Math 230 — Exam 2 — Thurs Oct 25

Fall 2018
Drew Armstrong

Problem 1.

(a) Use the Extended Euclidean Algorithm to find **one solution** $x, y \in \mathbb{Z}$ of the equation

$$36x + 15y = 3.$$

Consider the following table of triples $x, y, z \in \mathbb{Z}$ such that $36x + 15y = z$:

x	y	z	row operation	
1	0	36	(row 1)	
0	1	15	(row 2)	
1	-2	6	(row 3)	$=$ (row 1) $- 2 \cdot$ (row 2)
-2	5	3	(row 4)	$=$ (row 2) $- 2 \cdot$ (row 3)
5	-12	0	(row 5)	$=$ (row 3) $- 2 \cdot$ (row 4)

From (row 4) we obtain the solution $(x, y) = (-2, 5)$.

(b) Tell me the **general solution** $x, y \in \mathbb{Z}$ of the equation $36x + 15y = 0$. [You do not need to prove anything.]

Divide the equation by $\gcd(36, 15)$ (which is 3) to obtain $12x + 5y = 0$. Since 12 and 5 are coprime, the general solution is

$$(x, y) = (5k, -12k) \quad \text{for all } k \in \mathbb{Z}.$$

This solution can also be obtained from (row 5) above.

(c) Now tell me the **general solution** $x, y \in \mathbb{Z}$ of the equation $36x + 15y = 3$.

Adding the solutions from (a) and (b) gives

$$(x, y) = (-2, 5) + (5k, -12) = (-2 + 5k, 5 - 12k) \quad \text{for all } k \in \mathbb{Z}.$$

Problem 2. Consider $a, b, c, x \in \mathbb{Z}$ such that $a = bx + c$, and define the following sets:

$$\text{Div}(a, b) = \{d \in \mathbb{Z} : d|a \text{ and } d|b\}$$
$$\text{Div}(b, c) = \{d \in \mathbb{Z} : d|b \text{ and } d|c\}.$$

(a) Prove that $\text{Div}(b, c) \subseteq \text{Div}(a, b)$.

Proof. Let $d \in \text{Div}(b, c)$, so that $b = db'$ and $c = dc'$ for some $b', c' \in \mathbb{Z}$. Then we have

$$a = bx + c = (db')x + (dc') = d(b'x + c'),$$

which implies that $d|a$ and hence $d \in \text{Div}(a, b)$. $\square$

(b) Prove that $\text{Div}(a, b) \subseteq \text{Div}(b, c)$.

Proof. Let $d \in \text{Div}(a, b)$, so that $a = da'$ and $b = db'$ for some $a', b' \in \mathbb{Z}$. Then we have

$$c = a - bx = (da') - (db')x = d(a' - b'x),$$

which implies that $d|c$ and hence $d \in \text{Div}(b, c)$. □

(c) Use the result of (a) and (b) to prove that $\gcd(a, b) = \gcd(b, c)$.

Proof. From (a) and (b) we conclude tha $\text{Div}(a, b) = \text{Div}(b, c)$. Since the sets are equal, they must have the largest element. □

Problem 3. Division With Remainder.

(a) Accurately state the Division Theorem.

For all $a, b \in \mathbb{Z}$ with $b \neq 0$, there exist unique integers $q, r \in \mathbb{Z}$ such that

$$\begin{cases} a = qb + r, \\ 0 \leq r < |b|. \end{cases}$$

Remark: These unique q, r are called the quotient and remainder of a mod b.

(b) Explain why 3 is the remainder of 15 mod 6.

Because

$$\begin{cases} 15 = 2 \cdot 6 + 3, \\ 0 \leq 3 < |6|. \end{cases}$$

(c) Explain why the equation $15 = 6x$ has no integer solution $x \in \mathbb{Z}$.

Assume for contradiction that such an integer $x \in \mathbb{Z}$ exists. Then we have

$$\begin{cases} 15 = x \cdot 6 + 0, \\ 0 \leq 0 < |6|. \end{cases}$$

Since $0 \neq 3$ this contradicts the uniqueness of the remainder.

Problem 4. Let $\alpha \in \mathbb{R}$ be a real number that is **not** an integer.

(a) Use Well-Ordering to prove that there exists an integer $m \in \mathbb{Z}$ with $m - 1 < \alpha < m$. [Hint: Let S be the set of integers that are greater than α.]

Proof. Let S be the set of integers that are greater than α. By Well-Ordering this set has a least element, say m. Since $m \in S$ we have $\alpha < m$, and since $m - 1 < m$ we have $m - 1 \notin S$, hence $m - 1 \leq \alpha$. Finally, since α is not an integer we have $m - 1 < \alpha$. □

(b) If the integers $m, n \in \mathbb{Z}$ satisfy $m - 1 < \alpha < m$ and $n - 1 < \alpha < n$, prove that $m = n$. [Hint: Show that $m < n$ leads to a contradiction.]

Proof. Assume for contradiction that $m < n$. Then we have

$$n - 1 < \alpha < m < n,$$

which implies that $n - 1 < m < n$. This contradicts the fact that there are no integers between $n-1$ and n. If you don't believe that, subtract $n-1$ to obtain $0 < m-n+1 < 1$. This contradicts the fact that there are no integers between 0 and 1.

The same proof shows that $n < m$ is impossible, so we conclude that $m = n$. $\square$

[Remark: Putting (a) and (b) together, we conclude that there exists a **unique** integer $m \in \mathbb{Z}$ such that $m - 1 < \alpha < m$.]