MEM204-Number Theory

12th virtual lecture

Giorgos Kapetanakis

Spring semester 2019-20 - 13/05/2020

University of Crete

Diophantine Equations

Introduction

Let $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ be a polynomial of n variables with integer coefficients. An equation of the form

$$f(x_1, \ldots, x_n) = 0$$

is called a Diophantine equation. They are named after Diophantus of Alexandria, who extensively studied such equations.

In principle, we are interested in whether one such equation has integer solutions (i.e. $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ that satisfy the equation) or not and, in the former case, identify them.

A historical note

In 1900, David Hilbert conjectured the existence of an algorithm that would solve any Diophantine equation. This conjecture is known as Hilbert's 10th problem.

It would take 70 years for mathematicians to prove Hilbert wrong. Namely, in 1970, Yuri Matiyasevich, in his doctoral thesis proved that the conjecture is false. Amid the cold war, the Soviet mathematician, proudly acknowledged that his proof relied on previous works of the American mathematicians Julia Robinson, Martin Davis and Hilary Putnam.

The coresponding theorem is known as the MRDP theorem or Matiyasevich's theorem.

An example

We will identify the integer and rational solutions of

$$2x^3 + xy - 7 = 0.$$

Clearly, $x \neq 0$, hence the above can be rewritten as

$$y = \frac{-2x^3 + 7}{x}.$$

Hence, the rational solutions are of the form $(x, (-2x^3 + 7)/x)$, where $x \in \mathbb{Q} \setminus \{0\}$. It follows that the integer solutions are those where $x \in \mathbb{Z} \setminus \{0\}$ and $x \mid (-2x^3 + 7)$. The latter is true if and only if $x \mid 7$.

It follows that the integer solutions are $(1, 5)$, $(-1, -9)$, $(7, -97)$ and $(-7, -99)$.

Another example

We will now study the integer solutions of the equation

$$15x^2 - 7y^2 = 9.$$

Let (x, y) be an integer solution of the above. Then

$$-7y^2 \equiv 9 \pmod{5} \Rightarrow y^2 \equiv 3 \pmod{5}.$$

However, the latter is impossible, since $\left(\frac{3}{5}\right) = -1$. It follows that there are no integer solutions of this equation.

Linear Diophantine Equations

An existence criterion

A linear Diophantine equation is an equation of the form $f(x_1, \dots, x_n) = 0$, where $f \in \mathbb{Z}[x_1, \dots, x_n]$ and $\deg(f) = 1$. The following criterion fully characterizes the existence of integer solutions of such equations.

Proposition

Let $a_1, \dots, a_n, b \in \mathbb{Z}$, $a_i \neq 0$ for $i = 1, \dots, n$. If $d = (a_1, \dots, a_n)$, then the equation

$$a_1x_1 + \cdots + a_nx_n = b$$

has an integer solution if and only if $d \mid b$.

Proof

For every i, $d \mid a_i$, hence there exists some c_i, such that $a_i = dc_i$. Now, assume that the equation has an integer solution $(x_1, \ldots, x_n)$. Then

$$a_1x_1 + \cdots + a_nx_n = b \;\Rightarrow\; d(c_1x_1 + \cdots + c_nx_n) = b,$$

that is $d \mid b$.

Conversely, assume that $d \mid b$. Then $b = dc$ for some c. Further, there exist $c_1, \ldots, c_n$, such that $d = c_1a_1 + \cdots + c_na_n$. By multiplying both sides by c, we get

$$b = a_1x_1 + \cdots + a_nx_n,$$

where $x_i = c_ic$. The result follows.

Two variables

Proposition

Let $a, b, c \in \mathbb{Z}$, $a, b \neq 0$. If (x_0, y_0) is an integer solution of

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

and $d = (a, b)$, then all the solutions of (1) are given by the relations

$$x = x_0 + \frac{b}{d}t,\ y = y_0 - \frac{a}{d}t,\ t \in \mathbb{Z}.$$

Proof

Since $d = (a, b)$, there exist a', b', such that $a = da'$ and $b = db'$ and $(a', b') = 1$. First, we will show that

$$x = x_0 + b't,\ y = y_0 - a't,\ t \in \mathbb{Z}$$

are solutions of (1). Indeed, we have that

$$ax+by = a(x_0+b't)+b(y_0-a't) = ax_0+by_0+t(ab'-ba') = c,$$

since $ab' = ba'$.

Proof

Now, let (x', y') be an integer solution of (1). Then

$$ax_0 + by_0 = c = ax' + by' \;\Rightarrow\; a(x_0 - x') = b(y' - y_0),$$

that is,

$$a'(x_0 - x') = b'(y' - y_0).$$

Hence, $a' \mid b'(y' - y_0) \overset{(a',b')=1}{\Longrightarrow} a' \mid y' - y_0$. It follows that $y' = y_0 + a't$ and $x' = x_0 - b't$, for some t.

A method for two variables

From the last proposition, we get that, in order to completely solve a linear Diophantine equation, it suffices to find a special solution and from this build the whole set of solutions. Let us now demonstrate that method with an example.

An example

Example

Find all the integer solutions of

$$221x + 340y = 51.$$

An example

First, we employ the Euclidean algorithm and (from its first part) we get $(221, 340) = 17$. Since $17 \mid 51$, we know that the equation has integer solutions.

Next, from the second part of the Euclidean algorithm, we find that

$$17 = 2 \cdot 340 - 3 \cdot 221.$$

We multiply the above equation by 3 (because $51/17 = 3$) and get:

$$51 = 221(-9) + 340 \cdot 6,$$

in other words, $(-9, 6)$ is a solution. It follows that all the solutions are

$$x = -9 + 20t,\ y = 6 - 13t,\ t \in \mathbb{Z}.$$

Multiple variables

We conclude this lecture with an example that demonstrates how the two-variable method can be generalized to more than two variables. Our example has three variables, but its method can be easily extended to any number of variables.

Example

Find all the integer solutions of

$$6x + 4y + 8z = 2.$$

Multiple variables

First, notice that $(6, 4, 8) = 2 \mid 2$, hence the equation has integer solutions. Then, set $w = 3x + 2y$ (in general, we take the co-prime parts of the coefficients of x and y, so, here, we have $(6, 4) = 2$ and we take $3 = 6/2$ and $2 = 4/2$ respectively). Now, the original equation becomes

$$2w + 8z = 2.$$

By using the method for two-variable linear Diophantine equations described earlier, we find that all the solutions of the above are given by

$$w = 5 + 4t,\ z = -1 - t,\ t \in \mathbb{Z}.$$

Multiple variables

Now, it remains to solve

$$3x + 2y = 5 + 4t.$$

Again, the two-variable method yields the solutions

$$x = (5 + 4t) + 2s,\ y = -(5 + 4t) - 3s,\ s \in \mathbb{Z}.$$

It follows that the whole set of solutions of the original equation are given by

$$x = 5 + 4t + 2s,\ y = -5 - 4t - 3s,\ z = -1 - t,\ s, t \in \mathbb{Z}.$$

Stay safe!