Solution for the Simplest Diophantine Equation $ax + by = c$

NIKENASIH BINATARI[1]
Mathematics Education Department
Faculty of Mathematics and Natural Sciences
State University of Yogyakarta, Yogyakarta

I. Number Theory

In Number Theory, we usually deal with the properties of integers $Z = \{\cdots,-2,-1,0,1,2,\cdots\}$. Four fundamental operations in number that we have learned on elementary school are addition (+), substraction (-), multiplication (x) and division (/). For the first three operations, the result will result an integer while the last operations isn't necessary one. The first study about integers is divisibility.

Definition I.1 :
For an integer m and a nonzero integer n, we say that *m* is **divisible by** *n* or *n* divides *m* if there is an integer k such that *m* = *k* x *n*.

We denote this by *n* | *m*. If *m* is divisible by *n*, then *m* is called a multiple of *n* and *n* is called a divisor (or factor) of *m*. For any integers *m* and *n*, without loss of generality suppose *m* > *n*, *m* isn't guarantee divisible by *n*, vice versa. For some cases there exist integers *r* and *b*, where $0 < r < n$, such that *m* and *n* can be written as

$$m = bn + r \qquad \text{(I.1)}$$

For the form above, *b* is called a quotient and *r* is the remainder.

For a positive integer *m*, denoted D_m is the set of all factor of *m*. It's implied that for each $n \in D_m$, then *m* is divisible by *n*. An integer *e* is called common divisor of integer set $m_1, m_2, \cdots, m_k$ for some natural number *k*, if $e \in D_i, i = 1,2,\ldots,k$. As we can see here, that the value of *e* isn't always unique. The greatest number *e* which satisfies this property then is called as greatest common divisor (GCD) and is usually noted as $GCD(m_1, m_2, \cdots, m_k) = d$. So, for m_1, m_2 nonzero integers,

[1] Corresponding Author
E-mail address : **nikenasih@yahoo.com**

$GCD(m_1, m_2) = d$ such that for every common divisor *e*, satisfy *d* is divisible by *e* and d > 0.

Theorem 1.2 :
Let *b,n* and *r* be positive integers, then

$$GCD(bn + r, n) = GCD(n, r). \qquad \text{(I.2)}$$

As we had learned on secondary school that we can use prime factorization method to find the greatest common divisor of two integer *m* and *n*. Using Theorem I.2, we can find the greatest common divisor of two integer *m* and *n* with another way.

Theorem I.3 :
Let m and n be positive integers where $0 < n < m$. From Eq. I.1 we know that there exist integers *b* and *r* such that

$$m = bn + r,\ 0 < r < n$$

Therefore, by using Theorem I.2

$$GCD(m, n) = GCD(bn + r, n) = GCD(n, r)$$

Because *n* and *r* are positive integers where 0 < r < n, we know that there exist integers b_1 and r_1 such that

$$n = b_1 r + r_1,\ 0 < r_1 < r$$

Therefore, by using Theorem I.3

$$GCD(n, r) = GCD(b_1 r + r_1, r) = GCD(r, r_1)$$

If we continu this process, then there exist integers $r_2, r_3, \ldots, r_s$ such that

$$GCD(m, n) = GCD(n, r) = GCD(r, r_1) = GCD(r_1, r_2) = \cdots = GCD(r_{s-1}, r_s) = r_s.$$

Example I.4.
Find the greatest common divisor of 76.084 and 63.020.

II. Diophantine Equation

In its simplest definition, number theory deals with equations where the variables are integers. As such, all variables below will be integers unless otherwise noted.

Definition II.1 :
It's given equation of variables $x_1, x_2, \cdots, x_k$ as follows :

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

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.

Teorema II.2.
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.

Theorem II.3 :
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

$$a_1 x_2 + b_1 y_2 = 1$$

Multiply both side with d, we get

$$da_1 x_2 + db_1 y_2 = d \text{ or } ax_2 + by_2 = d = GCD(a,b).$$

Proof complete.

Theorem II.4

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 Theorem II.4 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 $ax + by = d_1$ if d_1 is divisible by GCD(a,b) is

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

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

Exercise

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

III. Conclusion

From the explanation 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 the general solution of it is

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

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