Math 3110: Worksheet on Linear Diophantine Equations

January 28, 2019

Your goal: Determine the complete description of the integer solutions to a linear Diophantine equation $ax + by = c$, where $a, b, c \in \mathbb{Z}$. The term *Diophantine* simply means that we are studying the equation for its integer solutions.

Linear Diophantine Equations: First Experimentation

1. Do integer solutions to $2x + 3y = 0$ exist? If so, find one. If not, explain why not.

2. Do integer solutions to $2x + 3y = 1$ exist? If so, find one. If not, explain why not.

3. Do integer solutions to $2x + 3y = 107$ exist? If so, find one. If not, explain why not.

   Is there a clever way to notice this using the previous items?

4. Do integer solutions to $10x + 15y = 5$ exist? If so, find one. If not, explain why not.

   Is there a clever way to notice this using the previous items?

5. Do integer solutions to $10x + 15y = 1$ exist? If so, find one. If not, explain why not.

Homogeneous Linear Diophantine Equations

The term *homogeneous* means the number after the = is zero.

1. Determine *all* the integer solutions to $2x + 3y = 0$. (Write your solution using set bracket notation.)

2. Fill in the Theorem statement:

   Theorem 1 (Homogeneous Case)**.** *Let* $a, b \in \mathbb{Z}$. *The set of integer solutions* (x, y) *to the equation* $ax + by = 0$ *is*

3. Give a careful proof of the theorem. Don't forget you must show that these are solutions and that there are no other solutions.

One will do it

1. Find one solution to $2x + 3y = 1$ (by inspection).

2. Find all solutions to $2x + 3y = 0$ (using the Homogeneous Case Theorem).

3. Using the previous two items, what are *all* the solutions to $2x + 3y = 1$? (Use set builder notation.)

4. Fill in the statement of the Theorem

   Theorem 2 (One Gives All Theorem)**.** *Let $a, b, c \in \mathbb{Z}$. Suppose that (x_0, y_0) is one integer solution to $ax + by = c$. Then the set of all integer solutions to the equation is*

An improvement

1. Find one solution to $2x + 3y = 107$ (Don't do this by inspection! Instead, adapt the solution you have to $2x + 3y = 1$.)

2. Using the previous item, and the homogeneous solution set, what are *all* the solutions to $2x + 3y = 107$? (Use set builder notation.)

3. Now we'll improve the One Gives All Theorem. Fill in the statement of the Theorem

   Theorem 3 (One Gives All Theorem, Improved)**.** *Let $a, b, c \in \mathbb{Z}$. Suppose that (x_0, y_0) is one integer solution to $ax + by = 1$. Then the set of all integer solutions to the equation $ax + by = c$ is*

4. Give a careful proof of the theorem. Don't forget you must show that these are solutions and that there are no other solutions.

The importance of the GCD

1. Above, you observed that $10x + 15y = 1$ had no solutions. What is the essential reason?

2. Fill in the Theorem statement:

   Theorem 4 (No solutions case)**.** *Let* $a, b, c \in \mathbb{Z}$*. If* ______________ *, then the equation* $ax + by = c$ *has no integer solutions.*

3. Write a careful proof of the Theorem.

4. I wonder, does the converse of this theorem hold? State the converse theorem.

5. State the converse theorem in another way. (One way is to say the non-existence of solutions implies something; the other is to say that something implies the existence of solutions.)

6. Do you believe it holds?

So what about that one solution?

Challenge: Suppose $\gcd(a, b) = 1$. How can you find a solution to $ax+by = 1$? One way to rephrase this is to ask for a linear combination of a and b that is 1. That is, you can add multiples of b to a, then multiples of a to the result, etc. etc., and you want to get a 1. Sound familiar?

1. Compute the $gcd(24, 17)$ using the Euclidean algorithm. Use the least positive remainder (standard division algorithm style), so we are all on the same page.

$$\begin{aligned} 24 &= \_\_ \cdot 17 + \_\_ \\ 17 &= \_\_ \cdot \_\_ + \_\_ \\ \_\_ &= \_\_ \cdot \_\_ + \_\_ \\ \_\_ &= \_\_ \cdot \_\_ + \_\_ \end{aligned}$$

2. Now fill out the corresponding "card" for each number. The card

(x, y) gives c

   tells you that the linear combination $24x + 17y = c$.

   Fill it out below. I've done the first line for you. **Notice how the "vectors" in the top row add and scalar multiply just like the numbers in the bottom row.**

$(1, 0)$ gives 24	$= 1 \cdot$	$(0, 1)$ gives 17	+	$(1, -1)$ gives 7
$(0, 1)$ gives 17	$= \_\_ \cdot$	(,) gives ___	+	(,) gives ___
(,) gives ___	$= \_\_ \cdot$	(,) gives ___	+	(,) gives ___
(,) gives ___	$= \_\_ \cdot$	(,) gives ___	+	(,) gives ___

3. Take a moment to check that your cards are still true. Meaning, does the indicated linear combination of 24 and 17 come out to the indicated value?

4. Looking at the above, write down a solution for $24x + 17y = 1$.

5. Now do you believe that the converse to the *No Solutions Case* Theorem holds? Write down an "if and only if" theorem.

   Theorem 5 (Existence of Solutions)**.** *Let $a, b, c \in \mathbb{Z}$. Then the equation $ax + by = c$ has at least one integer solution if and only if*

6. Give a complete and careful proof of this theorem.

Now test yourself

Use everything you've learned above to solve the following Diophantine equations completely (i.e. determine the complete solution set).

1. $18x + 16y = 5$

2. $23x + 19y = 17$