Exploration 1: Integer linear equations

Lacey Conrad (and Ali Alnasser)

due: 2/08/2016 (rough), 2/12/2016 (final)

Abstract

This report synthesizes and explains the discoveries our Number Theory class encountered while studying integer linear equations.

1 Introduction

Our exploration begun with a logical starting point for the study of number theory: solving Diophantine equations, which are of the form:

$$ax + by = n \tag{1}$$

with 2 prerequisites:

1. a, b, and n are integers,

2. we only looked for integer solutions to x and y.

2 Early discoveries: Brute force, looking for patterns, and discovering ideals

2.1 Fixing a, b and n

Initially, we solved equations such as

$$6x + 10y = 8 \tag{2}$$

by trying many different combinations of x and y, and seeing which ones produced 8. Clearly, this could become time intensive when solving a more complex equation. Once we had found values of x and y that produced the correct n, we began to notice trends. Taking a close look at equation (2), we noticed a clear trend to the values of x and y:

x	y
-7	5
-2	2
3	-1
8	-4
13	-7

A pattern appeared; the values of x increased by 5, and the values of y decreased by 3.

2.2 Fixing *just* a and b and observing n

Next, we decided to look exclusively at what values of n are possible when fixing a and b only, and observed the subsequent patterns. We sought to characterize the elements of I in the following equation:

$$I = \{ax + by \ : \ x, y \in \mathbb{Z}\} \tag{3}$$

Equation (3) is known as an ideal. An ideal has the following characteristics,

- $0 \in I$
- if $a, b \in I$, then $a + b$ and $a - b \in I$
- if $a \in I$, $k \in \mathbb{Z}$, then $ka \in I$

These characterisics will aid us in drawing conjectures regarding the solutions of equations such as (3), as well as when trying to find the theme in such solutions.

We analyzed the set that would be formed by solving equation (2) with different values for a and b. Consider the equation:

$$I = \{6x + 10y \ : \ x, y \in \mathbb{Z}\} \tag{4}$$

we discovered that I=2$\mathbb{Z}$, which is all even numbers.

3 The role of the greatest common divisor (=gcd) in solving integer linear equations

3.1 Conjecture from 2.2:

$I = \mathbb{Z}gcd(a, b)$

Which leades to the assumption that, if this conjecture is true,

$ax + by = n$ has a solution *if and only if* n is a multiple of $gcd(a, b)$.

The proof to this conjecture has 2 parts:

1. $gcd(a, b) \in \mathbb{Z}$
2. Every element of I is divisible by the gcd.

3.2 Theorem 1: $ax + by = n$ has a solution *if and only if* $n|gcd(a, b)$

If this theorem holds with $gcd(a, b) > 1$, then division by $gcd(a, b)$ reduces the equation to:

$$a'x + b'y = n' \tag{5}$$

where $gcd(a', b') = 1$. If x_0, y_0 is one solution of, then the general equation is:

$$\forall k \in \mathbb{Z} : x = x_0 + b'k, y = y_0 - a'k \tag{6}$$

proof:
Assume that a and b are non-zero. The integer multiples of gcd(a,b) is equivalent to the set of all integer combinations of a and b.

$$n|gcd(a, b) \iff \exists x, y \in \mathbb{Z} : n = ax + by \tag{7}$$

Suppose that x' and y' is any solution to the equation. The equation becomes:

$$a'x_0 + b'y_0 = n' \tag{8}$$

and

$$a'x' + b'y' = n' \tag{9}$$

Substitute equation (9) into equation (8):

$$a'x_0 + b'y_0 = a'x' + b'y' \tag{10}$$

Rearrange the equation:

$$a'(x' - x_0) = b'(y_0 - y') \tag{11}$$

As we can see from equation (9), $a'|b'(y_0 - y')$. From Euclid's Lemma: $a'|y_0 - y'$, since $gcd(a', b') = 1$. Therefore, $\exists k \in \mathbb{Z}$ such that

$$y_0 - y' = a'k \tag{12}$$

Substituting b' into equation (12) gives us:

$$x' - x_0 = b'k \tag{13}$$

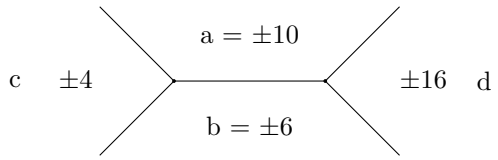
Solving for y' and x' in equation (12) and equation (13) gives us:

$$x' = x_0 + b'k, y' = y_0 - a'k \tag{6}$$

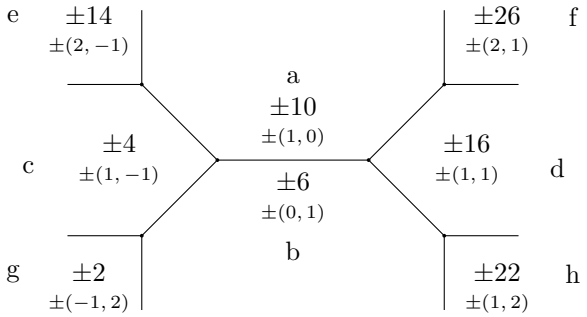
for some $k \in \mathbb{Z}$, which is what we claimed in equation (6).

4 Ideal Visualization Technique: Conway's Topograph

Since equation (3) is an ideal, we can use this fact to more rapidly find the GCD. One method is to use a topograph, as seen below. To use, we start by placing a and b in their respective places on the topograph. One of the characteristics of an ideal is if a and b are in the I, then so is $a + b$ and $a - b$. We see the outcomes of this arithmatic at quadrants c (where we subtract 6 from 10 or -6 from -10) and d (where we add 6 to 10 or -6 to -10).



Adding in the x, y values to the respective outcomes of $a+b$ and $a-b$, we begin to see a trend. When we add $a+b$ (10+6), we obtain 16. In addition, the x, y values of $a+b$ are also added together, giving us the x, y values of $a+b$ (as seen in "d"). We can view this easiest as the addition of two vectors:



We can view this easiest as the addition of two vectors:

$$\begin{pmatrix}1\\0\end{pmatrix} \quad + \begin{pmatrix}0\\1\end{pmatrix} \quad = \begin{pmatrix}1\\1\end{pmatrix}$$

Here, the x, y coordinates of a are being added to the x, y coordinates of b, giving us the x, y coordinates of d. Another example shows us $b+d$:

$$\begin{pmatrix}0\\1\end{pmatrix} \quad + \begin{pmatrix}1\\1\end{pmatrix} \quad = \begin{pmatrix}1\\2\end{pmatrix}$$

4.1 The relationship between topography and matrices

As is initially described in the previous section, it is not an accident that there is a relationship between the values of $a+b$ and the values of $x+y$. In the 2nd topograph of section 4, we can create a 2x2 matrix out of the x, y values of adjacent cells. For example, here is a matrix of cells a and b:

$$\begin{pmatrix}1 & 0\\-1 & 1\end{pmatrix}$$

the determinant of any matrix made by adjacent cells will equal ± 1. Since every operation performed in the topograph amounts to a column operation in the matrix, the determinant will not change, since column operations do not change determinants.

5 Prime factorization

5.1 Conjecture:

For x, y to appear in the topograph from section 4, $\pm x, y$ must be coprime.