MATH 135 Fall 2020: Extra Practice 7

Warm-Up Exercises

WE01. Find the complete integer solution to $7x + 11y = 3$.

Solution. Begin by applying the EEA to determine one solution for x and y:

x	y	r	q
1	0	7	0
0	1	11	0
-1	1	4	-1
2	-1	3	2

which gives $7(2)+11(-1) = 3$. Since 7 and 11 are prime, we immediately know their GCD is 1. Now, apply the LDET to determine the complete solution set:

$$\{(x, y) : x = 2 + 11n, y = -1 - 7n, n \in \mathbb{Z}\}$$ □

WE02. Find the complete integer solution to $28x + 60y = 10$.

Solution. Begin by applying the EEA to find the GCD:

y	x	r	q
1	0	60	0
0	1	28	0
1	-4	4	2
-7	29	0	7

Therefore, $\gcd(28, 60) = 4$. However, $4 \nmid 10$, so there are no solutions to this equation. □

Recommended Problems

RP01. Find all non-negative integer solutions to $12x + 57y = 423$.

Solution. Since $12 = 3 \times 4$ and $57 = 3 \times 19$, clearly $\gcd(12, 57) = 3$. We also have that $423 \mid 3$, so solutions exist. Applying EEA, we have

y	x	r	q
1	0	57	0
0	1	12	0
1	-4	9	4
-1	5	3	1

so our base solution is $12(5) + 57(-1) = 3$. Multiplying through by $\frac{423}{3} = 141$, we have $12(705) + 57(-141) = 423$. By the LDET, we arrive at our solution set in the integers:

$$\{(x, y) : x = 705 + 19n, y = -141 - 4n, n \in \mathbb{Z}\}$$

However, we want to restrict $x \geq 0$ and $y \geq 0$. Notice that $x \geq 0$ when $n \geq -\frac{705}{19}$, that is, $n \geq -37$. Likewise, $y \geq 0$ when $n \leq -\frac{141}{35}$, that is, $n \leq -36$.

This just means that $-37 \leq n \leq -36$, or $n = -37, -36$. Therefore, the solution set is $(x, y) \in \{(2, 7), (21, 3)\}$. □

RP02. Prove or disprove the following implications:

(a) For all integers a, b, and c, if there exists an integer solution to $ax^2 + by^2 = c$, then $\gcd(a, b) \mid c$.

Proof. Let a, b, and c be integers. Suppose there is an integer solution in x and y to the equation $ax^2 + by^2 = c$. Since x^2 and y^2 are integers, this is a solution to the equation $as + bt = c$ with integers $s = x^2$ and $t = y^2$.

It immediately follows from the LDET that $\gcd(a, b) \mid c$. □

(b) For all integers a, b, and c, if $\gcd(a, b) \mid c$, then there exists an integer solution to $ax^2 + by^2 = c$.

Proof. Consider the counterexample where $a = b = 1$ and $c = -2$. We have that $\gcd(a, b) = \gcd(1, 1) = 1$ and clearly $1 \mid -2$.

We now have the equation $(1)x^2 + (1)y^2 = -2$. From the properties of integers, $x^2 \geq 0$ and $y^2 \geq 0$, so $x^2 + y^2 \geq 0$. Then, $x^2 + y^2 \geq 0$ but -2 is not non-negative. Therefore, no solutions to $x^2 + y^2 = -2$ exist. □

RP03. Consider the following statement: For all integers a, b, c, and x_0, there exists an integer y_0 such that $ax_0 + by_0 = c$.

(a) Carefully write down the negation of this statement and prove that this negation is true.

Proof. We prove the negation:

There exist integers a, b, c, and x_0 such that for all integers y_0, $ax_0 + by_0 \neq c$.

Select $a = x_0 = 1$, $b = 0$, and $c = 2$. Let y_0 be an integer. We must show that $(1)(1) + (0)y_0 \neq (2)$. This is just $1 \neq 2$, which is true independent of y_0. □

(b) Let $a, b, c \in \mathbb{Z}$. Fill in the blank to make the following statement true and prove that it is true. $\boxed{b \text{ is non-zero, } b \mid a \text{, and } b \mid c}$ if and only if for all integers x_0, there exists an integer y_0 such that $ax_0 + by_0 = c$.

Proof. Let a, b, and c be integers.

We prove the biconditional by proving both implications.

($\Rightarrow$) Suppose b is non-zero, $b \mid a$, and $b \mid c$. We break into cases on a:

If $a = 0$, then we must show that there exists a y_0 such that $by_0 = c$. This follows immediately from the fact that $b \mid c$.

If a is non-zero, it follows that $\gcd(a, b) = |b|$. Then, since $b \mid c$, we have $\gcd(a, b) \mid c$. We may now apply the LDET. The solution set to the linear Diophantine equation $ax_0 + by_0 = c$ is

$$\{(x_0, y_0) : x_0 = x + \frac{b}{|b|}n, y_0 = y + \frac{a}{|b|}n, n \in \mathbb{Z}\}$$

for some initial solution (x, y). Since n ranges through all integers, we may drop the absolute value bars. Then, $x_0 = x + n$, so every integer x_0 appears in the solution set at $n = x_0 - x$, with a corresponding y_0.

Alternatively stated, for every integer x_0, there exists a y_0 such that $ax_0 + by_0 = c$.

($\Leftarrow$) Suppose that for all integers x_0, we may choose an integer y_0 so $ax_0 + by_0 = c$. Let x_0 be an integer.

Suppose for a contradiction that $b = 0$, so $ax_0 = c$. This is clearly not true for all a, c, and x_0. Therefore, b is non-zero.

Now, break into cases on a. Suppose that $a = 0$. Then, we may find y_0 such that $by_0 = c$, which is the same as saying $b \mid c$.

Suppose that a is non-zero. Since both a and b are non-zero and $ax_0 + by_0 = c$ is a solution to the LDE $ax + by = c$, the LDET applies, giving $\gcd(a, b) \mid c$.

However, since the LDET applies, there is an entire solution set given by

$$\{(x, y) : x = x_0 + \frac{b}{\gcd(a, b)}n, y = y_0 + \frac{a}{\gcd(a, b)}n, n \in \mathbb{Z}\}$$

Now, recall that x_0 is an arbitrary integer. Therefore, the values of x given in the set above must also span the integers, that is, any arbitrary integer x may be written $x_0 + \frac{b}{\gcd(a,b)}n$.

This implies that $\frac{b}{\gcd(a,b)} = 1$, that is, $b = \gcd(a, b)$, since GCD is positive.

Therefore, b is non-zero, $\gcd(a, b) = b$ divides c, and by definition, b divides a. □

RP04. Suppose a and b are integers. Prove that $\{ax+by : x, y \in \mathbb{Z}\} = \{n \gcd(a, b) : n \in \mathbb{Z}\}$.

Proof. Let a and b be integers with GCD d. We prove $\{ax + by : x, y \in \mathbb{Z}\} = \{nd : n \in \mathbb{Z}\}$ by mutual containment.

($\subseteq$) Let x and y be integers. Then, since $d \mid a$ and $d \mid b$, $d \mid (ax + by)$. This means we may write $ax + by$ as nd, as desired.

($\supseteq$) Let n be an integer. By Bézout's Lemma, we may write $d = xs + yt$ for integers s and t. Multiplying through by n, we have $nd = (ns)x + (nt)y$. We may let $a = ns$ and $b = nt$, which are integers, and have $nd = ax + by$ as desired.

Therefore, since the sets are mutually contained, they are equal. □

Note: This is essentially a restatement of Jerry Wang's GCD derivation by subgroups.

Challenge

C01. For how many integer values of c does $8x + 5y = c$ have exactly one solution where both x and y are strictly positive integers?