Math 310 Homework 3

Jacob Shiohira

February 2, 2017

Note: This homework took a total of 6 hours. I initially did it alone, but I did review with Jacob Warner. He helped me a lot with Problem 2, namely, he introduced the idea of using if $a|b$ and $b|c$, then $a|c$.

Problem 1. Let $a, b, c \in \mathbb{Z}$ be so that $a, b, c \neq 0$. Write a formal definition for the greatest common divisor of a, b, c, denoted (a, b, c).

According to Bèzout's Identity, if $gcd(a_1, a_2, ..., a_n) = d$, then there are integers $x_1, x_2, ..., x_n$ such that $d = a_1x_1 + a_2x_2 + ... + a_nx_n$. Note that this was referenced in the formal definition of the greatest common denominator of two integers, and it can be extended to the definition of the greatest common denominator of three integers.

Definition Let $a, b, c, d \in \mathbb{Z}$, $abc \neq 0$ and $d > 0$. Then d is the greatest common divisor of a, b, and c if and only if d satisfies these conditions:

i $d|a$, $d|b$, and $d|c$

ii If $m|a$, $m|b$, and $m|c$, then $m \leq d$ for $m \in \mathbb{Z}$.

Problem 2. Show that for all integers a, b, c, all non-zero, $((a, b), c) = (a, (b, c)) = (a, b, c)$.

Note: In order to make this proof much shorter, we will use the following result (the proof follows):

If $a|b$ and $b|c$, then $a|c$.

Let a, b, and c be integers. Suppose that $a|b$ and $b|c$. We want to then show that $a|c$. Since $a|b$, we know $b = am$ for some integer m from the definition of divisibility. Likewise, we know $c = bn$ for some integer n. By substituting $b = am$ for b in $c = bn$, we get $c = (am)n$. By the associative property of the integers, we have that $c = a(mn)$. Thus, $c|a$.

Claim I We are going to first show that $((a, b), c) = (a, b, c)$.

Suppose that $(a, b, c) = e$, $((a, b), c) = f$, and $(a, b) = d$. Through substitution, $((a, b), c)$ becomes $(d, c) = f$. Then, Bèzout's Identity says that $e = au + bv + cw$ and $f = (a, b)u_0 + cv_0 = du_0 + cv_0$. By the definition of divisibility, we know that $f|d$ and $f|c$, which also means $c = fc_f$ for some integers c_f. We can use the result above to show that since $f|d$ and $d|a$

and $d|b$, we know $f|a$ and $f|b$, which means $a = fa_f$ and $b = fb_f$ for some integers a_f, b_f. Finally, from $(a, b, c) = e$, we know that $e|a$, $e|b$ and $e|c$, which means $a = ea_e$, $b = eb_e$ and $c = ec_e$ for some integers a_e, b_e, c_e. We can then take $e = au + bv + cw$ and substitute values for a, b, and c to get

$$e = (fa_f)u + (fb_f)v + (fc_f)w.$$

By the associative and distributive property of the integers, we then have

$$e = f(a_f u + b_f v + c_f w).$$

Since the integers are closed under addition and multiplication, $a_f u + b_f v + c_f w$ is an integer, and we have that $f|e$. By definition of divisibility, if $f|e$, then $f \leq e$. Now, we can then take $f = du_0 + cv_0$ and substitute d to get

$$f = (au + bv)u_0 + cv_0.$$

By the associative and distributive property of the integers, we then have

$$f = auu_0 + bvu_0 + cv_0.$$

We can now substitute our values for a, b, and c to get

$$f = (ea_e)uu_0 + (eb_e)vu_0 + (ec_e)v_0.$$

By the associative and distributive property of the integers, we then have

$$f = e(a_e uu_0 + b_e vu_0 + c_e v_0).$$

Since the integers are closed under addition and multiplication, $a_e uu_0 + b_e vu_0 + c_e v_0$ is an integer, and we have that $e|f$. By definition of divisibility, if $e|f$, then $e \leq f$. So, we have reached that $e \leq f$ and $f \leq e$. Thus, $e = f$, therefore proving that $((a, b), c) = (a, b, c)$.

Claim II We are going to first show that $(a, (b, c)) = (a, b, c)$.

Suppose that $(a, b, c) = e$, $(a, (b, c)) = f$, and $(b, c) = d$. Through substitution, $(a, (b, c))$ becomes $(a, d) = f$. Then, Bèzout's Identity says that $e = au + bv + cw$ and $f = au_0 + (b, c)v_0 = au_0 + dv_0$. By the definition of divisibility, we know that $f|a$ and $f|d$, which also means $a = fa_f$ for some integers a_f. We can use the result above to show that since $f|d$ and $d|b$ and $d|d$, we know $f|b$ and $f|c$, which means $b = fb_f$ and $c = fc_f$ for some integers b_f, c_f. Finally, from $(a, b, c) = e$, we know that $e|a$, $e|b$ and $e|c$, which means $a = ea_e$, $b = eb_e$ and $c = ec_e$ for some integers a_e, b_e, c_e. We can then take $e = au + bv + cw$ and substitute values for a, b, and c to get

$$e = (fa_f)u + (fb_f)v + (fc_f)w.$$

By the associative and distributive property of the integers, we then have

$$e = f(a_f u + b_f v + c_f w).$$

Since the integers are closed under addition and multiplication, $a_f u + b_f v + c_f w$ is an integer, and we have that $f|e$. By definition of divisibility, if $f|e$, then $f \leq e$. Now, we can then take $f = au_0 + dv_0$ and substitute d to get

$$f = au_0 + (bu + cv)v_0.$$

By the associative and distributive property of the integers, we then have

$$f = au_0 + buv_0 + cvv_0.$$

We can now substitute our values for a, b, and c to get

$$f = (ea_e)u_0 + (eb_e)uv_0 + (ec_e)vv_0.$$

By the associative and distributive property of the integers, we then have

$$f = e(a_e u_0 + b_e uv_0 + c_e vv_0).$$

Since the integers are closed under addition and multiplication, $a_e u_0 + b_e uv_0 + c_e vv_0$ is an integer, and we have that $e|f$. By definition of divisibility, if $e|f$, then $e \leq f$. So, we have reached that $e \leq f$ and $f \leq e$. Thus, $e = f$, therefore proving that $(a, (b, c)) = (a, b, c)$. We have now shown that $((a, b), c) = (a, b, c)$ and $(a, (b, c)) = (a, b, c)$, so $((a, b), c) = (a, (b, c)) = (a, b, c)$ must hold. $\square$

Problem 3. Show that for all $a, b \in \mathbb{Z}$, both non-zero, and all $m, n \in \mathbb{Z}$, $(a, b)|(am + bn)$.

To show $(a, b)|(am + bn)$, we must show that this is only true $iff r = 0$. Suppose that $(a, b) = d$ for some $d \in \mathbb{Z}$. Per Bèzout's Identity, this means there exist $u, v \in \mathbb{Z}$ such that $d = au + bv$. Further, per the definition of gcd, $d|a$ and $d|b$. The definition of divisibility gives us that $a = dp$ and $b = dp_0$ for $p, p_0 \in \mathbb{Z}$. Consider the following two cases:

(a) If (a, b) divides $(am + bn)$, then $r = 0$

(b) If $r = 0$, then (a, b) divides $(am + bn)$.

Claim I If (a, b) divides $(am + bn)$, then $r = 0$.

Suppose that (a, b) divides $(am + bn)$. We then want to show that $r = 0$ follows. By the division algorithm, there exist $q, r \in \mathbb{Z}$ such that

$$am + bn = (a, b)q + r,\ 0 \leq r < (a, b) = d.$$

Since we are looking at the values of r, we can rearrange the equation

$$r = (am + bn) - (a, b)q.$$

By substituting and distributing,

$$\begin{gathered} r = (am + bn) - dq, \\ r = am + bn - dq, \\ r = dpm + dp_0 n - dq, \\ r = d(pm + p_0 n - q). \end{gathered}$$

Since $\mathbb{Z}$ is closed under addition and multiplication, $pm + p_0 n - q$ is also an integer. Thus, d must divide r. However, that would mean that $d < r$, but the division algorithm says that $r < d$. So,

Claim II If $r = 0$, then (a, b) divides $(am + bn)$.

Suppose that $r = 0$. We then want to show that (a, b) divides $(am + bn)$. By the division algorithm, if $r = 0$, there exist $q \in \mathbb{Z}$ such that

$$(am + bn) = (a, b)q + 0.$$

Then,

$$(am + bn) = (a, b)q.$$

By the definition of divisibility, (a, b) must divide $(am + bn)$. We can now combine Claim I and Claim II, and we see that (a, b) divides $(am + bn)$ if and only if $r = 0$. $\square$

Problem 4. See items a, b, and c.

(a) Find $(6, 21)$.

We can use the Euclidean Algorithm to now find the $gcd(6, 21)$:

$$A = 21, B = 6$$

Use long division to find that $21/6 = 3$ with a remainder of 3. We can write this as: $21 = 6 \cdot 3 + 3$. Find GCD$(6, 3)$, since GCD$(21, 6)$ = GCD$(6, 3)$.

$$A = 6, B = 3$$

Use long division to find that $6/3 = 2$ with a remainder of 0. We can write this as: $6 = 6 \cdot 2 + 0-$. Find GCD$(3, 0)$, since GCD$(21, 6)$ = GCD$(3, 0)$.

$$A = 3, B = 0$$

Thus, we have shown that GCD$(21, 6)$ = GCD$(6, 3)$ = GCD$(3, 0) = 3$. Note: Since the process is the same for the 12 steps below, I will not repeat the Euclidean algorithm for each one.

(b) Compute $(6, 21+6n)$ for new values of n. Make a conjecture about the value for all n.

Note: The last column in each of the tables represents the GCD of $b+an$ for each iteration.

$n=0$	$(6, 21+6(0))$	$(6, 21)$	3
$n=1$	$(6, 21+6(1))$	$(6, 27)$	3
$n=2$	$(6, 21+6(2))$	$(6, 33)$	3
$n=3$	$(6, 21+6(3))$	$(6, 39)$	3

We have now seen that the GCD(a, b) =GCD$(a, b+an)$ independent for any integer n. Thus, we arrive at the following conjecture:

Conjecture For any integer n, $(a, b) = (a, b+an)$.

(c) Try different values of a, b and make a conjecture about $(a, b+an)$.

Trial 8 and 32:

$n=1$	$(8, 14+8(1))$	$(8, 14)$	2
$n=1$	$(8, 14+8(1))$	$(8, 22)$	2
$n=2$	$(8, 14+8(2))$	$(8, 30)$	2
$n=3$	$(8, 14+8(3))$	$(8, 38)$	2

Trial -1 and 7:

$n=0$	$(-1, 7-1(0))$	$(1, 7)$	1
$n=1$	$(-1, 7-1(1))$	$(1, 6)$	1
$n=2$	$(-1, 7-1(2))$	$(1, 5)$	1
$n=3$	$(-1, 7-1(3))$	$(1, 4)$	1

Trial 4 and -26:

$n=0$	$(4, -26+4(0))$	$(4, -26)$	2
$n=1$	$(4, -26+4(1))$	$(4, -22)$	2
$n=2$	$(4, -26+4(2))$	$(4, -18)$	2
$n=3$	$(4, -26+4(3))$	$(4, -14)$	2

We have now seen through multiple examples that, independent of integers a, b and n, the $gcd(a, b)$ is always the same as $gcd(a, b+an)$. Thus, we arrive at the following conjecture:

Conjecture For any integers a, b, $a, b \neq 0$, $(a, b) = (a, b+an)$ for any $n \in \mathbb{Z}$.

Problem 5. See items a and b.

(a) If $a, b, u, v \in \mathbb{Z}$ are such that $au + bv = 1$, prove that $(a, b) = 1$.

Suppose that $au + bv = 1$ and that a, b have a common divisor c. Then, we would have that $a = cx$ and $b = cy$. Substituting the new values of a and b would yield $(cx)u + (cy)v = 1$. From the associative property and distributive of the integers, we have that $c(xu + yv) = 1$. It then follows that $c|1$ because $xu + yv$ is an integer, as a result of the integers being closed under addition and multiplication. Since c is a divisor of 1, $c \leq 1$. The definition of *gcd* of two integers states that $c \geq 1$, and we arrive at the following restriction on 1: $1 \leq c \leq 1$. Referencing the fact that the integers are not dense, $1 = 1$ and $(a, b) = 1$. $\square$

(b) Show by example that if $au + bv = d > 1$, then (a, b) may not be d.

Consider $a = 1$, $b = 7$, $u = 1$, and $v = 1$. Then

$$au + bv = 7$$

but $gcd(1, 7) = 1$.

Problem 6. If $a|c$ and $b|c$ and $(a, b) = d$, prove that $ab|cd$.

Suppose $a|c$ and $b|c$ and $(a, b) = d$. Since $a|c$ and $b|c$, we know $c = ax$ and $c = by$ for some $x, y \in \mathbb{Z}$. Additionally, Bèzout's Identity gives us that $d = au + bv$ for some $u, v \in \mathbb{Z}$. We want to show that $ab|cd$ then follows. We can multiply by c on both sides of $d = au + bv$ to get

$$cd = c(au + bv).$$

By distribution property of the integers,

$$cd = cau + cbv.$$

We can now substitute $c = ax$ and $c = by$ and then apply the associative property of the integers to get

$$cd = (by)au + (ax)bv$$

and

$$cd = ab(yu) + ab(xv).$$

We can factor out ab from the right hand side to get

$$cd = ab(yu + xv).$$

Finally, we can then invoke the definition of divisibility because we know $yu + xv$ is also an integer since the integers are closed under addition and multiplication. Thus, ab must divide cd. $\square$