Intermediate Math Circles
February 29, 2012
Linear Diophantine Equations I

Diophantine equations are equations intended to be solved in the integers.

We're going to focus on Linear Diophantine Equations. That is, equations of the form $ax+by=c$, where a, b, c are given integers and we are solving for integers x and y.

For example:

$$7x + 3y = 4$$
or
$$10x + 4y = 12$$

How can we find solutions to these with x and y being integers?

Example 1: Suppose that Bob has \$1.55 in quarters and dimes. How many quarters and how many dimes does he have? (There might be more than one solution!)

Solution: We're trying to solve $25x + 10y = 155$ with x and y integers (which shouldn't, in this case, be negative!). By trial-and-error we can find

	$x = 1$	$y = 13$
or	$x = 3$	$y = 8$
or	$x = 5$	$y = 3$

Are there any other solutions?

Example 2: A robot can move backwards or forwards with big steps (130 cm) or small steps (50 cm). Is there a series of moves it can make to end up 10 cm ahead of where it started?
i.e., can we solve $130x + 50y = 10$?

Trial-and-error solution:

$x = 2 \qquad y = -5$

$\longrightarrow\longrightarrow$ 2 big steps forward

$\longleftarrow\longleftarrow\longleftarrow\longleftarrow\longleftarrow$ 5 small steps back

OR $\qquad x = 7 \qquad y = -18$

There are many solutions.

Its not always easy to find a solution to a linear Diophantine equation by trial and error. For example, suppose we were asked to find an integer solution to the linear Diophantine equation:

$$1053x + 481y = 13?$$

Main question: If a, b, and c are integers, then how can you find a solution to

$$ax + by = c$$

where x and y are integers?

Trick question! There might not be a solution!

For example, look at the equation

$$3x + 6y = 5$$

If we could find integers x and y for which that holds, then $x + 2y = \frac{5}{3}$.
And since x and y are integers, so is $x + 2y$. But $\frac{5}{3}$ is not an integer.

It appears as though, if any integer divides both a and b, then

$$ax + by = c$$

can only have a solution if that integer also divides c.

(An integer d "divides" another integer e if and only if there is some integer q such that $e = qb$).

Before we look at how to solve a linear Diophantine equation, let's first investigate when there is a solution. It appears as though the divisors of a and b are going to be important.

The **"greatest common divisor"** of a and b is the largest integer that divides a and divides b. We write it as gcd(a, b).

For example:

- gcd(3, 6) = 3
- gcd(10, 15) = 5
- gcd(117, 55) = 1
- gcd(84, 119) = 7
- gcd(481, 1053) = 13
- gcd(3551, 4399) = ?
- gcd(104723, 103093) = ?

1 divides everything, so gcd(a, b) is always at least 1.

What's the best way to calculate gcd(a, b)?

For small numbers a and b it's not too hard to find gcd by factoring a and b, but not as easy when trying to calculate

$$\text{gcd}(104723,\ 103093) \text{ or } \text{gcd}(3551,\ 4399)$$

You can try to find all divisors, and see which ones divide both, but that could take all day!

Instead, we'll use the **Euclidean Algorithm**.

First, the **Division Algorithm**: Suppose a, b are integers and $b > 0$.
There exists unique integers q, r such that
$a = qb + r$, where $0 \leq r < b$
(q - quotient, r - remainder)

For example,
$a = 15,\ b = 6 \qquad 15 = 2 \cdot 6 + 3$
$a = 30,\ b = 6 \qquad 30 = 5 \cdot 6 + 0$
$a = -10,\ b = 6 \qquad -10 = (-2) \cdot 6 + 2$
$a = -2,\ b = 6 \qquad -2 = (-1) \cdot 6 + 4$

Important Fact 1: $\boxed{\text{If } a = qb + r, \text{ then } \gcd(a, b) = \gcd(b, r).}$

For example,

$$\begin{aligned}
15 &= 2 \cdot 6 + 3 && \text{and} \quad \gcd(15, 6) = 3 = \gcd(6, 3) \\
30 &= 5 \cdot 6 + 0 && \text{and} \quad \gcd(30, 6) = 6 = \gcd(6, 0) \\
-10 &= (-2) \cdot 6 + 2 && \text{and} \quad \gcd(-10, 6) = 2 = \gcd(6, 2) \\
-2 &= (-1) \cdot 6 + 4 && \text{and} \quad \gcd(-2, 6) = 2 = \gcd(6, 4)
\end{aligned}$$

Why is this fact useful?

Example 3: Calculate gcd(117, 55)

Solution: $117 = 2 \cdot 55 + 7$, so

$$\gcd(117,\ 55) = \gcd(55,\ 7).$$

Now, $55 = 7 \cdot 7 + 6$, so

$$\gcd(55,\ 7) = \gcd(7,\ 6).$$

Again, $7 = 1 \cdot 6 + 1$, so

$$\gcd(7,\ 6) = \gcd(6,\ 1) = 1.$$

So $\gcd(117,\ 55) = 1$. $\square$

In Example 3 we used the "**Euclidean Algorithm**" for calculating $\gcd(a,\ b)$.

Step 1: Arrange a and b so that $a \geq b$.

Step 2: Write $a = qb + r$, with $0 \leq r < b$.

Step 3: If $r = 0$, then b divides a, so $\gcd(a,\ b) = b$. STOP!
If not then $\gcd(a,\ b) = \gcd(b,\ r)$.

Step 4: Go to Step 2 to calculate $\gcd(b,\ r)$.

Since the numbers get smaller after each iteration, you will eventually get an answer.

Example 4: Calculate gcd(481, 1053)

Solution:

$\gcd(481,\ 1053) = \gcd(1053,\ 481)$

$$\begin{aligned} 1053 = 2 \cdot 481 + 91,\ &\text{so} & \gcd(1053,\ 481) &= \gcd(481,\ 91) \\ 481 = 5 \cdot 91 + 26,\ &\text{so} & \gcd(481,\ 91) &= \gcd(91,\ 26) \\ 91 = 3 \cdot 26 + 13,\ &\text{so} & \gcd(91,\ 26) &= \gcd(26,\ 13) \\ 26 = 2 \cdot 13 + 0,\ &\text{so} & \gcd(26,\ 13) &= 13 \\ &\text{We have} & \gcd(481,\ 1053) &= 13. \end{aligned}$$

$\square$

Exercise Set 1

1. Calculate gcd(129, 48) by

   a) Factoring 129 and 48.

   b) The Euclidean Algorithm.

2. Use the Euclidean Algorithm to calculate gcd(427,616)

3. Use the Euclidean Algorithm to calculate gcd(3551, 4399)

4. Use the Euclidean Algorithm to calculate gcd(7826, 6279)

5. Use the Euclidean Algorithm to calculate gcd(104723,103093)

Answers to Exercise Set 1:

1. 3
2. 7
3. 53
4. 91
5. 1

An application of the Euclidean Algorithm: Solving linear Diophantine equations.

Example 5: Find integers x and y such that $1053x + 481y = 13$.

From the Euclidean Algorithm:

$$\begin{aligned} 1053 &= 2 \cdot 481 + 91 && (1) \\ 481 &= 5 \cdot 91 + 26 && (2) \\ 91 &= 3 \cdot 26 + 13 && (3) \\ 26 &= 2 \cdot 13 + 0 && (4) \end{aligned}$$

Working backwards:

$$\begin{aligned} 13 &= 91 - 3 \cdot 26 \quad \text{from } (3) \\ &= 91 - 3(481 - 5 \cdot 91) \quad \text{from } (2) \\ &= 16 \cdot 91 - 3 \cdot 481 \\ &= 16(1053 - 2(481)) - 3 \cdot 481 \quad \text{from } (1) \\ &= 16(1053) - 35(481) \end{aligned}$$

Therefore, a solution is $x = 16, y = -35$. (Check!)

$\square$

Example 6: Find integers x and y such that $1053x + 481y = 14$.

$1053x + 481y = 14$
Factoring gcd(1053,481) = 13 on the left:
$13(37x + 81y) = 14$, which is not possible if x and y are integers!
Therefore, there is no solution.

Important Fact 2: $\boxed{ax + by = c \text{ has a solution if and only if } \gcd(a,\, b) \text{ divides } c.}$

Exercise Set 2

1. Find an integer solution to $129x + 48y = 4$, or explain why one doesn't exist.

2. Find an integer solution to $117x + 55y = 1$, or explain why one doesn't exist.

3. Find an integer solution to $427x + 616y = 7$.

4. Find an integer solution to $3551x + 4399y = 53$.

5. Find an integer solution to $6279x + 7826y = 91$.

Answers to Exercise Set 2:

1. There is no solution since $\gcd(129, 48) = 3$, and 3 does not divide 4.
2. $(x, y) = (8, -17)$ is one (of many) solutions.
3. $(x, y) = (13, -9)$ is one (of many) solutions.
4. $(x, y) = (-26, 21)$ is one (of many) solutions.
5. $(x, y) = (5, -4)$ is one (of many) solutions.

What about solving $ax + by = c$ when c is <u>not</u> $\gcd(a,\ b)$?
We know from Important Fact 2, that if $\gcd(a,\ b)$ divides c, there is a solution.

Example 7: Find an integer solution to $1053x + 481y = 39$.

Since $\gcd(1053,\ 481) = 13$ and 13 divides 39, we know that there is a solution to this linear Diophantine equation.

We already know that	$1053(16) + 481(-35) = 13$
Multiplying both sides by 3:	$3 \cdot 1053(16) + 3 \cdot 481(-35) = 3 \cdot 13$
And so	$1053(3 \cdot 16) + 481(3 \cdot (-35)) = 39$
Therefore,	$1053(48) + 481(-105) = 39$

Therefore, $x = 48, y = -105$ is a solution.

$\square$

In general, how do we solve $ax + by = c$ when c is <u>not</u> $\gcd(a,\ b)$?

If $\gcd(a, b)$ does not divide c, then there is no solution.

If $\gcd(a, b)$ does divide c, then

1. Solve $ax + by = \gcd(a,\ b)$.
2. Multiply the x and y in the solution by $\dfrac{c}{\gcd(a,\ b)}$.