Now use the Characterization of the LCM Theorem to show that $m = \text{lcm}(-a,b)$.

Proof. Let a and b be nonzero integers. Now let $m = \text{lcm}(a,b)$. Then m satisfies

1. $m > 0$,
2. $a|m$ and $b|m$, and
3. for every integer c: if $a|c$ and $b|c$, then $m|c$.

To show that $m = \text{lcm}(-a,b)$, we need to check that m satisfies all of the above conditions with a replaced with $-a$. Now, 1. is immediate. As for 2., we know that $a|m$ and $b|m$. The Div. Thm. implies that $-a|m$, and so $-a|m$ and $b|m$. Finally, let c be an integer, and assume that $-a|c$ and $b|c$. Then as above, $a|c$. So now $a|c$ and $b|c$, hence $m|c$, as desired. □

(2b)[2 pts - completion] Use (1) to prove that for any integers a and b which are both nonzero, we have $\text{lcm}(a,b) = \text{lcm}(a,-b)$. Hint: for any integers x and y which are not both 0, we have $\text{lcm}(x,y) = \text{lcm}(y,x)$. Your proof should be very short; do NOT just rewrite the proof of (1) here but for b.

Proof. Let a and b be integers which are both not 0. Then $\text{lcm}(a,b) = \text{lcm}(b,a)$ (by the hint, which I told you that you didn't have to prove). By (2a), $\text{lcm}(b,a) = \text{lcm}(-b,a)$. Now by the hint again, $\text{lcm}(-b,a) = \text{lcm}(a,-b)$. This shows that $\text{lcm}(a,b) = \text{lcm}(a,-b)$. □

(2)(c)[2 pts - completion] Use the above to prove that for any integers a and b which are both nonzero, we have $\text{lcm}(a,b) = \text{lcm}(-a,-b)$.

Proof. Let a and b be integers which are both not 0. By (2a), $\text{lcm}(a,b) = \text{lcm}(-a,b)$. Now by (2b), $\text{lcm}(-a,b) = \text{lcm}(-a,-b)$. □

(3)[10 pts] Use problems (1) and (2) to prove that for any nonzero integers a and b, we have $\gcd(a,b) \cdot \text{lcm}(a,b) = |ab|$. Hint: use cases and the Relating the GCD and the LCM Theorem (February 27 notes), which proves the above in the case that a and b are positive. Remember that for any integer x, $|x| = x$ if $x \geq 0$ and $|x| = -x$ if $x < 0$.

Proof. Let a and b be nonzero integers. We will prove the above equation by cases, using (1) and (2).

Case 1: $a > 0$ and $b > 0$: then $\gcd(a,b) \cdot \text{lcm}(a,b) = ab = |ab|$ by the theorem from class.

Case 2: $a < 0$ and $b > 0$: then $-a > 0$ and $b > 0$. So by the theorem from class and problems (1) and (2), we have $\gcd(a,b) \cdot \text{lcm}(a,b) = \gcd(-a,b) \cdot \text{lcm}(-a,b) = -ab = |ab|$.

Case 3: $a > 0$ and $b < 0$: this is analogous to Case 2.

Case 4: $a < 0$ and $b < 0$: then $-a > 0$ and $-b > 0$. Then by the theorem from class and problems (1) and (2), $\gcd(a,b) \cdot \text{lcm}(a,b) = \gcd(-a,-b) \cdot \text{lcm}(-a,-b) = -a \cdot -b = ab = |ab|$ (since a and b are negative, ab is positive, so $ab = |ab|$). □

(4)[10 pts] Let p be a prime number and let a be any integer. Prove that either $p|a$ or that p and a are relatively prime (for the latter, do NOT try to write 1 as a linear combination of p and a; just use the definition of 'prime' and 'relatively prime.' You do NOT need any theorems to do this).

Proof. Let p be a prime number and a be an integer. Then either $p|a$ or $p \nmid a$. If $p|a$, we are done. So assume that $p \nmid a$. The only possible positive common factors of p and a are 1 and p since p is prime. Since we have assumed that $p \nmid a$, p is NOT a COMMON factor of p and a. This leaves 1 as the only positive common factor of p and a is 1, and so $\gcd(p,a) = 1$. □

5)[9 pts] Let $n > 1$ be an integer. Suppose that for any integers a and b: if $n|ab$, then $n|a$ or $n|b$. Prove that n is prime. Hint: if n is not prime, you can use a lemma to help you that I proved on 3/1.

Proof. Assume by way of contradiction that there exists an integer $n > 1$ such that for all integers a and b: if $n|ab$, then $n|a$ or $n|b$, yet n is not prime. Then by the lemma referenced above, $n = rs$ for some integers r and s such that $1 < r, s < n$. Since $n \cdot 1 = rs$, we see that $n|rs$. By the above condition, $n|r$ or $n|s$. But then $n \leq r$ or $n \leq s$, contradicting that $n > r$ and $n > s$. $\square$