Math 309 **Summer B 2018**
Linear Diophantine Equations **Drew Armstrong**

The handwritten notes don't go into full generality, so I decided to type up this supplement.

For any integers $a, b, c \in \mathbb{Z}$ we want to find **all integer solutions** $x, y \in \mathbb{Z}$ to the following linear equation:

$$ax + by = c. \tag{1}$$

If $a = b = 0$ then we have two very boring cases:

- If $c \neq 0$ then there is no solution.
- If $c = 0$ then all values of $x, y \in \mathbb{Z}$ are solutions.

Furthermore, if exactly one of a, b is zero (say $b = 0$) then equation (1) becomes

$$ax = c,$$

which has a unique solution or no solution, depending on whether a divides c. Having dispensed with these trivial cases, let us suppose that a, b are **both nonzero** and let

$$d := \gcd(a, b)$$

be the greatest common divisor, with $a = da'$ and $b = db'$ for some $a', b' \in \mathbb{Z}$. If equation (1) has a solution in this case then we must have

$$\begin{aligned} c &= ax + by \\ &= da'x + db'y \\ &= d(a'x + b'y), \end{aligned}$$

which implies that d divides c. We conclude the following:

if $d \nmid c$ then equation (1) has **no solution**.

So let us assume from now on that $d|c$, with $c = dc'$ for some $c' \in \mathbb{Z}$. In this case I claim that equation (1) is equivalent to the following **reduced equation**:

$$a'x + b'y = c'. \tag{2}$$

Proof: If $x, y \in \mathbb{Z}$ is a solution to (2) then it is also a solution to (1) because

$$\begin{aligned} a'x + b'y &= c' \\ d(a'x + b'y) &= dc' \\ (da')x + (db')y &= (dc') \\ ax + by &= c. \end{aligned}$$

Conversely, if $x, y \in \mathbb{Z}$ is a solution to (1) then it is also a solution to (2) because

$$\begin{aligned} ax + by &= c \\ (da')x + (db')y &= (dc') \\ \cancel{d}(a'x + b'y) &= \cancel{d}(c') \\ a'x + b'y &= c'. \end{aligned}$$

In the final step we canceled d from both sides, which is allowed because $d \neq 0$. $\square$

Thus we may throw away equation (1) forever and focus our attention on the "reduced" equation (2). Furthermore, I claim that equation (2) splits into two separate problems:

Problem 1. Find One Specific Solution. Let $x', y' \in \mathbb{Z}$ be one specific solution:

$$a'x' + b'y' = c'.$$

Problem 2. Find the General Homogeneous Solution. Let $x_0, y_0 \in \mathbb{Z}$ be the general solution of the associated **homogeneous** equation:

$$a'x_0 + b'y_0 = 0. \tag{3}$$

Then I claim that $(x, y) = (x' + x_0, y' + y_0)$ is the general solution of (2).

Proof: Let $x, y \in \mathbb{Z}$ and $x', y' \in \mathbb{Z}$ be any two solutions to (2). Then we have

$$a'(x - x') + b'(y - y') = (a'x + b'y) - (a'x' + b'y') = c' - c' = 0,$$

and it follows that $(x - x', y - y') = (x_0, y_0)$ is a solution of the homogeneous equation (3), hence (x, y) has the form $(x' + x_0, y' + y_0)$. Conversely, suppose that $x', y' \in \mathbb{Z}$ is a particular solution and $x_0, y_0 \in \mathbb{Z}$ is a homogeneous solution. Then $(x, y) = (x' + x_0, y' + y_0)$ is a solution of (2) because

$$a'(x' + x_0) + b'(y' + y_0) = (a'x' + b'y') + (a'x_0 + b'y_0) = c' + 0 = c'.$$

$\square$

It only remains so solve the Problems 1 and 2. Let's begin with Problem 1.

Solution to Problem 1. By applying the Extended Euclidean Algorithm, we can find specific integers $\alpha, \beta \in \mathbb{Z}$ such that

$$a\alpha + b\beta = \gcd(a, b) = d.$$

And then since $a = da'$ and $b = db'$ we have

$$\begin{aligned} a\alpha + b\beta &= d \\ (da')\alpha + (db')\beta &= d \\ \cancel{d}(a'\alpha + b'\beta) &= \cancel{d} \\ a'\alpha + b'\beta &= 1. \end{aligned}$$

It follows from this that

$$\begin{aligned} a'\alpha + b'\beta &= 1 \\ c'(a'\alpha + b'\beta) &= c'(1) \\ a'(c'\alpha) + b'(c'\beta) &= c', \end{aligned}$$

and thus have found our desired specific solution:

$$(x', y') = (c'\alpha, c'\beta).$$

$\square$

Solution to Problem 2. From the solution to Problem 1, we saw that there exist specific integers $\alpha, \beta \in \mathbb{Z}$ such that

$$a'\alpha + b'\beta = 1.$$

It follows from this equation that

$$\gcd(a', b') = 1.$$

Indeed, suppose that δ is any common divisor of a' and b'; let's say $a' = \delta a''$ and $b' = \delta b''$ for some integers $a'', b'' \in \mathbb{Z}$. Then we must have

$$1 = a'\alpha + b'\beta = (da'')\alpha + (db'')\beta = d(a''\alpha + b''\beta),$$

from which it follows that $\delta \leq 1$. Since every common divisor of a', b' satisfies $\delta \leq 1$ is must be that the greatest common divisor satisfies $\gcd(a', b') \leq 1$, and hence $\gcd(a', b') = 1$.

Now I claim that the general solution $x_0, y_0 \in \mathbb{Z}$ of the homogeneous equation (3) is given by

$$(x_0, y_0) = (b'k, -a'k) \text{ for some } k \in \mathbb{Z}.$$

Proof: Let $x_0, y_0 \in \mathbb{Z}$ be any solution of equation (3):

$$a'x_0 + b'y_0 = 0.$$

It follows from this that

$$a'x_0 = -b'y_0,$$

which implies that $a'|(b'y_0)$ and $b'|(a'x_0)$. Then since $\gcd(a', b') = 1$, Euclid's Lemma[1] tells us that $a'|y_0$ and $b'|x_0$. Specifically, let us say that

$$x_0 = b'k \quad \text{and} \quad y_0 = a'\ell \qquad \text{for some } k, \ell \in \mathbb{Z}.$$

Finally, we have

$$\begin{aligned} a'x_0 &= -b'y_0 \\ a'b'k &= -b'a'\ell \\ (a'b')(k + \ell) &= 0. \end{aligned}$$

Since a', b' are both nonzero we have $a'b' \neq 0$ and hence

$$\begin{aligned} (k + \ell) &= 0 \\ \ell &= -k. \end{aligned}$$

It follows that

$$(x_0, y_0) = (b'k, a'\ell) = (b'k, -a'k) \text{ for some } k \in \mathbb{Z},$$

as desired. $\square$

Putting everything together, we obtain the following general solution.

Theorem. Let $a, b, c \in \mathbb{Z}$ with a, b both nonzero. Let $d = \gcd(a, b)$ with $a = da'$ and $b = db'$, and let us also suppose that $c = dc'$ for some $c' \in \mathbb{Z}$. If $\alpha, \beta \in \mathbb{Z}$ are any specific integers satisfying $a'\alpha + b'\beta = 1$, then the complete solution of the linear Diophantine equation

(1) $$ax + by = c$$

is given by

$$(x, y) = (x' + x_0, y' + y_0) = (c'\alpha + b'k, c'\beta - a'k) \quad \text{for all } k \in \mathbb{Z}.$$

Time for an example.

[1] See the Homework.

Worked Example. Let us consider the equation

$$385x + 84y = 21.$$

So in this case we have

$$a = 385, \qquad b = 84 \qquad \text{and} \qquad c = 21.$$

In order to compute the gcd of 385 and 84 we use the classical Euclidean Algorithm:

$$\begin{array}{rcrcr} 385 & = & 4 \cdot 84 & + & 49 \\ 84 & = & 1 \cdot 49 & + & 35 \\ 49 & = & 1 \cdot 35 & + & 14 \\ 35 & = & 2 \cdot 14 & + & \boxed{7} \\ 14 & = & 2 \cdot 7 & + & 0 \end{array}$$

We conclude that

$$d = \gcd(a, b) = \gcd(385, 84) = 7,$$

and hence that

$$a' = a/d = 55, \qquad b' = b/d = 12 \qquad \text{and} \qquad c' = c/d = 3.$$

Thus the reduced equation is

$$55x + 12y = 3,$$

which has exactly the same solution as the original equation. We are guaranteed that $\gcd(a', b') = \gcd(55, 12) = 1$, and our final goal is to find some particular integers $\alpha, \beta \in \mathbb{Z}$ such that

$$55\alpha + 12\beta = 1.$$

To do this we will use the Extended Euclidean Algorithm. That is, we will consider the set of all triples $(x, y, z) \in \mathbb{Z}^3$ satisfying $55x + 12y = z$. Then we will begin with the easy triples $(1, 0, 55)$ and $(0, 1, 12)$ and combine them using linear combinations, until we reach a triple of the form $(\alpha, \beta, 1)$:

x	y	z	
1	0	55	(Row 1)
0	1	12	(Row 2)
1	-4	7	(Row 3) = (Row 1) $-$ 4 $\cdot$ (Row 2)
-1	5	5	(Row 4) = (Row 2) $-$ 1 $\cdot$ (Row 3)
2	-9	2	(Row 5) = (Row 3) $-$ 1 $\cdot$ (Row 4)
-5	23	1	(Row 6) = (Row 4) $-$ 1 $\cdot$ (Row 5)

The final row tells us that

$$\alpha = -5 \qquad \text{and} \qquad \beta = 23$$

is one possible solution. Putting everything together, we conclude that the general solution to the original equation is

$$\begin{aligned} (x, y) &= (c'\alpha + b'k, c'\beta - a'k) \quad \text{for all } k \in \mathbb{Z} \\ &= (3 \cdot (-5) + 12k, 3 \cdot 23 - 55k) \quad \text{for all } k \in \mathbb{Z} \\ &= (-15 + 12k, 69 - 55k) \quad \text{for all } k \in \mathbb{Z} \end{aligned}$$

Great, but isn't there a faster way?

The Faster Way. In order to solve the linear Diophantine equation

$$385x + 84y = 21,$$

we will apply the Extended Euclidean Algorithm right from the start. That is, we will consider the set of all triples $(x, y, z) \in \mathbb{Z}^3$ that satisfy the equation. Then we will begin with the easy triples $(1, 0, 385)$ and $(0, 1, 84)$ and proceed with the steps of the Euclidean Algorithm until we hit a triple of the form $(x, y, 0)$:

x	y	z	
1	0	385	(Row 1)
0	1	84	(Row 2)
1	-4	49	(Row 3) = (Row 1) $-$ 4 $\cdot$ (Row 2)
-1	5	35	(Row 4) = (Row 2) $-$ 1 $\cdot$ (Row 3)
2	-9	14	(Row 5) = (Row 3) $-$ 1 $\cdot$ (Row 4)
-5	23	7	(Row 6) = (Row 4) $-$ 1 $\cdot$ (Row 5)
12	-55	0	(Row 7) = (Row 5) $-$ 2 $\cdot$ (Row 6)

Row 7 tells us that the associated homogeneous equation has complete solution

$$384(12k) + 84(-55k) = 0 \qquad \text{for all } k \in \mathbb{Z},$$

and Row 6 tells us one particular solution:

$$\begin{aligned} 385(-5) + 84(23) &= 7 \\ 385(-5 \cdot 3) + 84(23 \cdot 3) &= 7 \cdot 3 \\ 385(-15) + 84(69) &= 21. \end{aligned}$$

Adding these together gives the complete solution of the original equation:

$$384(-15 + 12k) + 84(69 - 55k) = 21 \qquad \text{for all } k \in \mathbb{Z}.$$

Picture. The equation $385x + 84y = 21$ defines a **line** in the real x, y-plane. The whole number solutions which we have calculated,

$$(x, y) = (-15 + 12k, 69 - 55k) \qquad \text{for all } k \in \mathbb{Z},$$

are just the points on this line that have **integer coordinates**. There are infinitely many.