April 3–Diophantine equations

Good news, everyone! We are starting Diophantine equations, which are the type of problems that Ximera can actually check. We will pause to give people a chance to solve the problem themselves.

Definition 1. A *Diophantine equation* is any equation in one or more variables to be solved in the integers.

Linear Diophantine equations

Definition 2. Let $a_1, a_2, \ldots, a_n, b \in \mathbb{Z}$ with $a_1, a_2, \ldots, a_n$ not zero. A Diophantine equation of the form

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

is a *linear Diophantine equation in the n variable $x_1, \ldots, x_n$.*

The participation assignment classifies linear Diophantine equations in one variable.

The question of whether there are solutions to Diophantine equations becomes harder when there is more than one variable. Then next step is to classify Diophantine equations in two variables.

Theorem 1. Let $ax + by = c$ be a linear Diophantine equation in the variables x and y. Let $d = (a, b)$. If $d \nmid c$, then the equation has no solutions; if $d \mid c$, then the equation has infinitely many solutions. Furthermore, if x_0, y_0 is a particular solution of the equation, then all solution are given by $x = x_0 + \frac{b}{d}n$ and $y = y_0 - \frac{a}{d}n$ where $n \in \mathbb{Z}$.

Proof Since $d \mid a, d \mid b$, we have that $d \mid c$. So, if $d \nmid c$, then the given linear Diophantine equation has no solutions.

Assume that $d \mid c$. Then, there exists $r, s \in \mathbb{Z}$ such that

$$d = (a, b) = ar + bs.$$

Furthermore, $d \mid c$ implies $c = de$ for some $e \in \mathbb{Z}$. Then

$$c = de = (ar + bs)e = a(re) + b(se).$$

Learning outcomes:
Author(s):

Thus, $x = re$ and $y = se$ are integer solutions.

Let x_0, y_0 be a particular solution to $ax + by = c$ Then, if $n \in \mathbb{Z}, x = x_0 + \frac{b}{d}n$ and $y = y_0 - \frac{a}{d}n$,

$$ax + by = a(x_0 + \frac{b}{d}n) + b(y_0 - \frac{a}{d}n) = ax_0 + \frac{abn}{d} + by_0 - \frac{abn}{d} = c.$$

We now need to show that every solution has this form. Let x and y be any solution to $ax + by = c$. Then

$$(ax + by) - (ax_0 + by_0) = c - c = 0.$$

Rearranging, we get

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

Dividing both sides by d gives

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y).$$

Now $\frac{b}{d} \mid \frac{a}{d}(x - x_0)$ and $(\frac{a}{d}, \frac{b}{d}) = 1$, so $\frac{b}{d} \mid x - x_0$. Thus, $x - x_0 = \frac{b}{d}n$ for some $n \in \mathbb{Z}$. The proof for y is similar. ■

Example 1. Is $24x + 60y = 15$ is solvable?

Multiple Choice:

(a) Yes

(b) No ✓

Example 2. Find all solutions to $803x + 154y = 11$.

Using the Euclidean Algorithm, we find:

$$\begin{aligned} 803 &= 154 * 5 + 33 \\ 154 &= 33 * 4 + 22 \\ 33 &= 22 * 1 + 11 \end{aligned}$$

Thus

$$\begin{aligned} (803, 154) &= 33 - 22 \\ &= 33 - (154 - 33 * 4) = 33 * 5 - 154 \\ &= (803 - 154 * 5) * 5 - 154 = 803 * 5 - 154 * 26 \end{aligned}$$

Thus, all solutions to the Diophantine equation have the form $x = 5 + \frac{154}{11}n$ and $y = -26 - \frac{803}{11}n$.

Example 3. There is a famous riddle about Diophantus: "God gave him his boyhood one-sixth of his life, One twelfth more as youth while whiskers grew rife; And then yet one-seventh ere marriage begun; In five years there came a bouncing new son. Alas, the dear child of master and sage After attaining half the measure of his father's life chill fate took him. After consoling his fate by the science of numbers for four years, he ended his life."

That is: Diophantus's childhood was $1/6^{th}$ of his life, adolescence was $1/12^{th}$ of his life, after another $1/7^{th}$ of his life he married, his son was born 5 years after he married, his son then died at half the age that Diophantus died, and 4 years later Diophantus died.

The Diophantine equation that let's us solve this riddle is:

$$x = \frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4.$$

Then, Diophantus's childhood was 14 years, his adolescence was 7 years, he married when he was 33, his son was born when he was 38 and died 42 years later, then Diophantus died when he was 84.

Nonlinear Diophantine equations

Definition 3. A Diophantine equation is *nonlinear* if it is not linear.

Example 4. (a) The Diophantine equation $x^2 + y^2 = z^2$ is our next section. Solutions are called Pythagorean triples.

(b) Let $n \in \mathbb{Z}$ with $n \geq 3$. The Diophantine equation $x^n + y^n = z^n$ is the subject of the famous Fermat's Last Theorem. We will also prove one case of this.

(c) Let $n \in \mathbb{Z}$. The Diophantine equation $x^2 + y^2 = n$ tells us which integers can be represented as the sum of two squares.

(d) Let $d, n \in \mathbb{Z}$. The Diophantine equation $x^2 - dy^2 = n$ is known as Pell's equation.

Sometimes we can use congruences to show that a particular nonlinear Diophantine equation has no solutions.

Example 5. Prove that $3x^2 + 2 = y^2$ is not solvable.

Assume that there is a solution. Then any solution to the Diophantine equation is also a solution to the congruence $3x^2 + 2 \equiv y^2 \mod 3$, which implies $2 \equiv y^2 \mod 3$, which we know is false. Thus there are no integer solutions to $3x^2 + 2 = y^2$.

Note: viewing the same equation modulo 2 says $x^2 \equiv y^2 \mod 2$, which does not give us enough information to prove a solution does not exist.

Pythagorean triples

One of the most famous math equations is $x^2 + y^2 = z^2$, probably because we learn it in high school. We are going to classify all integer solutions to the equation.

Definition 4. A triple (x, y, z) of positive integers satisfying the Diophantine equation $x^2 + y^2 = z^2$ is called *Pythagorean triple*.

Select the Pythagorean triples:

Select All Correct Answers:

(a) 3,4,5 ✓

(b) 5,12,13 ✓

(c) -3,4,5

(d) 6,8,10 ✓

(e) 0,1,1

It is actually possible to classify all Pythagorean triples, just like we did for linear Diophantine equations in two variables. To simplify this process, we will work with $x, y, z > 0$, and $(x, y, z) = 1$. For any given solution of this form, we have that $(-x, y, z), (x, -y, z), (x, y, -z), (-x, -y, z), (x, -y, -z), (-x, y, -z)$, and $(-x, -y, -z)$ are also solutions to the Diophantine equation, as is (nx, ny, nz) for any integer n. Thus, we call such a solution a *primitive Pythagorean triple*. We call $(0, n, \pm n)$ and $(n, 0, \pm n)$ the *trival solutions*.

Theorem 2. For a primitive Pythagorean triple (x, y, z), exactly one of x and y is even.

Proof If x and y are both even, then z must also be even, contradicting that $(x, y, z) = 1$.

If x and y are both odd, then z is even. Now we can work modulo 4 to get a contradiction. Since x and y are odd, we have that $x^2 \equiv y^2 \equiv 1 \pmod 4$. Since z is even, we have that $z^2 \equiv 0 \pmod 4$, but $x^2 + y^2 \equiv 2 \pmod 4$.

Thus, the only remaining option is exactly one of x and y is even. ■