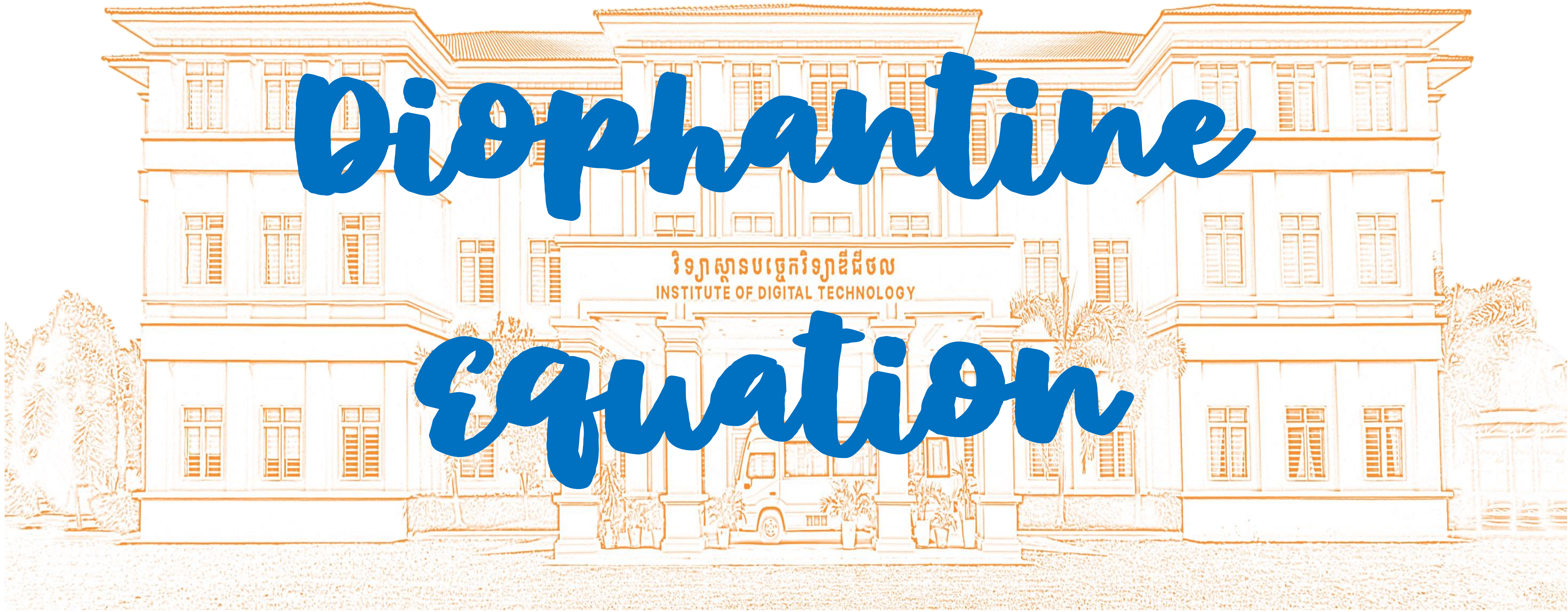
CADT IDT វិទ្យាស្ថានបច្ចេកវិទ្យាឌីជីថល
Institute of Digital Technology

Department of Foundation Year



Diophantine Equation

NGETH YOUDARITH

youdarith.ngeth@cadt.edu.kh

(+855) 12 600 012

How to Solve Linear Diophantine Equation in 3 Variables

A Diophantine equation is a polynomial equation whose solutions are restricted to integers. These types of equations are named after the ancient Greek mathematician Diophantus. A **linear Diophantine equation** is a first-degree equation of this type. Diophantine equations are important when a problem requires a solution in whole amounts.

Example: How many ways are there to make $2.00 from only nickels and quarters?

Let *n* be the number of nickels and let *q* be the number of quarters. Then a solution to this problem would satisfy the equation $5n + 25q = 200$.

How to Solve Linear Diophantine Equation in 3 Variables

However, this is a bit different from simply solving an equation because

- there is more than one solution to account for;
- the solutions are restricted by the fact that they must be non-negative integers.

The study of problems that require integer solutions is often referred to as **Diophantine analysis**. Although the practical applications of Diophantine analysis have been somewhat limited in the past, this kind of analysis has become much more important in the digital age. Diophantine analysis is very important in the study of public-key cryptography

How to Solve Linear Diophantine Equation in 3 Variables

Initial Solution to a Diophantine Equation

You may have observed from the examples above that finding solutions to linear Diophantine equations involves finding an **initial solution**, and then altering that solution in some way to find the remaining solutions. The process of finding this initial solution isn't always as straightforward as the examples above. Fortunately, there is a formal process to finding an initial solution.

First, it is important to recognize when solutions exist. Recall the previous example in which there were no solutions. There was a common factor between the coefficients of the variables, but the constant term was not divisible by this factor. This observation is generalized with the Bézout's identity:

How to Solve Linear Diophantine Equation in 3 Variables

- **Bézout's Identity:**
- Let aa and bb be non-zero integers and let $d = \gcd(a, b)$. Then there exist integers *x* and *y* that satisfy $ax + by = d$.
- Furthermore, there exist integers *x* and *y* that satisfy $ax + by = n$
- if and only if $d \mid n$.
- *One can determine if solutions exist or not by calculating the GCD of the coefficients of the variables, and then determining if the constant term can be divided by that GCD.*
- Find all integers solutions to the equation$14x + 91y = 53$.
- First, calculategcd(14,91)=7. Then, observe that $7 \nmid 53$. Therefore, by Bézout's Identity, there are no integer solutions to the equation

How to Solve Linear Diophantine Equation in 3 Variables

If solutions do exist, then there is an efficient method to find an initial solution.

The Euclidean algorithm gives both the GCD of the coefficients and an initial solution.

Method for computing the initial solution to a linear Diophantine equation in 2 variables

Given an equation $ax + by = n$:

- Use the Euclidean algorithm to compute $\gcd(a, b) = d$, taking care to record all steps.
- Determine if $d \mid n$. If not, then there are no solutions.
- Reformat the equations from the Euclidean algorithm.
- Using substitution, go through the steps of the Euclidean algorithm to find a solution to the equation $ax_i + by_i = d$.
- The initial solution to the equation $ax + by = n$ is the ordered pair $\left(x_i \cdot \frac{n}{d}\ ,\ y_i \cdot \frac{n}{d}\right)$

How to Solve Linear Diophantine Equation in 3 Variables

Find an initial integer solution to the equation $141x + 34y = 30$.

Using the Euclidean algorithm, we have

$141 = 4(34) + 5$

$34 = 6(5) + 4$

$5 = 1(4) + 1$

there for GCD(141,34)=1 and Solution exist because 1|30

$5 = 141 - 4(34)$

$4 = 34 - 6(5)$

$1 = 5 - 1(4)$

How to Solve Linear Diophantine Equation in 3 Variables

Now use substitute to find a solution to equation $141x_i + 34y_i = 1$

$$1 = 5 - 1(4)$$

$$1 = 5 - 1[34 - 6(5)]$$

$$1 = 7(5) - 1(34)$$

$$1 = 7[141 - 4(34)] - 1(34)$$

$$1 = 7(141) - 29(34)$$

This give $x_i = 7\ and\ y_i = -29$ as a solution to the equation $141x_i + 34y_i = 1$

then the initial solution to the equation $14x + 34y = 1$ is

$$x = 7 \cdot 30 = 210$$

$$y = -29 \cdot 30 = -870$$

How to Solve Linear Diophantine Equation in 3 Variables

General Solution to Linear Diophantine Equations

In the example above, an initial solution was found to a linear Diophantine equation.

This is just one solution of the equation, however. When integer solutions exist to an equation $ax + by = n$, there exist **infinitely many** solutions.

If (x_0 , y_0) is an integer solution of the Diophantine equation $ax + by = n$, then all integer solutions to the equation are of the form

$(x_0 + \frac{b}{GCD(a,b)} t , y_0 - \frac{a}{GCD(a,b)} t)$ for some integer t.

How to Solve Linear Diophantine Equation in 3 Variables

Find all integer solution to the equation

1. $141x + 34x = 30$
2. $4x + 7y = 97$

How to Solve Linear Diophantine Equation in 3 Variables

Equations with more than 2 Variables

Now, consider the linear Diophantine equation in three variables

$ax+by+cz=d$. Again by Bézout's Identity, as aa and bb range over all integer values, the set of values $ax+by$ is equal to the set of multiples of gcd(a,b). This shows that the Diophantine equation $ax+by+cz=d$ has integer solutions if and only if gcd(a,b)$w+cz=d$ has integer solutions, for $ax+by$=gcd(a,b)w. By the above reasoning, the second equation has integer solutions if and only gcd(a,b,c) divides d.

How to Solve Linear Diophantine Equation in 3 Variables

- By continuing this argument, the linear Diophantine equation
- $a_1x_1 + a_2x_2 + \cdots + a_nx_n = d$
- has integer solution (x_1 , x_2 , x_3 , … … , x_n) if and only if $GCD(a_1, a_2, a_3, \dots, a_n)|d$
- Example : Find all integer $28x + 30y + 31z = 365$

How to Solve Linear Diophantine Equation in 3 Variables

- Find all integer $6x + 15y + 10z = 53$