Linnæus University
School of Computer Science, Physics and Mathematics

Degree Project

Solving Linear Diophantine Equations and Linear Congruential Equations

2012-06-01
Author: Deniz Yesilyurt
Subject: Mathematics
Level: Bachelor
Course code: 2MA11E

Abstract

This report represents GCD, euclidean algorithm, linear diophantine equation and linear congruential equation. It investigates the methods for solving linear diophantine equations and linear congruential equations in several variables. There are many examples which illustrate the methods for solving equations.

Contents

1 Introduction

Linear diophantine equations got their name from Diophantus. Diophantus of Alexandria was a mathematician who lived around the 3rd century. Diophantus wrote a treatise and he called 'Arithmetica' which is the earliest known book on algebra.

A Diophantine equation is an algebraic equation for which rational or integral solutions are sought. An algebraic equation is one that involves only polynomial expressions in one or more variables. What makes the equation 'Diophantine' is that the coefficients of the polynomials should be rational numbers(or often integers)and also solutions must be only rational(or integer).

Brahmagupta(598-670)was the first mathematician who gave general solution of the linear diophantine equation ($ax + by = c$). Diophantus didn't use complicated algebraic notation, but Brahmagupta used the complicated notations for solving equation.

Two well known results from beginning number theory are examples of diophantine equations which predate Diophantus. Both of these problems were known by the Babylonians. These are;

1. Linear equations of two variables, $ax + by = c$
2. The quadratic equation of three variables, $x^2 + y^2 = z^2$

And also we can mention linear congruences. First, Carl Freidrich Gauss considered the congruences and he developed congruences. Gauss noticed; when he try to solve the linear diophantine equations($ax+by = c$); if $m|(a-b)$, then we write $a \equiv b \pmod{m}$, and a is congruent to b modulo m.

Except Gauss, many scientist seek the linear congruences and solutions of them. Some of them; J.konig [1],Th.Schnemann [2] and M.Fekete [3].

Congruences are used in our daily life, today is monday or the time is 15:00. The periodic nature of dates and time can be described using congruences.

The purpose of this study is derive algorithms for finding all the solutions of linear diophantine equation of the form

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

and also we will derive algorithm for solving the linear congruential equation;

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n \equiv b \pmod{m}.$$

In this project, we have two main sections. First section is about linear diophantine equation. There are required definitions and theorems for explaining linear diophantine equation. These are GCD, euclidean algorithm,

extended euclidean algorithm and linear diophantine equation. There are also some examples for understand the theorems and definitions better. In the last part of first section, there are two applications which are related to linear diophantine equation. We will see that linear diophantine equation in more than two variables can be solved by induction method.

Second section is about linear congruential equation. It contains introduction to congruences, basic congruences theorems, linear congruences theorems and also definitions for solving linear congruential equation in several variables. We will search for the number of incongruent solutions of linear congruential equation in various variables. We will find the number of solutions to linear congruential equation in one variable and by generalization, we will get the linear congruential equation in n variables has $|m|^{n-1} \cdot d$ incongruent solutions.

2 Linear Diophantine Equations

2.1 Greatest Common Divisor

Definition 2.1.1. Given the integers $a, b > 0$, we define greatest common divisor of a and b, as the largest number that divides both a and b. It is denoted in two ways: $(a, b) = c$ or $gcd(a, b) = c$. We will use (a, b) to denote the greatest common divisor.

Example 2.1.1. Let's find GCD of 15 and 35. The divisors are of 15; $\pm1, \pm3, \pm5, \pm15$,the divisors of 35 are;$\pm1, \pm5, \pm7, \pm35$, and the common divisors of 15 and 35 are; $\pm1, \pm5$, and the greatest common divisor is 5, so the gcd of 15 and 35 is 5 and by notation $(15, 35) = 5$.

Definition 2.1.2. If the greatest common divisor of $(a, b) = 1$, we say that the integers are relatively prime.

Theorem 2.1.1. a and b integers with $(a, b) = d$. Then $(\frac{a}{d}, \frac{b}{d}) = 1$

Proof. Assume that $(\frac{a}{d}, \frac{b}{d}) = k$, then $\frac{a}{d} = mk$, $\frac{b}{d} = nk$ where m, n are any integers and we get $a = mkd$, $b = nkd$, therefore $kd|a$ and $kd \mid b$. Since d is the greatest common divisor for a and b, $kd \leq d$, $k \leq 1$ then k must be equal to 1, if k is bigger than 1, d isn't gcd of a and b, so $k = 1$ and$(\frac{a}{d}, \frac{b}{d}) = 1$. □

Let's illustrate the theorem.

Example 2.1.2. Let's find gcd of 12 and 18. By factorization $12 = 2^2 \cdot 3$ and $18 = 3^2 \cdot 2$, hence we can see gcd of 12 and 18 equal to 6, namely $(12, 18) = 6$.

$$(\frac{12}{6}, \frac{18}{6}) = (2, 3) = 1.$$

Theorem 2.1.2. Let a, b and c be integers. Then $(a + cb, b) = (a, b)$.

Proof. Suppose that $(a, b) = d$ and $(a + cb, b) = k$ and we should prove that $d = k$. If $(a, b) = d$, we can write $a = dt$ and $b = dp$ where t, p are any integers.
If $(a + cb, b) = k$, then $a + cb = km$ and $b = kn$ where m, n are any integers. In $a + cb$, we should write instead of a and b,$a = dt$ and $cb = cdp$ then $(dt + cdp, dp) = (d(t + cp), dp)$ and from this equality, it is clear that the gcd of $d(t+cp)$ and dp is equal to d, since d divide $t+cp$ and p. So $(a+cb, b) = d$. Hence we find $d = k$. □

Example 2.1.3. Let's consider those numbers; $a = 190, b = 76, c = 38$. Then according to theorem, it must be like below;

$$(190 + 38 \cdot 76, 76) = (190, 76)$$

$$(3078, 76) = (190, 76)$$

For be sure of the equality, we must find the $(3078, 76)$ and $(190, 76)$

$$76 = 2^2 \cdot 19$$
$$190 = 2 \cdot 5 \cdot 19$$
$$3078 = 2 \cdot 3^4 \cdot 19.$$

So, we see $(3078, 76) = (190, 76) = 38$.

Definition 2.1.3. If a and b integers, the linear combination of a and b is a sum of the form $ax + by$, where x and y are integers.

Theorem 2.1.3. Given integers $a, b > 0$, then $d = (a, b)$ is the least positive integer that can be represented as $ax + by$ and x, y integer numbers.

Proof. Assume that k is the smallest integer, $k = ax+by$. If $d|a$ and $d|b$ then, $d|ax+by$, and also $d \leq k$. k should divide a; otherwise $a = uk+r$, $0 < r < k$ where $u, r \in \mathbb{Z}$; $r = a - uk = a - u(ax + by) = a(1 - ux) + b(-uy)$, so we found another linear combination and $r < k$. It is a contradiction, because our assumption was k is the smallest integer which can be represented as $ax + by$. The process is same for proving that $k|b$.
Then, we get $k \leq (a, b) = d$ and $k = d$. □

Example 2.1.4. Assume that $a = 169$ and $b = 13$

$$26 = 2 \cdot 13$$

$$169 = 13 \cdot 13$$

We find $(26, 169) = 13$.
If we choose $x = 1$, $y = -6$, we can write the equation below

$$169 - 26 \cdot 6 = 13 = (26, 169).$$

Theorem 2.1.4. If a, b, m and n are integers, and if $c|a$ and $c|b$, then $c|(ma + nb)$.

Proof. If $c|a$ and $c|b$, we can find e and f are integers, $a = ce$, $b = cf$. Then, $ma + nb = mce + ncf = c(me + nf)$. Hence, we saw that $ma + nb$ is a multiple of c. Thus, $c|ma + nb$. □

Example 2.1.5. Assume that $a = 16$, $b = 44$ and $c = 4$

$$16 = 2^4$$

$$44 = 2^2 \cdot 11.$$

So, 4 divides 16 and 44.
And assume that $m = 6$, $n = -2$, then

$$6 \cdot 16 - 2 \cdot 44 = 96 - 88 = 8.$$

And $4|8$. Because $8 = 2 \cdot 4$.

Theorem 2.1.5. If a and b are positive integers, then the set of linear combinations of a and b is the set of integer multiplies of (a, b).

Proof. Suppose that $(a, b) = c$. Let's show that every linear combination of a and b must also be a multiple of c. We know that $(a, b) = c$, then $c|a$ and $c|b$. Every linear combination of a and b is the form $ma + nb$ and by Theorem 2.1.4. we can see $c|ma + nb$, then $ma + nb = ck$. By Theorem 2.1.3. $(a, b) = c$ can be represented a linear combination of a and b, there are integers s.t. x and y, (a, b) can be written like; $(a, b) = ax + by$. If we multiply both of sides with s, we get $sc = sax + sby$. Hence, we saw that every multiple of c is a linear combination of a and b. □

Example 2.1.6. Suppose that $a = 28$, $b = 196$

$$28 = 2^2 \cdot 7$$

$$196 = 2^2 \cdot 7^2$$

Then $(28, 196) = 14$.
For any $x, y \in \mathbb{Z}$, there are some k values which provide the equation $28x + 196y = 14k$. If we consider the which x and y give us $k = 2$.

$$28x + 196y = 14 \cdot 2.$$

If we divide both sides by 28, the equation reduced to

$$x + 7y = 1.$$

Hence, we find $x = 8$ and $y = -1$.

Definition 2.1.4. We will also define GCD for more than two integers. Consider n integers, not all 0. The GCD is the largest number in the common divisors. The notation is $(a_1, a_2, \ldots, a_n)$.

Example 2.1.7. We can see $(6, 9, 12) = 3$ and $(5, 35, 50) = 5$.

But,sometimes we have more than three variables or complicated numbers, we can't find the gcd easily. We can use the Theorem 2.1.6. in such cases.

Theorem 2.1.6. If $a_1, a_2, \ldots, a_n$ are integers, not all 0, then $(a_1, a_2, \ldots, a_{n-1}, a_n) = (a_1, a_2, \ldots, (a_{n-1}, a_n))$.

Proof. Now, we have to find gcd of n integers. We know that any common divisor of $a_1, a_2, \cdots, a_{n-1}, a_n$ is also divisor of a_{n-1} and a_n. If we say that $d_1 = (a_{n-1}, a_n)$, it reduces to $n-1$ integers $a_1, a_2, \cdots, a_{n-2}, d_1$. Also, any common divisor of the $n-1$ integers $a_1, a_2, \cdots, a_{n-2}$ and (a_{n-1}, a_n) is common divisor of n integers, if it divides $d_1 = (a_{n-1}, a_n)$ and both of a_{n-1},a_n. The gcd of n integers, the gcd of first $n-2$ integers and the gcd of the last two integers are same, namely their gcd is equal. □

Example 2.1.8. Find the gcd of 256,342,578,1000 and 3472.
Using the Theorem 2.1.6. By prime factorization

$$256 = 2^8$$
$$342 = 2 \cdot 3^2 \cdot 19$$
$$578 = 2 \cdot 17^2$$
$$1000 = 2^3 \cdot 5^3$$
$$3472 = 2^4 \cdot 7 \cdot 31.$$

$$\begin{aligned}(256, 342, 578, 1000, 3472) &= (256, 342, 578, (1000, 3472)) \\ &= (256, 342, 578, 8) \\ &= (256, 342, (578, 8)) \\ &= (256, 342, 2) \\ &= (256, (342, 2)) \\ &= (256, 2) \\ &= 2.\end{aligned}$$

Lemma 2.1.1. If e and d are integers and $e = dq + r$, where q and r are integers, then $(e, d) = (d, r)$.

Proof. This lemma follows directly from Theorem 2.1.2, taking $a = r, b = d, c = q$. Suppose that $a = (d, e)$, then $a|d$ and $a|e$. And there are integers such that t and s, it can be written $d = at$ and $e = as$. Multiply both sides by q in the equation $d = at$, and it will be equal to $qd = qat$. Now, we can

mention the equation $qd-e$. We found the values of qd and e. If we put up these values in the equation $qd-e$, we will find $qd-e=qat-as=a(qt-s)$ and $a|qd-e$, in other words $a|r$. Then a is a common divisor of d and r. If b is a common divisor of d and r so $b|dq+r$, namely $b|e$. b is a common divisor of d and e. $b \leq a$ and from definition of gcd we get $a=(d,r)$ $\square$

Example 2.1.9. Consider the equation below;

$$27 = 6 \cdot 4 + 3.$$

If we analyse the equation according to theorem, we will reach;

$$e = 27, d = 6, r = 3$$

$$6 = 2 \cdot 3$$

$$27 = 3^3.$$

$$(6, 27) = (6, 3) = 3.$$

2.2 Euclidean Algorithm

Now, we can determine euclidean algorithm. The euclidean algorithm is a way to find the gcd of two positive integers. The euclidean algorithm is an extremely fast way to find gcd.

Theorem 2.2.1. *(Euclidean Algorithm)*To compute the gcd of two numbers a and b, let $r_{-1} = a$, let $r_0 = b$, and compute successive quotients and remainders

$$r_{i-1} = q_{i+1} \cdot r_i + r_{i+1}.$$

for $i = 0, 1, 2, \ldots$ until some remainder r_{n+1} is 0. The last nonzero remainder r_n is then the gcd of a and b.

Proof. The algorithm will work in the following way:

$$a = b \cdot q_1 + r_1, 0 \leq r_1 < b$$

$$b = r_1 \cdot q_2 + r_2, 0 \leq r_2 < r_1$$

$$r_1 = r_2 \cdot q_3 + r_3, 0 \leq r_3 < r_2$$

$$r_2 = r_3 \cdot q_4 + r_4, 0 \leq r_4 < r_3$$

$$\vdots$$

$$r_{i-1} = r_i \cdot q_{i+1} + r_{i+1}, 0 \leq r_{i+1} < r_i$$

$$\vdots$$

$$r_{n-3} = r_{n-2} \cdot q_{n-1} + r_{n-1}, 0 \leq r_{n-1} < r_{n-2}$$

$$r_{n-2} = r_{n-1} \cdot q_n + r_n \to (gcd), 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = r_n \cdot q_{n+1} + 0.$$

We will answer that why is the last nonzero remainder r_n a common divisor of a and b?

It is clear from the last line that r_n divides r_{n-1}. Then the previous line r_n divides r_{n-2}, since it divides both r_{n-1} and r_n, (we can see it by Lemma 2.1.1. $(r_n, r_{n-1}) = (r_{n-1}, r_{n-2})$). Moving up to previous line, r_n divides r_{n-3}, since r_{n-3} divides r_{n-1} and r_{n-2} and $(r_{n-3}, r_{n-2}) = (r_{n-2}, r_{n-1})$. In the middle line, we can see r_n divides r_{n+1}, because of Lemma 2.1.1. says $(r_n, r_{n-1}) = (r_{n-1}, r_{n-2}) = (r_{n-2}, r_{n-3}) = \cdots = (r_{i-1}, r_i) = (r_i, r_{i+1})$.
Moving up line by line,when we arrive the second line we already know that r_n divides r_2 and r_1, then $(r_n, r_{n-1}) = (r_{n-1}, r_{n-2}) = (r_{n-2}, r_{n-3}) = \cdots = (r_2, r_1)$. Then the second line $b = q_2 \cdot r_1 + r_2$ tells us if r_n divides r_2 and r_1, also r_n divides b, $(r_n, r_{n-1}) = (r_{n-1}, r_{n-2}) = (r_{n-2}, r_{n-3}) = \cdots = (r_2, r_1) = (r_1, b)$. And in conclusion r_n divides r_1 and b, so it divides also a, by using Lemma 2.1.1. $r_n = (r_n, r_{n-1}) = (r_{n-1}, r_{n-2}) = (r_{n-2}, r_{n-3}) = \cdots = (r_2, r_1) = (r_1, b) = (a, b)$.
Now, we know that the last nonzero remainder will be gcd, but now we must answer that how do we know that we always get a remainder that equals to 0? When we compute a quotient with remainder, we get;
$A = Q \cdot B + R$.
The remainder will be between 0 and $B - 1$. This is clear, since if $R \geq B$, then we can add one more to the quotient Q and substract B from R. So the remainders will be decreasing;
$b = r_0 > r_1 > r_2 > r_3 \cdots$
But all of the remainders are greater than or equal to 0, so we have decreasing sequence of nonnegative integers. After all we conclude remainder that equals to 0 and it is clear that we will reach a remainder of 0 in at most b steps. □

Example 2.2.1. We illustrate the euclidean algorithm:
$(128, 442)$

$$442 = 128 \cdot 3 + 58$$

$$128 = 58 \cdot 2 + 12$$

$$58 = 12 \cdot 4 + 10$$

$$12 = 10 \cdot 1 + 2$$

$$10 = 2 \cdot 5 + 0.$$

Euclidean algorithm says; the gcd of two variables is the last nonzero remainder, in the question the last nonzero remainder is 2. Then $(128, 442) = 2$

If we have more than two variables and we want to find gcd, we can use euclidean algorithm in connection with Theorem 2.1.6.

Example 2.2.2. Find $(63, 217, 350, 728, 7077, 9100)$ using euclidean algorithm.

$$(63, 217, 350, 728, (7077, 9100))$$

Let's find $(7077, 9100)$ using euclidean algorithm.

$$9100 = 7077 \cdot 1 + 2023$$

$$7077 = 2023 \cdot 3 + 1008$$

$$2023 = 1008 \cdot 2 + 7$$

$$1008 = 7 \cdot 144 + 0.$$

The last nonzero remainder 7. So, $(7077, 9100) = 7$.
The equation reduce to $(63, 217, 350, 728, 7)$.
And the other step $(63, 217, 350, (728, 7))$

$$728 = 7 \cdot 104 + 0$$

The remainder is 0. So, $7|728$ and $(728, 7) = 7$.
$(63, 217, (350, 7))$

$$350 = 7 \cdot 50 + 0$$

As is seen from above 350 is a multiple of 7. Then, $(350, 7) = 7$ and we should find $(63, (217, 7))$

$$217 = 7 \cdot 31 + 0$$

217 is a multiple of 7. That's why $(217, 7) = 7$.
It reduce to $(63, 7)$.

$$63 = 7 \cdot 9 + 0$$

We found $(63, 7) = 7$.
Then, $(63, 217, 350, 728, 7077, 9100) = 7$.

2.2.1 Extended Euclidean Algorithm

We already know how can we find the gcd of two numbers by euclidean algorithm. Suppose that $r_n = (a, b)$, $a > b$ and

$$a = b \cdot q_1 + r_1$$

$$b = r_1 \cdot q_2 + r_2$$

$$r_1 = r_2 \cdot q_3 + r_3$$

$$r_2 = r_3 \cdot q_4 + r_4$$

$$\vdots$$

$$r_{i-1} = r_i \cdot q_{i+1} + r_{i+1}$$

$$\vdots$$

$$r_{n-3} = r_{n-2} \cdot q_{n-1} + r_{n-1}$$

$$r_{n-2} = r_{n-1} \cdot q_n + r_n$$

$$r_{n-1} = r_n \cdot q_{n+1} + 0.$$

When we want to write gcd of two integers as a linear combination of these integers,we use the process in the following way.
The equation $(a, b) = r_n = r_{n-2} - r_{n-1} \cdot q_n$ express (a, b) as a linear combination of r_{n-2} and r_{n-1}. If we move to penultimate equation we can write;

$$r_{n-1} = r_{n-3} - r_{n-2} \cdot q_{n-1}.$$

So,we get

$$\begin{aligned} r_n &= r_{n-2} - (r_{n-3} - r_{n-2} \cdot q_{n-1}) \cdot q_n \\ &= r_{n-2}(1 + q_{n-1} \cdot q_n) - q_n \cdot r_{n-3}. \end{aligned}$$

The last expression shows us that it is a linear combination of r_{n-2} and r_{n-3}.
We continue to process(express (a,b) as a linear combination of each pair of remainders) until find (a, b) as a linear combination of a and b. If we write particular line,

$$(a, b) = k \cdot r_i + m \cdot r_{i-1}$$

Since,

$$r_i = r_{i-2} - r_{i-1} \cdot q_{i-1}$$

So,we have

$$\begin{aligned}(a,b) &= k(r_{i-2} - r_{i-1} \cdot q_{i-1}) + m \cdot r_{i-1} \\ &= k \cdot r_{i-2} + (m - k \cdot q_{i-1}) r_{i-1}.\end{aligned}$$

If we continue until the top line, we can find (a,b) as a linear combination of a and b. The following theorem gives the induction method for finding (a,b) as a linear combination of a and b.

Theorem 2.2.2. Let a and b be a positive integers. Then
$(a,b) = k_n \cdot a + m_n \cdot b$
where k_n and m_n the nth terms of the sequences defined recursively by

$$k_0 = 1, m_0 = 0$$

$$k_1 = 0, m_1 = 1.$$

and
$k_i = k_{i-2} - q_{i-1} \cdot k_{i-1}$, $m_i = m_{i-2} - q_{i-1} \cdot m_{i-1}$
for $i = 2, 3, \cdots, n$ where the q_i are the quotients in the divisions of the euclidean algorithm when it is used to find (a,b).

Proof. Let's prove that

$$r_i = k_i \cdot a + m_i \cdot b \tag{1}$$

for $i = 0, 1, \cdots, n$ since $(a,b) = r_n$, we mentioned the equation (1), we know that

$$(a,b) = r_n = k_n \cdot a + m_n \cdot b$$

If we use mathematical induction in equation (1),
For $i = 0$,

$$\begin{aligned}r_0 &= k_0 \cdot a + m_0 \cdot b \\ &= 1 \cdot a + 0 \\ &= a.\end{aligned}$$

For $i = 1$,

$$\begin{aligned} r_1 &= k_1 \cdot a + m_1 \cdot b \\ &= 0 + 1 \cdot b \\ &= b. \end{aligned}$$

We can see that equation (1) is valid for $j = 0, 1$.
Now, we assume that

$$r_i = k_i \cdot a + m_i \cdot b$$

for $i = 1, 2, \cdots, p-1$. Then, from the pth step of the euclidean algorithm, we know

$$r_p = r_{p-2} - r_{p-1} \cdot q_{p-1}$$

If we use induction method, we get

$$\begin{aligned} r_p &= (k_{p-2} \cdot a + m_{p-2} \cdot b) - (k_{p-1} \cdot a + m_{p-1} \cdot b) \cdot q_{p-1} \\ &= (k_{p-2} - k_{p-1} \cdot q_{p-1}) \cdot a + (m_{p-2} - m_{p-1} \cdot q_{p-1}) \cdot b \\ &= k_p \cdot a + m_p \cdot b. \end{aligned}$$

And as a result, we can write the (a, b) as a linear combination of a and b. The proof finishes.

□

Example 2.2.3. Let's illustrate Theorem 2.2.2. by finding integers x and y such that

$$12740x + 1610y = (12740, 1610).$$

First we use euclidean algorithm for finding $(12740, 1610)$.

$$12740 = 1610 \cdot 7 + 1470$$

$$1610 = 1470 \cdot 1 + 140$$

$$1470 = 140 \cdot 10 + 70$$

$$140 = 70 \cdot 2 + 0.$$

The last nonzero remainder is 70, so $(12740, 1610) = 70$.
We now use back substitution to express 70 as a linear combination of 12740 and 1610.

$$\begin{aligned}
70 &= 1470 - 140 \cdot 10 \\
&= 1470 - (1670 - 1470) \cdot 10 \\
&= 11 \cdot 1470 - 1610 \\
&= 11 \cdot (12740 - 1610 \cdot 7) - 1610 \\
&= 11 \cdot 12740 - 78 \cdot 1610.
\end{aligned}$$

We conclude that an integer solution of $12740x + 1610y = (12740, 1610)$ is $x = 11, y = -78$.

2.3 Linear Diophantine Equation

Definition 2.3.1. The diophantine equation is the polynomial equation which the coefficients are integers and diophantine equations whose solutions we seek in the set of integers or natural numbers. The most basic diophantine equation is the linear case. We can write $ax + by = c$ where $a, b, c \in \mathbb{Z}$.

Theorem 2.3.1. Let a,b, and c be integers with a and b not both zero. The linear diophantine equation

$$ax + by = c$$

has a solution if and only if $d = (a, b)$ divides c.

Proof. ($\Rightarrow$)

Suppose that x_0 and y_0 is a solution. Then $ax_0 + by_0 = c$. Since $d|a$ and $d|b$, we get that $d|ax_0 + by_0$ and $d|c$.

($\Leftarrow$)

Suppose that $d|c$. then $c = dk$ where k is an integer. We already know that by Theorem 2.1.5 (a, b) can be written as a linear combination of a and b. So, there exist $u, v \in \mathbb{Z}$ with $au + bv = d$. Hence $a(uk) + b(vk) = dk = c$. So the equation $ax + by = c$ has a solution(namely $x = uk, y = vk$). □

Example 2.3.1. Find the solution of $155x + 45y = 7$

First, we must find $(155, 45) =?$

$$(155, 45) = 5.$$

5 and 7 relatively prime. So we can't find a solution. Because, there is no solution.

Theorem 2.3.2. Let a and b integers with $d = (a, b)$. The equation $ax + by = c$ has no integral solutions if d doesn't divide c. If $d|c$, then there are infinitely many integral solutions. Moreover, if $x = x_0$, $y = y_0$ is a particular solution of the equation, then all solutions are given by

$$x = x_0 + \frac{b}{d}n, y = y_0 - \frac{a}{d}n,$$

where n is an integer.

Proof. We already know that there is a solution if and only if $d|c$ by Theorem 2.3.1.

For the second part of the theorem, let x_0,y_0 be a particular solution

$$ax_0 + by_0 = c.$$

If we put

$$x = x_0 + \frac{bn}{d}, y = y_0 - \frac{an}{d}$$

where n is any integer, then

$$ax + by = a(x_0 + \frac{bn}{d}) + b(y_0 - \frac{an}{d}) = ax_0 + by_0 = c,$$

so x, y are also solution.

We know from the previous Theorem 2.3.1., x and y integers since d divides b and a. This gives us many solutions , for different integers n. Let's show that these are any solution; x, y be any integer solution, so $ax+by = c$. Since $ax + by = c = ax_0 + by_0$ we have

$$a(x - x_0) + b(y - y_0) = 0,$$

so dividing by d we get

$$\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0). \tag{2}$$

Now, a and b aren't both 0, assume that $b \neq 0$. If we divide both the sides with $\frac{b}{d}$ and since $(\frac{a}{d}, \frac{b}{d}) = 1$, $\frac{b}{d}$ divides $x - x_0$(by $k|pr$ and $(k, p) = 1$, then $k|r$). Thus $x - x_0 = \frac{bn}{d}$ for some integer n, so $x = x_0 + \frac{bn}{d}$.
Substituting back for $x - x_0$ in (2) we obtain;

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

So dividing by $\frac{b}{d}$ (which is nonzero) we have

$$y = y_0 - \frac{an}{d}.$$

□

Example 2.3.2. Let the equation be

$$60x + 33y = 9.$$

And we will find all solution to $60x + 33y = 9$.
So, $a = 60$, $b = 33$, $c = 9$ and $(60, 33) = 3$, we can see $3|9$. So we can search for solutions.
First, we use euclidean algorithm

$$60 = 1 \cdot 33 + 27$$
$$33 = 1 \cdot 27 + 6$$
$$27 = 4 \cdot 6 + 3$$
$$6 = 2 \cdot 3 + 0.$$

We see the last nonzero remainder is 3 so $(60, 33) = 3$.
Reverse by step

$$\begin{aligned} 3 &= 27 - 4 \cdot 6 \\ &= 27 - 4 \cdot (33 - 27) \\ &= 5 \cdot 27 - 4 \cdot 33 \\ &= 5 \cdot (60 - 33) - 4 \cdot 33 \\ &= 5 \cdot 60 - 9 \cdot 33. \end{aligned}$$

So we take $u = 5$ and $v = -9$. One solution is then,

$$x_0 = 5 \cdot \frac{9}{3} = 15.$$
$$y_0 = -9 \cdot \frac{9}{3} = -27.$$

All the solutions are given by

$$x = 15 + \frac{33n}{3} \Rightarrow x = 15 + 11n.$$
$$y = -27 - \frac{60n}{3} \Rightarrow y = -27 - 20n.$$

where $n \in \mathbb{Z}$.

Now,we can extend the Theorem 2.3.2 with more than two variables.

Theorem 2.3.3. If $a_1, a_2, \ldots, a_n$ are non zero positive integers, then the equation $a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$ has an integral solution if and only if $d = (a_1, a_2, \ldots, a_n)$ divides c. Furthermore, when there is a solution, there are infinitely many solutions.

Proof. Suppose that $d = (a_1, a_2, \ldots, a_n)$ and $d|c$, we have many solutions. Let's use the mathematical induction.
For $n = 2$ we know that how we can find the solution of linear diophantine equation by Theorem 2.3.2.
Suppose that there are infinitely many solutions for the equation in $n = k$ variables, then we can write $a_1x_1 + a_2x_2 + \cdots + a_kx_k = c$ and $d|c$.
The original equation in $n = k + 1$ variables can be reduced to a linear diophantine equation in n variables. The equation in $n = k + 1$ variables; $a_1x_1 + a_2x_2 + \cdots + a_kx_k + a_{k+1}x_{k+1} = t$ and $d|t$ then, $t = dp$.
By Theorem 2.1.5., the set of linear combinations $a_kx_k + a_{k+1}x_{k+1}$ is the same as the set of multiplies of (a_k, a_{k+1}). So, for every integer p there are many solutions of the linear diophantine equations $a_kx_k + a_{k+1}x_{k+1} = (a_k, a_{k+1})p$. Then, the equation reduced to k variables.

$$a_1x_1 + a_2x_2 + \cdots + a_{k-1}x_{k-1} + (a_k, a_{k+1})p = c.$$

By Theorem 2.1.6. c is divisible by $(a_1, a_2, \ldots, a_{k-1}, (a_k, a_{k+1}))$, this gcd equals $(a_1, a_2, \ldots, a_k, a_{k+1})$.
By the inductive hypothesis, this equation has many solution (it is also a linear diophantine equation has n variables) because gcd of $a_1, a_2, \ldots, a_n, a_{n+1}$ divides c. We completed our proof and we see there are many solutions to the original equation. □

Let's illustrate the theorem:

Example 2.3.3. We will find the solutions of $4x + 8y + 5z = 7$
First we find $(4, 8) = 4$, then;
$(4, 8)(x + 2y) + 5z = 7$ and if we say $x + 2y = w$

$$4w + 5z = 7$$

$$5 = 4 \cdot 1 + 1$$

$$4 = 1 \cdot 4 + 0.$$

The $(4, 5) = 1$ and 1 divides 7, there are many solutions.

$$1 = 5 - 4 \cdot 1$$

$$w_0 = -1, z_0 = 1$$

Its general solution is

$$w = -7 + 5k$$

$$z = 7 - 4k.$$

Next we find x and y

$$x + 2y = -7 + 5k.$$

$(1, 2)|(-7 + 5k)$, the equation is solvable and the solution is

$$x = 1 \cdot (-7 + 5k) + 2p$$
$$y = 0 \cdot (-7 + 5k) - p$$
$$z = 7 - 4k$$

where $p \in \mathbb{Z}$ is another parameter.

$$k, p = 0, \pm 1, \pm 2, \ldots$$

If we want to solve in different way;

$$4x + 8y + 5z = 7$$
$$4x + (8, 5)(8y + 5z) = 7$$

Assume that $8y + 5z = t$

$$4x + t = 7$$

$x_0 = 0$ and $t_0 = 1$.
Then,

$$x = s$$
$$t = 7 - 4s$$

We said that $8y + 5z = t$ and we found $t = 7 - 4s$, so we can write $8y + 5z = 7 - 4s$.
$(8, 5)|7 - 4s$ so there is a solution.

$$8 = 5 \cdot 1 + 3$$
$$5 = 3 \cdot 1 + 2$$
$$3 = 2 \cdot 1 + 1$$
$$2 = 1 \cdot 2 + 0.$$

And by extended euclidean algorithm;

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ &= 3 - (5 - 3) \\ &= 2 \cdot 3 - 1 \cdot 5 \\ &= 2 \cdot (8 - 5) - 5 \\ &= 2 \cdot 8 - 3 \cdot 5. \end{aligned}$$

Hence we find $y_0 = 2, z_0 = -3$.

$$x = s$$

$$\begin{aligned} y &= 2 \cdot (7 - 4s) + 5m \\ &= 14 - 8s + 5m. \end{aligned}$$

$$\begin{aligned} z &= -3 \cdot (7 - 4s) - 8m \\ &= -21 + 12s - 8m. \end{aligned}$$

where s, m are the integers.
And then we have two different systems of equation with different parameters

$$\begin{aligned} x &= -7 + 5k + 2p, \\ y &= -p, \\ z &= 7 - 4k. \end{aligned}$$

and for the second system

$$\begin{aligned} x &= s, \\ y &= -8s + 5m, \\ z &= 12 - 8m. \end{aligned}$$

Let's find the s, m in terms of k, p from the two systems;
For x
$x = -7 + 5k + 2p$ and $x = s$.
Then

$$s = 5k + 2p - 7$$

For y we have;
$y = -p$ and $y = 14 - 8s + 5m$

$$-p = 14 - 8s + 5m$$

If we put $s = 5k + 2p - 7$ we get;

$$-p = 14 - 40k - 16p + 56 + 5m \Rightarrow m = \frac{15p - 70 + 40k}{5} = 3p + 8k - 14$$

and if we put these values(s and m)in the z equality,we will see;

$$z = 7 - 4k, z = -21 + 12s - 8m$$

Put the values of s and m in terms of k and p

$$7 - 4k = -21 + 12(-7 + 5k + 2p) - 8(3p - 14 + 8k)$$

Hence,we get

$$7 = 7$$

So,our equality is always true.
Now, we have

$$s = -7 + 5k + 2p$$
$$m = 3p - 14 + 8k.$$

We reduced the our equation system to two parameter as k and p.

2.4 Some Applications For Linear Diophantine Equations

Example 2.4.1. Clara wants to buy pizza and cola to her family. She has 400 SEK.

If we know that each pizza 57 SEK and each bottle of cola cost 22 SEK, how many pizzas and bottles of cola she can buy?

We can write the equation as the linear diophantine equations

$$57x + 22y = 400$$

Let's find the GCD of 57 and 22 using the euclidean algorithm;

$$57 = 22 \cdot 2 + 13$$
$$22 = 13 \cdot 1 + 9$$
$$13 = 9 \cdot 1 + 4$$
$$9 = 4 \cdot 2 + 1$$
$$4 = 1 \cdot 4 + 0.$$

So, the last non zero remiander 1 and $(57, 22) = 1$ and $1|400$, there are many solutions.

$$\begin{aligned}1 &= 9 - 4 \cdot 2 \\ &= 9 - 2 \cdot (13 - 9) \\ &= 3 \cdot 9 - 2 \cdot 13 \\ &= 3 \cdot (22 - 13) - 2 \cdot 13 \\ &= 3 \cdot 22 - 5 \cdot 13 \\ &= 3 \cdot 22 - 5 \cdot (57 - 2 \cdot 22) \\ &= 13 \cdot 22 - 5 \cdot 57.\end{aligned}$$

We can find $x_0^* = -5$ and $y_0^* = 13 \Rightarrow x_0 = 400 \cdot (-5) = -2000$ and $y_0 = 400 \cdot 13 = 5200$
We write the general solution;

$$x = -2000 + 22n$$

$$y = 5200 - 57n.$$

$x \geq 0$ and $y \geq 0$. Because x and y determine the number of pizzas and bottles of colas. That's why x and y can't be negative.
$5200 - 57n \geq 0$ then $5200 \geq 57n$, if divide both sides by 57, we find $n \leq 91$.
$-2000 + 22n \geq 0$, so $22n \geq 2000$, divide both sides by 22, we get $n \geq 90,9 \cong 91$, so $n = 91$.
If we put $n = 91$ in general solution we find $x = -2000 + (22 \cdot 91) = 2$ and $y = 5200 - (57 \cdot 91) = 13$, so she can buy 2 pizza and 13 bottles of cola.

Example 2.4.2. Assume that, there is discount for some stuffs in the restaurant and the pizza's price changed from 57 SEK to 55 SEK. How many pizzas and bottles of cola she can buy?

$$55x + 22y = 400$$

Using the euclidean algorithm;

$$55 = 22 \cdot 2 + 11$$

$$22 = 11 \cdot 2 + 0.$$

$(55, 22) = 11$ and 11 doesn't divide 400. So there is no solution.

Example 2.4.3. Peter wants to buy pets. He has 151 euros and he must choose at least one of each pet. The prices are; fishes 3 euro each, cats are 5 euro each, dogs are 10 euros each. How many fishes, cats and dogs he can buy?

$3x + 5y + 10z = 151$.
If we use the same method which have been used in Example 2.3.3, then we write
$(3, 5)3x + 5y + 10z = 151$ and $3x + 5y = v$.

$$v + 10z = 151$$

The general solutions are given by

$$v = 151 + 10t$$

$$z = -t.$$

And we assumed that $3x + 5y = v$ and then $3x + 5y = 151 + 10t$;
The general solution

$$x = 47 + 5k$$

$$y = 2 + 2t - 3k.$$

where $t, k \in \mathbb{Z}$.
x, y, z should be bigger than zero, so we can find the ranges for t and k.

$$47 + 5k > 0,$$

$$2 + 2t - 3k > 0,$$

$$-t > 0.$$

If we calculate the ranges, we find;

$$k > -10,$$

$$2t - 3k > -2,$$

$$t > 0.$$

Now, we should find the ranges. For example, consider $2t - 3k > -2$ and we know that t a is negative parameter. So, if we put $t = -1$ in $2t - 3k > -2$, it is equal to $(2 \cdot -1) - 3k > -2$ and $k < 0$. So, the ranges for k should be $-10 < k < 0$ and let's continue to process, if we choose $t = -2$, the inequality will be $k < 0$ again, and for $t = -3$, it will be $k < -2$ and if we continue that calculation when we reach $t = -16$, we will get $k < -10$ and it will be wrong, because k should be bigger than -10. So, range for t should be $-16 < t \leq -1$. And the ranges are;

$$-10 < k < 0,$$

$$-16 < t \leq -1.$$

If we choose $t = -14$, k can be only equal to -9, and if we put those values on the x, y, z equation, we find $x = 47+5(-9) = 2$, $y = 2+2(-14)-3(-9) = 1$ and $z = -(-14) = 14$. So he can buy 2 fishes, 1 cat and 14 dogs and he pays 151 euros. If we choose the t values according to range, then k depends on t.
We will find that how many solutions are there for these equations after the theorem for solving linear congruence in n variables.

3 Linear Congruence

3.1 Introduction to Congruence

Definition 3.1.1. $a, b, m \in \mathbb{Z}$ and such that $m > 0$ if $m|a-b$, we say that a is congruent to b modulo m. We denote it by

$$a \equiv b \pmod{m}$$

Example 3.1.1. $11 \equiv 3 \pmod 4$ and $43 \equiv 1 \pmod 6$
since
$4|(11-3)$ and $6|(43-1)$.

Theorem 3.1.1. If a and b are integers, then $a \equiv b \pmod m$ if and only if there is an integer k such that $a = b + mk$.

Proof. ($\Rightarrow$) We know that from the definition of congruence; if $a \equiv b \pmod m$, then $m|(a-b)$. Namely, $a - b = km \Rightarrow a = b + km$.

($\Leftarrow$) Assume that $a = b + km$, then $a - b = km$. Hence $m|a-b$, and this means $a \equiv b \pmod m$. □

Example 3.1.2. Suppose that $a = 185$, $b = 3$ and $m = 14$, then

$$185 = 3 + (14 \cdot 13).$$

It is equal to $3 = 185 - 14 \cdot 13$, it means $185 \equiv 3 \pmod{14}$.

Theorem 3.1.2. If a, b, c and m are integers such that $m > 0$, $d = (c, m)$ and $ac \equiv bc \pmod m$, then $a \equiv b \pmod{\frac{m}{d}}$.

Proof. If $ac \equiv bc \pmod m$, so $m|ac - bc$. Then, $m|c(a-b)$.
If m divide $c(a-b)$, then there is an integer like t and it can be written like $c(a-b) = mt$. Divide by d both sides, we got;

$$\frac{c(a-b)}{d} = \frac{mt}{d}$$

And we know from Theorem 2.1.1 if $d = (c, m)$; then $(\frac{c}{d}, \frac{m}{d}) = 1$. Hence, we can write $(\frac{c}{d})(a-b) = \frac{m}{d}t$ and $\frac{m}{d}$ is a multiple of $(a-b)$. Then, $\frac{m}{d}|(a-b)$. Namely, $a \equiv b \pmod{\frac{m}{d}}$ □

Example 3.1.3. $45 \equiv 3 \pmod 6$ and if write 45 as a multiple of 3, we get
$15 \cdot 3 = 3 \cdot 1 \pmod 6$, so if we consider for theorem $c = 3$, then $(3, 6) = 3$, we see that $\frac{45}{3} \equiv \frac{3}{3} \pmod{\frac{6}{3}}$ or $15 \equiv 1 \pmod 2$.

3.2 Linear Congruences

A linear congruence is an equation of the form $ax \equiv b \pmod{m}$. Solving this equation means identisfying which values of x satisfy it.

Theorem 3.2.1. Let $a, b, c \in \mathbb{Z}$ with a and b nonzero. If (x_0, y_0) is a solution to

$$ax + by = c$$

then x_0 is a solution to the associated congruence

$$ax \equiv c \pmod{m}$$

where $m = |b|$.

Conversely, if x_0 is a solution to the above congruence, then there is a y_0 such that (x_0, y_0) is a solution to the above diophantine equation.

Proof. For the first part of theorem, observe that b divides $(ax_0 - c)$. Thus m divides $(ax_0 - c)$.

For the second part of theorem, since x_0 solve the congruence, $m|(ax_0 - c)$. Thus $ax_0 - c$ is a multiple of b. Hence $ax_0 - c = y_0 b$ for some $y_0 \in \mathbb{Z}$. Then (x_0, y_0) solves the Diophantine equation. □

Example 3.2.1. Let us solve the diophantine equation

$$7x + 9y = 41 \tag{3}$$

We convert equation (3) to a congruence (mod 9) namely,

$$7x \equiv 41 \pmod{9} \tag{4}$$

which reduces to

$$7x \equiv 5 \pmod{9} \tag{5}$$

the unique solution of congruence (5) is given by

$$x \equiv 2 \pmod{9} \tag{6}$$

which we convert the equation

$$x = 2 + 9t \tag{7}$$

Note that $x_0 = 2$. Now $y_0 = [41 - 7 \cdot 2]|9 = 3$, so we have

$$y = 3 - 7t \tag{8}$$

To complete solution to the equation (3) is given by equations (7) and (8), where t is an arbitrary integer.

Example 3.2.2. Solve $7x \equiv 5 \pmod 9$ by using diophantine equation.
To find a solution, we need only obtain a solution of the linear diophantine equation $7x - 9y = 5$. The euclidean algorithm gives

$$9 = 7 \cdot 1 + 2$$

$$7 = 2 \cdot 3 + 1$$

$$3 = 3 \cdot 1 + 0.$$

By extended euclidean algorithm

$$\begin{aligned} 1 &= 7 - 2 \cdot 3 \\ &= 7 - 3 \cdot (9 - 7) \\ &= 4 \cdot 7 - 3 \cdot 9. \end{aligned}$$

Therefore a particular solution to the linear diophantine equation is

$$x_0 = 4$$

$$y_0 = 3.$$

The general solution is

$$x = 4 \cdot 5 + 9r$$

It means $x = 20 + 9r$, namely $x \equiv 20 \pmod 9$ which reduces to $x \equiv 2 \pmod 9$.

You can find more detail, look at [13].

Remark: When the refer to the numbers of solutions of $ax \equiv b \pmod m$, we mean the number of incongruent integers satisfying this congruence.

Theorem 3.2.2. The linear congruence $ax \equiv b \pmod m$ has a solution if and only if $d|b$, where $d = (a, m)$. If $d|b$, then it has d incongruent solutions modulo m.

Proof. We already known that the given congruence is equivalent to the linear diophantine equation$(ax - my = b)$. From Theorem 2.3.1, the diophantine equation can be solved if and only if $d|b$; also if it is solvable and x_0, y_0 are one specific solutions, then any other solution has the form

$$x = x_0 + \frac{m}{d} \cdot t, y = y_0 + \frac{a}{d} \cdot t$$

for some t.
Among the several integers satisfying the first of these formulas, consider those that result when t takes on the consecutive values, $t = 0, 1, 2, \cdots, d-1$:

$$x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, \cdots, x_0 + \frac{d-1}{d} \cdot m.$$

We claim that these integers are incongruent modulo m, and all other such integers x are congruent to some one of them. If it happened that

$$x_0 + \frac{m}{d} \cdot t_1 \equiv x_0 + \frac{m}{d} \cdot t_2 \pmod{m}$$

where $0 \leq t_1 < t_2 \leq d - 1$, then we would have

$$\frac{m}{d} \cdot t_1 \equiv \frac{m}{d} \cdot t_2 \pmod{m}$$

Now, $(\frac{m}{d}, m) = \frac{m}{d}$ and by Theorem 3.1.2 the factor $\frac{m}{d}$ cancel to arrive at the congruence

$$t_1 \equiv t_2 \pmod{d}$$

This shows that all values of set of incongruent solutions are by taking $x = x_0 + (\frac{m}{d}) \cdot t$, where t ranges with a complete system of residues modulo d. One set is given by $x = x_0 + \frac{m}{d} \cdot t$, where $t = 0, 1, 2, \cdots, d - 1$. □

Corollary 3.2.1. If $(a, m) = 1$, then the linear congruence $ax \equiv b \pmod{m}$ has a unique solution modulo m.

Proof. $(a, m) = 1$ and $(a, m)|b$. So, by Theorem 3.2.2, the congruence $ax \equiv b \pmod{m}$ has exactly $(a, m) = 1$ incongruent solution modulo m. □

Example 3.2.3. Consider the congruence $9x \equiv 30 \pmod{42}$. $(9, 42) = 3$ and 3 divides 42. And the Theorem 3.2.2 guarentees the existence of exactly 3 solutions, which are incongruent modulo 42. By inspection, one solution is found to be $x = 8$. Our analysis tells us that three solutions are as follows:

$$x \equiv 8 + (\frac{42}{3}) \cdot t \equiv 8 + 14 \cdot t.$$

where $t = 0, 1, 2$ and then $x \equiv 8, 22, 36$.

Example 3.2.4. $35x \equiv 9 \pmod{13}$, if we want to solve that congruence, we will find by inspection $x = 1$. According to Corollary 3.2.1 if $(a, m) = 1$,there is a unique solution and for that example $(35, 13) = 1$,then we have a unique solution. Let's prove it. Suppose, the general solutions are $x_1 = 1 + 13 \cdot t_1$

and $x_2 = 1+13\cdot t_2$. Suppose two solutions of this form are congruent modulo 13. If there is a unique solution ; it should be $x_1 = x_2 \pmod{13}$.

$$x_1 \equiv x_2 \pmod{13}$$

$$1 + 13 \cdot t_1 \equiv 1 + 13 \cdot t_2 \pmod{13}$$

$$13 \cdot t_1 \equiv 13 \cdot t_2 \pmod{13}.$$

If divide both sides by 13

$$t_1 \equiv t_2 \pmod{1}.$$

Hence x_1 always congruent to x_2. We have a unique solution.

Definition 3.2.1. Given an integer a with $(a, m) = 1$, a solution of $ax \equiv 1 \pmod{m}$ is called an inverse of a modulo m.

Example 3.2.5. Assume that $a = 20$ and $m = 11$, $20x \equiv 1 \pmod{11}$, by trial and error $x = 5 \pmod{11}$, 5 and all integers congruent to 5 and modulo 11, are inverse of 20 modulo 11.

Theorem 3.2.3. The linear congruence $a_1x_1 + \cdots + a_nx_n \equiv b \pmod{m}$ has solutions if and only if $d = (a_1, \cdots, a_n, m)|b$.

Proof. $\Rightarrow$ Suppose that $x_1, \cdots, x_n, y_0$ are solutions for the equation. Then $a_1x_1 + \cdots + a_nx_n - my_0 = b$. Since $d|x_1, \cdots, x_n, m$, we get $d|a_1x_1 + \cdots + a_nx_n - my_0$, then $d|b$.

$\Leftarrow$ Suppose that $d|b$. Then $d = bk$ where k is an integer. We know by theorem 2.1.5. $d = (a_1, \cdots, a_n, m)$ can be written as a linear combination of $a_1, \cdots, a_n, m$. So there exist $e, \cdots, v, w \in \mathbb{Z}$ with $a_1e + \cdots + a_nv - mw = d$. If we multiply both of sides with k, we get $a_1ek + \cdots + a_nvk - mwk = dk = b$. So the equation $a_1x_1 + \cdots + a_nx_n - my = b$ has a solution, namely $x_1 = ek, \cdots, x_n = vk$. □

Theorem 3.2.4. The congruence $a_1x_1 + \cdots + a_nx_n \equiv b \pmod{m}$,$m_1 \neq 0$ with $(a_1, \cdots, a_n, m) = d$ and $d|b$ has $d \cdot |m|^{n-1}$ incongruent solutions.

Proof. Because $a_1x_1 + \cdots + a_nx_n \equiv b \pmod{m} \Leftrightarrow a_1x_1 + \cdots + a_nx_n \equiv b \pmod{-m}$, we can consider $m > 0$. We use induction.
For $n = 1$, we have proved by Theorem 3.2.2.
Suppose that it is true for $n - 1$. Let's prove that it is true for n. Let the congruence with n variables $a_1x_1 + \cdots + a_nx_n \equiv b \pmod{m}$, namely $a_1x_1 + \cdots + a_{n-1}x_{n-1} \equiv b - a_nx_n \pmod{m}$. If we consider that x_n is fixed, the congruence $a_1x_1 + \cdots + a_{n-1}x_{n-1} \equiv b - a_nx_n \pmod{m}$ is a congruence with $n - 1$ variables. To have solutions we must have $(a_1, \cdots, a_{n-1}, m) = s$

and $s|b - a_n x_n \Leftrightarrow b - a_n x_n \equiv 0 \pmod{s}$.
It is clear, $s|m \Rightarrow \frac{m}{s} \in \mathbb{Z}$, therefore we can multiply the previous congruence with $\frac{m}{s}$. It results that

$$\frac{ma_n}{s} x_n \equiv \frac{mb}{s} \pmod{s\frac{m}{s}} \tag{9}$$

which has $(\frac{ma_n}{s}, s\frac{m}{s}) = \frac{m}{s}(a_n, (a_1, \cdots, a_{n-1}, m)) = \frac{m}{s}(a_1, \cdots, a_{n-1}, a_n, m)$ and $\frac{m}{s} \cdot d$ incongruent solutions for x_n. Let x_n^0 be a particular solution of the congruence (9). It results that $a_1 x_1 + \cdots + a_{n-1} x_{n-1} \equiv b - a_n x_n^0 \pmod{m}$ has, assimilate to the induction's hypothesis, $s \cdot m^{n-2}$ incongruent solutions for $x_1, \cdots, x_{n-1}$ where $s = (a_1, \cdots, a_{n-1}, m)$. Therefore the congruence $a_1 x_1 + \cdots + a_{n-1} x_{n-1} + a_n x_n \equiv b \pmod{m}$ has $\frac{m}{s} \cdot d \cdot s \cdot m^{n-2} = d \cdot m^{n-1}$ incongruent solutions for $x_1, \cdots, x_{n-1}, x_n$. □

You can look also [14].

Corollary 3.2.2. If we have linear congruence in two variables $ax + by \equiv c \pmod{m}$ and if $(a, b, m)|c$, there is a solution and we have $d \cdot m$ distinct solutions.

Proof. Applying the above Theorem 3.2.4 with $n = 2$, we saw that there are $m^{2-1} \cdot d$, namely $m \cdot d$ incongruent solutions. □

Example 3.2.6. Consider the linear congruence $2x + 6y \equiv 4 \pmod{12}$.
First, we must check $(2, 6, 12)|4$ and $2|4$, then we have a solution.
We can solve the congruence above as linear diophantine equation in three variables.
The given equation is equivalent to

$$2x + 6y - 12z = 4$$

for some z.
$(2, 6)x + 3y - 12z$ and if we say to $w = x + 3y$.
We get;
$2w - 12z = 4$ and simply $w - 6z = 2$, now we got the diophantine equation in two variables.
The general solution is;

$$w = 8 + 6k$$
$$z = 1 + k$$

where $k \in \mathbb{Z}$.
And then;

$$x + 3y = 8 + 6k$$

The general solution;

$$x = 8 + 3t$$

$$y = 2k - t$$

where $t \in \mathbb{Z}$.
So, we found our general solution for x and y.
And $t = 0, 1, \cdots, 11$ will produce incongruent values of x modulo 12. We found $y = 2k - t$ and in the linear diophantine it is equal to $3y = 3 \cdot (2k - t) = 6k - 3t$. So if we choose $k = 2$,it will be equal to 12 and it repeat itself in y mod 12. So, the all possibilities for y mod 12 by letting $k = 0, 1$. In this question we have 12 t values and 2 k values, so we find 24 solutions. It is also true with theorem, $m = 12$ and $d = 2$, we have $12 \cdot 2 = 24$ incongruent solutions.
All incongruent solutions mod 12 are;

$$x = 8 + 3t$$

$$y = 2k - t$$

where $t = 0, 1, \cdots, 11$ and $k = 0, 1$.

Example 3.2.7. And also,we can calculate the number of solution in Example 2.4.3. Remember the question; $3x + 5y + 10z = 151$ and if we write as a linear congruence $3x + 5y \equiv 1 \pmod{|-10|}$. If we use the theorem 3.2.4 for that question, $a = 3$, $b = 5$, $c = 1$ and $m = 10$. Since $(3, 5, 10)|1$, then there is a solution. The number of solution $m^{n-1} \cdot d$. In our question $m = 10$ and $d = 1$ and we have two variables. $10^{2-1} \cdot 1 = 10$, so we have 10 incongruent solution.We found that the general solution

$$x = 47 + 5k$$

And we can write for x modulo 10

$$x = 7 + 5k$$

$$y = 2 + 2t - 3k.$$

Hence $k = 0, 1$ produce incongruent values of x mod 10. Because if $k = 2$, it will repeat itself in mod 10. And $t = 5$, it will be equal to 10 and repeat itself. That's why, the all possibilities for y mod 10 $t = 0, 1, 2, 3, 4$. The incongruent solutions are;

$$x = 7 + 5k$$

$$y = 2 + 2t - 3k$$

where $k = 0, 1$ and $t = 0, 1, 2, 3, 4$.
Then, we have two k values and five t values. We find $5 \cdot 2 = 10$ values. It confirms the Theorem 3.2.4.

4 Conclusion

As has been explained above, linear diophantine equation in two variables can be solved by euclidean algorithm and extended euclidean algorithm. When the solution has been searched for linear diophantine equation in two variables, as $ax + by = c$, first should be checked $(a, b)|c$. If $(a, b)|c$, then there is a solution. To find the solution for linear diophantine equation in n variables, as $a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$, again should be checked $(a_1, a_2, \cdots, a_n)|c$ by mathematical induction.
The linear congruences and linear diophantine equations are relatable. As seen above that the linear congruences in one variable $ax \equiv b \pmod{m}$ can be written $ax - my = b$ as a linear diophantine equation in two variables. We can generalize the method to more variable. The number of solutions can be found to

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n \equiv b \pmod{m}$$

as $|m|^{n-1}d$.

References

[1] J.Knig, *Einleitung, Algebraischen Grszen* Leipzig, 1903, 347-460

[2] Th.Schnemann, *Jour fr.Math* 19, 1839, 292

[3] M.Fekete, *Mathès Phys.Lapok*, Budapest, 17, 1908, 328-49

[4] Leonard Eugene Dickson,*History Of The Theory Of Numbers*, Chelsea Publishing Company, New York, 1992

[5] Gareth A.Jones and J.Mary Jones, *Elemantary Number Theory*, Springer-Verlag London Limited, Great Britain, 1998

[6] Joseph H.Silverman, *A Friendly Introduction To Number Theory*, Precentice-Hall,Inc., New Jersey, 2001

[7] H.E.Rose, *A Course In Number Theory*,Clarendon Press, New York, 1994

[8] William Judson Leveque, *Topics In Number Theory*, Addison-Wesley Publishing Company, USA, 1958

[9] Ivan Niven, Herbert S.Zuckerman, *An Introduction To The Theory Of Numbers*, John Wiley Sons,Inc., USA, 1967

[10] W.Narkiewicz, *Number Theory*, PWN(Polish Scientific Publishers), Warszawa, 1977

[11] Kenneth H.Rosen, *Elemantary Number Theory And Its Applications*, Greg Tobin, USA, 2005

[12] Peter J.Eccles, *An Introduction To Mathematical Reasoning:Numbers,Sets And Functions*, Cambridge University Press, United Kingdom, 1997

[13] Neville Robins, *Beginning Number Theory*, Jones And Barlett Publishers, USA, 2006

[14] http://arxiv.org/ftp/math/papers.com

[15] http://www.math.cornell.edu

[16] http://public.csusm.edu

[17] http://math.buffalostate.edu

Linnæus University
School of Computer Science, Physics and Mathematics

SE-351 95 Växjö / SE-391 82 Kalmar
Tel +46-772-28 80 00
dfm@lnu.se
Lnu.se/dfm