Diophantine equations

Manuela Girotti

MATH 250 Fundamentals of Math

These notes are based on M. Girotti's personal notes from the course "Precorso" given at Università degli Studi di Milano in far 2005.

We will first review some known results on integer numbers and the Division Theorem, which will prepare us to learn how to solve a Diophantine equation.

1 Integers and the Division Theorem

We denote by $\mathbb{Z}$ the set of all integers:

$$\mathbb{Z} := \{0, +1, -1, +2, -2, \dots\}$$

Definition 1. Given two integers $a, b \in \mathbb{Z}$, $a, b \neq 0$, we say that b divides a or that b is a **divisor** of a if

$$\exists\ k \in \mathbb{Z} \qquad \text{such that} \qquad a = b \cdot k\ .$$

In this case, we can use the symbol $b|a$.

An easy observation is the following: given $a, b \in \mathbb{Z}$, if a divides b and b divides a, then $a = b$ or $a = -b$:

$$a|b\ \wedge\ b|a \qquad \Rightarrow \qquad a = b\ \vee\ a = -b\ .$$

Indeed, if $a|b$, then $b = a \cdot k$ for some $k \in \mathbb{Z}$; similarly, if $b|a$, then $a = b \cdot k'$ for some $k' \in \mathbb{Z}$. Then, we have

$$a = b \cdot k' = (a \cdot k) \cdot q' = akk' \qquad \text{i.e.} \qquad kk' = 1 \ \ (\text{since } a \neq 0)$$

and the only integers whose product is equal to one are 1 or -1.

Theorem 2 (**Division Theorem**). *Given two integers $a, b \in \mathbb{Z}$ and $b > 0$, there exist unique integers $q \in \mathbb{Z}$ (the "quotient") and $r \in \mathbb{Z}$ (the "remainder") such that*

$$a = bq + r\ , \qquad \textit{and} \qquad 0 \leq r < b\ .$$

Proof. See the proof in Section 5.3 of our textbook. □

Note that we can relax the assumption that $b > 0$, by just requiring $b \neq 0$ and $0 \leq r < |b|$.

Examples.

- given 34 and 7, then $34 = 7 \cdot 4 + 6$
- given -34 and 7, then $-34 = 7 \cdot (-5) + 1$
- given 34 and -7, then $34 = (-7) \cdot (-4) + 6$
- given -34 and -7, then $-34 = (-7) \cdot 5 + 1$

Definition 3. Given $a, b \in \mathbb{Z}$, not both zero, the **greatest common divisor** d of a and b (denoted $\gcd(a, b)$) is the largest positive integer such that

1) d divides both a and b: $d|a \ \wedge d|b$

2) any other number c that divides both a and b, c divides d as well: if $c|a$ and $c|b$, then $c|d$.

If either a or b is zero, then we set $\gcd(a, 0) = |a|$ (similarly $\gcd(0, b) = |b|$).

The fundamental result about the greatest common divisor is the following:

Theorem 4. *Let $a, b \in \mathbb{Z}$, not both zero. Then, the greatest common divisor* $\gcd(a, b)$ *exists and it is unique.*

The proof of Theorem 4 is constructive and it relies on the so called

Euclidean Algorithm

Step 1. Arrange a, b so that $a \geq b$

Step 2. Use the Division Theorem to find $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < |b|$

Step 3. If $r = 0$, we stop. And we get $\gcd(a, b) = \gcd(b, 0) = |b|$

Step 4. If $r \neq 0$, we swap (a, b) with (b, r) and return to Step 1.

That is, we repeatedly apply the Division Theorem 2 to get

$$\begin{aligned}
a &= bq^{(1)} + r^{(1)} && \text{where } q^{(1)}, r^{(1)} \in \mathbb{Z}\ , 0 \leq r^{(1)} < b \\
b &= r^{(1)}q^{(2)} + r^{(2)} && \text{where } q^{(2)}, r^{(2)} \in \mathbb{Z}\ , 0 \leq r^{(2)} < r^{(1)} \\
r^{(1)} &= r^{(2)}q^{(3)} + r^{(3)} && \text{where } q^{(3)}, r^{(3)} \in \mathbb{Z}\ , 0 \leq r^{(3)} < r^{(2)} \\
r^{(2)} &= \dots
\end{aligned}$$

The algorithm will eventually stop, say after n steps, because each new remainder is strictly smaller than the previous one:

$$\begin{aligned}
&\dots \\
r^{(n-2)} &= r^{(n-1)}q^{(n)} + r^{(n)} \\
r^{(n-1)} &= r^{(n)}q^{(n+1)} + 0
\end{aligned}$$

Then, the great common divisor is

$$r^{(n)} = d = \gcd(a, b)\ .$$

This iterative method that relies on the simple fact that

Lemma 5. *If d is the greatest common divisor of a and b and $a = bq + r$, then d is also the greatest common divisor of b and r.*

Proof. Let $d = \gcd(a, b)$, then we know that $d|a$ and $d|b$. This implies that d divides also any linear combination of a and b, in particular $d|a - bq$, i.e. $d|r$. This shows that d is a common divisor of b and r.

It remains to prove that d is the greatest common divisor of b and r. Let $w \in \mathbb{Z}_+$ such that $w|b$ and $w|r$, then w divides any linear combination of b and r, in particular $w|bq + r$, i.e. $w|a$. This implies that $w|d$, since $d = \gcd(a, b)$. □

Proof of Theorem 4. The existence follows from Lemma 5 and the Euclidean Algorithm. The proof of uniqueness is left as an exercise. □

Example. Let $a = 9180$ and $b = 1122$.

$$\begin{aligned} 9180 &= 1122 \cdot 8 + 204 \\ 1122 &= 204 \cdot 5 + 102 \\ 204 &= 102 \cdot 2 + 0 \end{aligned}$$

Thus, $\gcd(9180, 1122) = 102$.

Proposition 6. *Given two positive integers $a, b \in \mathbb{Z}$, not both zero, let d be the great common divisor of a and b: $d = \gcd(a, b)$. Then, there exists $x, y \in \mathbb{Z}$ such that*

$$d = ax + by \ .$$

Equivalently, d is a linear combination of a and b with integer coefficients.

The proof again lies on the Euclidean Algorithm and it is constructive: by following all the steps of the proof we can find the two integers $x, y \in \mathbb{Z}$ that solve the equation $d = ax + by$.

Proof. We know that in order to find the great common divisor d of a and b, we need to apply the Euclidean Algorithm of successive divisions:

$$\begin{aligned} a &= bq + r \\ b &= rq' + r' \\ r &= r'q'' + r'' \\ r' &= \dots \end{aligned}$$

The algorithm will eventually stop, say after n steps:

$$\begin{aligned} &\dots \\ r^{(n-2)} &= r^{(n-1)}q^{(n)} + r^{(n)} \\ r^{(n-1)} &= r^{(n)}q^{(n+1)} + 0 \end{aligned}$$

where we recover the great common divisor

$$r^{(n)} = d = \gcd(a, b) \ .$$

We now rewrite each equations above by highlighting the remainder, and we substitute in the subsequent equations:

$$
\begin{aligned}
r &= a - bq\\
r' &= b - rq' = b - \underbrace{(a-bq)}_{r}q' = a(-q') + b\left(1+qq'\right)\\
r'' &= r - r'q'' = \underbrace{(a-bq)}_{r} - \underbrace{\left[b-(a-bq)q'\right]}_{r'}q'' = a\left(1+q'q''\right) + b\left(-q-q''-qq'q''\right)\\
&\vdots\\
r^{(n)} &= r^{(n-2)} - r^{(n-1)}q^{(n)} = \ldots = a\big(\text{some combination of } q, q', \ldots\big) + b\big(\text{some other combination of } q, q', \ldots\big)
\end{aligned}
$$

We can notice that each remainder $r^{(k)}$ can be expressed as a linear combination of a and b with integer coefficients; in particular, we will have

$$d = r^{(n)} = a\underbrace{\left(\text{some combination of } q, q', \ldots\right)}_{=:x} + b\underbrace{\left(\text{some other combination of } q, q', \ldots\right)}_{=:y}$$

□

Example. Let $a = 204$ and $b = 99$. Then, $\gcd(204, 99) = 3$: indeed,

$$
\begin{aligned}
204 &= 99 \cdot 2 + 6\\
99 &= 6 \cdot 16 + 3\\
6 &= 3 \cdot 2 + 0
\end{aligned}
$$

therefore 3 is the greatest common divisor of 204 and 99.

Now we rearrange the equations to find $x, y \in \mathbb{Z}$ such that

$$3 = 204x + 99y\ .$$

We start with the first equation

$$6 = 204 + 99 \cdot (-2)$$

and we substitute in the second equation, and we expand:

$$
\begin{aligned}
3 &= 99 - 6 \cdot 16\\
&= 99 - \underbrace{\left[204 + 99 \cdot (-2)\right]}_{=6} \cdot 16\\
&= 204 \cdot (-16) + 99 \cdot [1 + 2 \cdot 16]\\
&= 204 \cdot \underbrace{(-16)}_{=:x} + 99 \cdot \underbrace{33}_{=:y}
\end{aligned}
$$

2 Diophantine Equations

Next, let's consider a more general case: let $a, b, c \in \mathbb{Z}$, with $a, b \neq 0$. We are now looking for integer solutions for the equation

$$ax + by = c \ .$$

This type of equation is called **(linear) Diophantine equation**.

Changing perspective, we can reformulate the problem in a geometrical way: consider the equation

$$c = ax + by \ , \quad \text{or equivalently} \quad y = -\frac{a}{b}x + \frac{c}{b} \ .$$

This is the equation of a line on the cartesian plane and we are wondering whether the line crosses points whose coordinates are integers (see Figure 1).

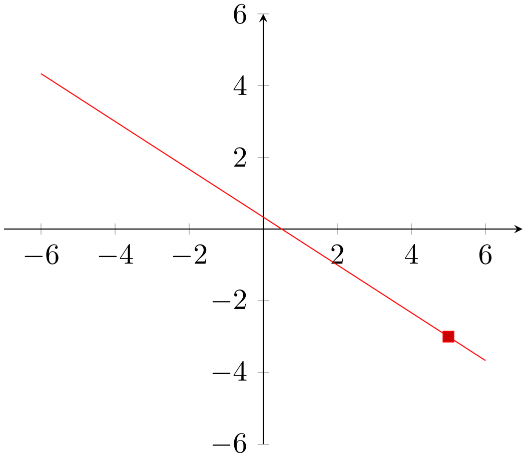

Figure 1: An example of a line in the cartesian plane $y = -\frac{2}{3}x + \frac{1}{3}$, with one integer solution $(5, -3)$.

Example. Let's first look at some examples where we can easily find a solution.

- $6x + 5y = 3$ – by trial and error, we can guess a solution: $x = 3$, $y = -3$
- every time the number c happens to be $\gcd(a, b)$, we have a procedure to find a solution (Proposition 6).
- $24x + 16y = 7$ – this equation cannot have a solution because if we divide both sides by the $\gcd(24, 16) = 8$, we find

  $$3x + 2y = \frac{7}{8} \ ;$$

  clearly, the sum of integers cannot add up to a fraction.

From the last example, it is clear that a necessary condition for a Diophantine equation to have a solution is that the number c is divisible by $\gcd(a, b)$.

Proposition 7. *Given a Diophantine equation $ax + by = c$, if it admits a solution, then c is divisible by* $\gcd(a, b)$.

Proof. Given

$$a\bar{x} + b\bar{y} = c \ ,$$

with $(\bar{x}, \bar{y}) \in \mathbb{Z} \times \mathbb{Z}$ a solution to the Diophantine equation, and knowing that $d = \gcd(a, b)$, we can rewrite the numbers a and b as

$$a = a_0 \cdot d \qquad \text{aand} \qquad b = b_0 \cdot d$$

for some $a_0, b_0 \in \mathbb{Z}$ (note that a_0, b_0 are coprimes). Therefore, the Diophantine equation becomes

$$a_0 d\bar{x} + b_0 d\bar{y} = c \qquad \text{i.e.} \qquad d(a_0\bar{x} + b_0\bar{y}) = c \ .$$

The left hand side can be clearly divided by d and, since we have an equality, this implies that the right hand side must also be divisible by d. □

It turns out that c being divisible by $\gcd(a, b)$ is also a sufficient condition for having a solution to the equation.

Proposition 8. *Given a Diophantine equation $ax + by = c$, if c is divisible by $\gcd(a, b)$, then it admits a solution.*

Proof. The proof will be constructive.

Let $d = \gcd(a, b)$. Since c is divisible by d, we can write $c = c_0 \cdot d$, for some $c_0 \in \mathbb{Z}$. As in the proof of Proposition 7, we can always write a and b as $a = a_0 \cdot d$ and $b = b_0 \cdot d$.

Then, the Diophantine equation becomes

$$ax + by = c_0 d \ .$$

In Proposition 6, we proved (constructively) that there exists a solution to the equation $ax+by = d$: let $(\bar{x}, \bar{y}) \in \mathbb{Z}$ be such a solution. Then,

$$(c_0\bar{x}, c_0\bar{y})$$

is a solution to the Diophantine equation $ax + by = c$. Indeed,

$$a \cdot c_0\bar{x} + b \cdot c_0\bar{y} = c_0 \underbrace{(a\bar{x} + b\bar{y})}_{=d} = c_0 d = c$$

□

In conclusion, we just proved the following theorem.

Theorem 9 **(Existence of a solution).** *Given $a, b, c \in \mathbb{Z}$, with $a, b \neq 0$. The Diophantine equation*

$$ax + by = c$$

has a solution if and only if c is divisible by $\gcd(a, b)$.

So far, we have no information on how many pairs of solutions $(\bar{x}, \bar{y})$ exist: one? a handful? several? The next theorem will answer this question.

Theorem 10 (Set of solutions). *Given $a, b, c \in \mathbb{Z}$, with $a, b \neq 0$. Consider the Diophantine equation*

$$ax + by = c$$

and let $(\bar{x}, \bar{y})$ be a solution.

Then, all solutions to the equation are of the form

$$(\bar{x} + b_0 n\ ,\ \bar{y} - a_0 n) \qquad \textit{with } n \in \mathbb{Z}\ ,$$

where $a_0 = \frac{a}{\gcd(a,b)}$ and $b_0 = \frac{b}{\gcd(a,b)}$.

Proof. We already have one solution $(\bar{x}, \bar{y})$. We now need to prove two things:

1. $(\bar{x} + b_0 n, \bar{y} - a_0 n)$ is another solution, for any choice of $n \in \mathbb{Z}$
2. any other solution $(\tilde{x}, \tilde{y})$ can be written as $(\bar{x} + b_0 m, \bar{y} - a_0 m)$ for some $m \in \mathbb{Z}$

The first point is easy to prove: we plug the pair $(\bar{x}+b_0 n, \bar{y}-a_0 n)$ into the equation and expand.

$$\begin{aligned} a(\bar{x} + b_0 n) + b(\bar{y} - a_0 n) &= \underbrace{a\bar{x} + b\bar{y}}_{=c} + ab_0 n - ba_0 n \\ &= c + a\frac{b}{\cancel{\gcd(a,b)}}n - b\frac{a}{\cancel{\gcd(a,b)}}n \\ &= c \end{aligned}$$

Let's assume now we have found another solution $(\tilde{x}, \tilde{y})$:

$$a\tilde{x} + b\tilde{y} = c\ ;$$

but also

$$a\bar{x} + b\bar{y} = c\ .$$

Putting the two equations together we have

$$a\tilde{x} + b\tilde{y} = a\bar{x} + b\bar{y} \qquad \text{i.e.} \qquad a(\tilde{x} - \bar{x}) = -b(\tilde{y} - \bar{y})$$

Recall that $d = \gcd(a, b)$ $(\neq 0)$:

$$a_0 d(\tilde{x} - \bar{x}) = -b_0 d(\tilde{y} - \bar{y}) \qquad \text{i.e.} \qquad a_0(\tilde{x} - \bar{x}) = b_0(\bar{y} - \tilde{y})\ .$$

The last equality implies that a_0 divides the quantity $b_0(\tilde{y} - \bar{y})$ (indeed, it obviously divides the left hand side); on the other hand, b_0 cannot be divisible by a_0 because a_0 and b_0 are coprimes (i.e. only the number 1 divides both of them). Necessarily, we have that a_0 divides $\tilde{y} - \bar{y}$, meaning that there exists an integer $m \in \mathbb{Z}$ such that $\bar{y} - \tilde{y} = a_0 m$, i.e.

$$\tilde{y} = \bar{y} - a_0 m\ .$$

We then substitute back into the equation:

$$\begin{aligned} a_0(\tilde{x} - \bar{x}) &= b_0(\bar{y} - \tilde{y}) \\ &= b_0\left[\bar{y} - (\bar{y} - a_0 m)\right] \\ &= b_0 a_0 m \end{aligned}$$

Simplifying a_0, we get

$$\tilde{x} - \bar{x} = b_0 m \qquad \text{i.e.} \qquad \tilde{x} = \bar{x} + b_0 m\ .$$

□

Example. Find all the solutions to the following Diophantine equation:

$$207x + 86y = 3$$

We start by looking for the $\gcd(207, 86)$ using the Euclidean algorithm:

$$\begin{aligned} 207 &= 86 \cdot 2 + 35 \\ 86 &= 35 \cdot 2 + 16 \\ 35 &= 16 \cdot 2 + 3 \\ 16 &= 3 \cdot 5 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

therefore 1 is the greatest common divisor of 207 and 86 (these numbers are coprimes):

$$207 = \underbrace{207}_{a_0} \cdot 1 \qquad 86 = \underbrace{86}_{b_0} \cdot 1$$

Clearly, 1 divides 3,

$$3 = \underbrace{3}_{c_0} \cdot 1 \ ,$$

therefore the equation admits solutions.

We solve the equation

$$207x + 86y = 1$$

to find one solution, as we did in a previous example:

$$35 = 207 + 86 \cdot (-2)$$

$$16 = 86 - 35 \cdot 2 = 86 - \underbrace{[207 + 86 \cdot (-2)]}_{=35} \cdot 2 = 207 \cdot (-2) + 86 \cdot 5$$

$$3 = 35 - 16 \cdot 2 = \underbrace{[207 + 86 \cdot (-2)]}_{35} - \underbrace{(207 \cdot (-2) + 86 \cdot 5)}_{=16} \cdot 2 = 207 \cdot 5 + 86 \cdot (-12)$$

$$1 = 16 - 3 \cdot 5 = \underbrace{(207 \cdot (-2) + 86 \cdot 5)}_{=16} - \underbrace{(207 \cdot 5 + 86 \cdot (-12))}_{=3} \cdot 5 = 207 \cdot \underbrace{(-27)}_{=:\bar{x}} + 86 \cdot \underbrace{65}_{=:\bar{y}}$$

Finally, the solution to the original equation can be found by multiplying $\bar{x}, \bar{y}$ by c_0 and adding/-subtracting multiples of a_0 and b_0:

$$\left((-27) \cdot \underbrace{3}_{c_0} + \underbrace{86}_{b_0} n \ , \ 65 \cdot \underbrace{3}_{c_0} - \underbrace{207}_{a_0} \cdot n \right) = (-81 + 86n \ , \ 195 - 207n) \ , \quad n \in \mathbb{Z} \ .$$

As a last remark, we can notice that since the Diophantine equation is linear, it is not surprising that the set of solutions has the following expression:

$$\underbrace{(\bar{x} \ , \ \bar{y})}_{\text{particular solution}} \qquad + \qquad \underbrace{(b_0 n \ , \ -a_0 n)}_{\text{homogeneous solutions}}$$

the pair $(\bar{x}, \bar{y})$ is one particular solution to the equation $ax + by = c$, while the pair $(b_0 n, -a_0 n)$ (for any $n \in \mathbb{Z}$ solves the associate homogeneous equation $ax + by = 0$.

Problems.

- A rabbit can make long jumps 8 metres in length, or short jumps 3 metres in length. A carrot is lying 10 metres away. Is there a sequence of jumps that will allow the rabbit to land on the carrot (and eat it)?

- The owner of a shoe store can buy shoes from his supplier in bundles of 14 or 35, and can sell them in the same quantities. Is there a way to buy and sell bundles so that exactly 4 shoes remain in the store at the end of the day?

- Sam needs 2.15$ to buy a large coffee. She only has 25-cent and 10-cent coins, and the cashier insists that she pays with exact change. Is there a combination of these coins that will total 2.15$?