5.1: Linear Diophantine Equations

Thinking out loud

Mary went to a park and saw vehicles with 2 wheels and 4 wheels. She counted the wheels. When she came home she told her mom that the vehicles she had seen had a total of 28 wheels. Her mom asked how many vehicles had 2 wheels and how many vehicles had 4 wheels. What was Mary's response?

Diophantine Equation

A Diophantine equation is a polynomial equation with 2 or more integer unknowns.

A Linear Diophantine equation (LDE) is an equation with 2 or more integer unknowns and the integer unknowns are each to at most degree of 1.

Linear Diophantine equation in two variables takes the form of \( ax+by=c \) where \( x, y \in \mathbb{Z} \) and a, b, c are integer constants. x and y are unknown variables.

A Homogeneous Linear Diophantine equation (HLDE) is \( ax+by=0, x, y \in \mathbb{Z} \). Note that \( x=0 \) and \( y=0 \) is a solution, called the trivial solution for this equation.

Example of a homogeneous linear diophantine equation:

\( 5x-3y=0, x, y \in \mathbb{Z} \).
In this case \((x=3), (y=5)\) is a solution as is \((x=6), (y=10)\). Hence \((x=3k), (y=5k), k \in \mathbb{Z}\) represent all the solutions.

Check: \((5(3k)-3(5k)=15k-15k=0)\)

**** NOTE**** In a homogeneous linear diophantine equation, the minute the equation is an addition, one of the variable is required to be negative.

In the case of \((5x+3y=0), (x, y) \in \mathbb{Z}\), \((x=-3k), (y=5k), k \in \mathbb{Z}\) are solutions.

THEOREM: Homogeneous Linear Diophantine Equation

Let \((ax+by=0), (x, y) \in \mathbb{Z}\) be a homogeneous linear Diophantine equation.

If \(\gcd(a, b)=d\), then the complete family of solutions to the above equation is \((x=\frac{b}{d}k, y=-\frac{a}{d}k), k \in \mathbb{Z}\).

Example \((\PageIndex{2})\): Solve the Homogeneous linear Diophantine equation

\((6x+9y=0), (x, y) \in \mathbb{Z}\).

Solution:

Note that GCD of 6 and 9 is 3. Hence the solutions are \((x=\frac{9k}{3}=3k), (y=-\frac{6k}{3}=-2k), k \in \mathbb{Z}\).

Use the following steps to solve a non-homogeneous linear Diophantine equation.

Solve the linear Diophantine Equations: \((ax+by=c), (x, y) \in \mathbb{Z}\).

Use the following steps to solve a non-homogeneous linear Diophantine equation.

Step 1: Determine the GCD of a and b. Let suppose \(\gcd(a, b)=d\).

Step 2: Check that the GCD of a and b is divides c. NOTE: If YES, continue on to step 3. If NO, STOP as there are no solutions.

Step 3: Find a particular solution to \((ax+by=c)\) by first finding \((x_0, y_0)\) such that \((ax+by=d)\). Suppose \((x=\frac{c}{d}x_0)\) and \((y=-\frac{c}{d}y_0)\).

Step 4: Use a change of variables: Let \((u=x-\frac{c}{d}x_0)\) and \((v=y+\frac{c}{d}y_0)\), then we will see that \((au+bv=0)\) (important to check your result).

Step 5: Solve \((au+bv=0)\). That is: \((u=\frac{c}{d} \{d\}m)\) and \((v=\frac{c}{d} \{d\}m)\), \((m \in \mathbb{Z})\).

Step 6: Substitute for \((u)\) and \((v)\). Thus the general solutions are \((x=\frac{c}{d} \{d\}x_0-\frac{c}{d} \{d\}m)\) and \((y=\frac{c}{d} \{d\}y_0+\frac{c}{d} \{d\}m)\), \((m \in \mathbb{Z})\).

Example \((\PageIndex{3})\):

Solve the linear Diophantine Equations: \((5x+3y=4), (x, y) \in \mathbb{Z}\).

UC Davis ChemWiki is licensed under a Creative Commons Attribution-Noncommercial-Share Alike 3.0 United States License.
Solution:
Step 1: Determine the GCD of 5 and 3 (a and b). Since \(\gcd(5, 3)=1\), \(\gcd(5, 3)=1\).
Step 2: Since \(\gcd(5, 3)=1\), we will continue on to Step 3.
Step 3: Find a particular solution to \((5x+3y=4, x, y \in \mathbb{Z})\).
Since \((5+3(-7)=4, x=5)\) and \((y=-7)\) is a particular solution.
Step 4: Let \((u=x-5)\) and \((v=y+7)\). Note: The opposite integer of Step 4, so if it's positive in step 4 it will be negative in step 5 and vice versa.
   Then \((5u+3v=5(x-5)+3(y+7))\)
   \(=5x-25+3y+21\)
   \(=5x+3y-4\)
   \(=4-4\) (because the equation is \((5x+3y=4)\))
   \(=0\).
Step 5: Solve \(5u+3v=0\)
   The general solutions are \((u=-3m)\) and \((v=5m, m \in \mathbb{Z})\).
Step 6: \((x-5=-3m)\) and \((y+7=5m, m \in \mathbb{Z})\).
   Hence the general solutions are \((x=-3m+5, y=5m-7, m \in \mathbb{Z})\).
Example PageIndex{4}:
Solve the linear Diophantine Equations: \((2x+4y=21, x, y \in \mathbb{Z})\).
Solution:
Since \((\gcd(2, 4)=2)\) and \((2)\) does not divide \((21)\), \((2x+4y=21)\) has no solution.
Example PageIndex{5}:
Solve the linear Diophantine Equation \((20x+16y=500, x, y \in \mathbb{Z}_+)\).
Solution
Both \((x, y \geq 0)\).
\(500 = 20(x) + 16(y)\).

Step 1: \((\gcd(20, 16) = 4)\). Since 4 \(\mid\) 500, we expect a solution.

Step 2: A solution is \(4125=20(1)(125)+16(-1)(125)\).
\(500= 20(125)+16(-125)\)
Hence, \(x = 125\) and \(y = -125\) is a solution to \(500 = 20x + 16y\).
**Step 3:** Let \( u = x - 125 \) and \( v = y + 125 \).

Consider that

\[
20u + 16v = 20(x - 125) + 16(y + 125)
\]

\[
= 20x + 16y - (20)(125) + (16)(125)
\]

\[
= 20x + 16y - 500.
\]

Thus, \( 20u + 16v = 0 \).

**Step 4:** In general, the solution to \( ax + by = 0 \) is \( x = bk \) and \( y = -dk \), \( k \in \mathbb{Z} \setminus \{0\} \), \( d = \gcd(a, b) \). Recall, \( \gcd(20, 16) = 4 \).

Thus \( u = 16k/4 = 4k \) and \( v = -20k/4 = -5k \), \( k \in \mathbb{Z} \).

**Step 5:** Replace \( u \) and \( v \).

Consider \( 4k = x - 125 \) and \( -5k = y + 125 \).

Hence, \( x = 4k + 125 \) and \( y = -5k - 125 \).

**Step 6:** Both \( x \) and \( y \geq 0 \). \( x \leq 25 \) and \( y \leq 31 \) since total is 500.

\[
4k + 125 \geq 0, \quad k \geq -125/4, \quad \text{?} \quad k \geq -31.25.
\]

\[
4k + 125 \leq 25, \quad 4k \leq -100, \quad \text{?} \quad k \leq -25.
\]

Thus, the possible solutions are:
Let $k = -25$ then $x = 25, y = 0$.

Let $k = -26$ then $x = 21, y = 5$.

Let $k = -27$ then $x = 17, y = 10$.

Let $k = -28$ then $x = 13, y = 15$.

Let $k = -29$ then $x = 9, y = 20$.

Let $k = -30$ then $x = 5, y = 25$.

Let $k = -31$ then $x = 1, y = 30$.

Thus the options of $(x,y)$ that satisfy the given equation are:

\{ (25,0), (21,5), (17,10), (13,15), (9,20), (5,25), (1,30) \}

PRACTICAL USES

- Cryptography
- Designing different combinations of a variety of elements.