Math 3110: Quiz #1 – Solutions

February 5, 2019

Name:

Question 1

(10 minutes / 10 points)

1. (4 points) State the definition of the *greatest common divisor* of two integers a and b. You will be graded on mathematical correctness as well as writing.

   Definition 1. *Let $a, b \in \mathbb{Z}$. A non-negative integer g is called the* greatest common divisor of a and b *if it satisfies the following properties:*

   (a) $g \mid a$ *and* $g \mid b$

   (b) for any other integer d, if $d \mid a$ and $d \mid b$ then $d \mid g$.

   In this case, we write $g = \gcd(a, b)$.

   Please see the separate sheet on writing definitions in general.

2. (6 points) Prove the following theorem. You will be graded on mathematical correctness as well as writing. Hint: Use the definition of the gcd.

   Theorem 1. *Let $a, b, c \in \mathbb{Z}$. Then* $\gcd(a, c) \mid \gcd(ab, c)$.

   Proof. We know $\gcd(a, c) \mid a$ and $\gcd(a, c) \mid c$ from the definition of $\gcd(a, c)$. Using the former, by the transitivity of divisibility, we obtain $\gcd(a, c) \mid ab$. Therefore $\gcd(a, c)$ is a common divisor of ab and c. By the definition of $\gcd(ab, c)$, then $\gcd(a, c) \mid \gcd(ab, c)$. □

Question 2

(20 minutes / 20 points) This question has two parts.

1. (8 points) Demonstrate and explain the Euclidean Algorithm to find the greatest common divisor of 489 and 165. Other methods will receive no credit. For full credit, write several clear sentences indicating what you are doing (don't just show computations). You do not need to explain why it works, but explain *what* you are doing. You will be graded on mathematical correctness and presentation/writing.

   To perform the Euclidean algorithm, we successively replace a given pair of numbers with a simpler pair having the same gcd. If we have pair (a, b), $a > b$, we use the division algorithm to write

$$a = bq + r, \quad 0 \leq r < b$$

and then continue with the new pair (b, r). We stop when we reach $\gcd(g, 0)$ for some g, which is the gcd.

$$\begin{aligned} 489 &= 2 \cdot 165 + 159 \\ 165 &= 1 \cdot 159 + 6 \\ 159 &= 26 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0 \end{aligned}$$

From the computation above, $\gcd(489, 165) = 3$.

2. (12 points) Find all integer solutions to the equation $489x + 165y = 9$. For full credit, show and justify all your work. You will be graded on mathematical correctness and presentation/writing.

   We perform the Extended Euclidean algorithm on the coefficients 489 and 165:

$(1, 0)$ gives 489	$= 2 \cdot$	$(0, 1)$ gives 165	$+$	$(1, -2)$ gives 159
$(0, 1)$ gives 165	$= 1 \cdot$	$(1, -2)$ gives 159	$+$	$(-1, 3)$ gives 6
$(1, -2)$ gives 159	$= 26 \cdot$	$(-1, 3)$ gives 6	$+$	$(27, -80)$ gives 3
$(-1, 3)$ gives 6	$= 2 \cdot$	$(27, -80)$ gives 3	$+$	$(-55, 163)$ gives 0

   This informs us that $(27, -80)$ is a solution to $489x + 165y = 3$.

   Therefore, multiplying by 3, $(81, -240)$ is a solution to $489x + 165y = 9$.

   Since $\gcd(489, 165) = 3$, the homogeneous solution set to $489x + 165y = 0$ is

$$\{(-(165/3)k, (489/3)k) : k \in \mathbb{Z}\}\{(-55k, 163k) : k \in \mathbb{Z}\}$$

   Therefore, combining our particular solution with the homogeneous solution set, we obtain a complete solution set for $489x + 165y = 9$:

$$\{(81 - 55k, -240 + 163k) : k \in \mathbb{Z}\}.$$

Question 3

(10 minutes / 10 points)

Prove the following theorem (this is the division algorithm). You will be graded on mathematical correctness as well as writing. Hints: The textbook started by considering the quantity $a/b - \lfloor a/b \rfloor$. In class, we began by letting $q = \lfloor a/b \rfloor$.

Theorem 2. *Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist integers q and r satisfying*

$$a = bq + r, \quad 0 \leq r < b.$$

See your class notes or textbook, both of which have proofs of this.

Question 4

(5 minutes / 5 points)

Prove the following theorem. You will be graded on mathematical correctness as well as writing. Hint: Use a linear diophantine equation.

Theorem 3. *Suppose that a, b, c are integers, and $\gcd(a, b) = 1$. Suppose that $a \mid bc$. Then $a \mid c$.*

This is a famous argument called *Euclid's Lemma.*

Solution #1. Since $\gcd(a, b) = 1$, we know $1 = ax + by$ for some x and y. Therefore $c = c(ax + by) = acx + bcy$. But a divides both of these terms, so $a \mid c$. □

Solution #2. Since $a \mid bc$, there is some integer k such that $ak = bc$. Therefore $-ak + bc = 0$. Therefore, $(-k, c)$ is a solution to the homogeneous linear diophantine equation $ax + by = 0$. The solutions set to this equation is $\{(-bn, an) : n \in \mathbb{Z}\}$. Since $(-k, c)$ is in this set, $c = an$ for some integer n. That is, $a \mid c$. □