Introduction to Number Theory

Part C.

- Linear Diophantine Equation
- Arithmetic Functions

Nikenasih B, M.Si
Mathematics Educational Department
Faculty of Mathematics and Natural Science
State University of Yogyakarta

Contents all part

- Preliminary
- Divisibility
- Congruence
- Unique Factorisation
- Linear Diophantine Equation
- Arithmetic Functions

Linear Diophantine Equation (LDE)

- It's given equation of variables $x_1, x_2, \cdots, x_k$ as follows :

$$f(x_1, x_2, \cdots, x_k) = 0$$

- Problem of finding the integer solution(s) of equation above is named Diophantine problem and the equation is named Diophantine equation.

- Suppose *x* and *y* are variables of integers. The simplest form of Diophantine equation is

$$ax + by = c$$

Where *a* and *b* are positive integers.

- Now, we would like to find the general integers solution of the simplest form of Diophantine Equation above if it exists.

- At first, it is defined that two integers is called relative prime if the greatest common divisor of a and b is 1.

LDE – Theorem 1

If *a* and *b* are relative prime, then there exist x_1 and y_1 integers such that

$$ax_1 + by_1 = 1$$

Proof :

Without loss of Generalization, suppose b > 0. Consider the sequence as follows :

$$a \cdot 1, a \cdot 2, a \cdot 3, \cdots, a \cdot b, a \cdot (b+1), \cdots$$

Because *a* and *b* are relative prime, then if we devide all numbers by b, for the first *b-1* numbers, the remainders are $\{1,2,3,\cdots,b-1\}$ and there are no two or more numbers have similar remainder. From this point, there exist $x_1 \in \{1,2,3,\ldots,b-1\}$ such that the remainder of ax_1 if it is divided by *b* is 1. This is implied that there exist an integer y^* such that

$$ax_1 = by^* + 1$$

Take $y_1 = -y^*$, then it follows that there exist x and y integers such that

$$ax_1 + by_1 = 1.$$

Proof complete.

LDE – Theorem 2

The greatest common divisor of two positive integers a and b can be stated as linear combination of a_1 and b, that is there exist integers x_2 and y_2 such that

$$GCD(a,b) = ax_2 + by_2. \qquad (I.2)$$

Proof :

Suppose that $GCD(a,b) = d$. It is implied that a and b is divisible by d or there exist integers a_1 and b_1 such that $a = da_1$ and $b = db_1$. Because d is the greatest common divisor then a_1 and b_1 are relative prime. By using Theorem II.2, then there exist integer x_2 and y_2 such that

$$a_1x_2 + b_1y_2 = 1$$

Multiply both side with d, we get

$$da_1x_2 + db_1y_2 = d \text{ or } ax_2 + by_2 = d = GCD(a,b).$$

Proof complete.

LDE – Theorem 3

If a and b are two positive integers and d_1 is divisible by $GCD(a,b)$ then there exist integers x_3 and y_3 such that

$$ax_3 + by_3 = d_1$$

Proof :

Suppose that $GCD(a,b) = d$. As given that d_1 is divisible by $GCD(a,b)$ which means that there exist s such that $d_1 = ds$. From the Theorem II.3, there exist integer x_2 and y_2 such that

$$ax_2 + by_2 = d$$

Multiply both side with s then we get

$$asx_2 + bsy_2 = ds$$

Suppose $x_3 = sx_2$ and $y_3 = sy_2$, then

$$ax_3 + by_3 = d_1.$$

Proof complete.

From The Theorems above, we can conclude that there exist integers solution for $ax + by = d_1$, if d_1 is divisible by GCD(a,b). Suppose (x_0, y_0) is one solution for the simplest linear diophantine equation above, then

$$ax_0 + by_0 = d_1$$

Now, we would like to find the general formula for its solution if its given specific solution of simplest linear diophantine equation (x_0, y_0). Suppose

$$x = x_0 + p, y = y_0 + q$$

Substitute to the equation, we get

$$a(x_0 + p) + b(y_0 + q) = d_1$$

Because (x_0, y_0) is one solution, then

$$ap + bq = 0$$

$$p = -\frac{bq}{a}$$

Suppose d=GCD(a,b), then there exist integers a_1 and b_1 such that $a = da_1$ and $b = db_1$. In other words, a_1 and b_1 are relative prime . Here, we get

$$da_1 p + db_1 q = 0$$

$$p = -\frac{b_1 q}{a_1}$$

Because a_1 and b_1 are relative prime and p is an integer, then q must be multiple of a_1. Suppose k is any integers such that $q = a_1 k$, then

$$p = -\frac{bq}{a} = -\frac{ba_1 k}{da_1} = -\frac{bk}{d}$$

$$-\frac{bk}{d} = -\frac{bq}{a} \rightarrow q = \frac{a}{d}k$$

Here, we get

the general solution for the simplest linear diophantine equation $ax + by = d_1$ and (x_0, y_0) is one solution, if d_1 is divisible by GCD(a,b), is

$$x = x_0 + \frac{b}{\gcd(a,b)}k$$

$$y = y_0 - \frac{a}{\gcd(a,b)}k$$

LDE - Exercises

- Find one integer solution for $17x + 83y = 5$.
- Find all positive number (x,y) which satisfy $12x + 5y = 125$.
- Exploration. Find all positive solution for $17x – 83y = 5$.
- It's given positive integer $x > 1$ and y which satisfy equation $2007x – 21y = 1923$. Find the minimum value for $x + y$.

Arithmetic Functions

An *arithmetic function f is a function whose domain is the set of positive integers and whose range is a subset of the complex* numbers.

The following functions are of considerable importance in Number Theory:

- *d(n) the number of positive divisors of the number n.*
- σ(*n) the sum of the positive divisors of n.*
- ϕ(*n) the number of positive integers not exceeding n and relative prime to n.*
- ω(*n) the number of distinct prime divisors of n.*
- Ω(*n) the number of primes dividing n, counting multiplicity.*

- The symbols of above functions are

$$d(n) = \sum_{d|n} 1,\ \sigma(n) = \sum_{d|n} d,\ \omega(n) = \sum_{p|n} 1,\ \Omega(n) = \sum_{p^\alpha \| n} \alpha,$$

and

$$\phi(n) = \sum_{\substack{1 \le k \le n \\ (k,n)=1}} 1.$$

let n have the prime factorisation $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. Then

$$d(n) = (1 + a_1)(1 + a_2) \cdots (1 + a_r).$$