ALGORITHMS FOR SOLVING LINEAR CONGRUENCES
AND SYSTEMS OF LINEAR CONGRUENCES

Florentin Smarandache
University of New Mexico
200 College Road
Gallup, NM 87301, USA
E-mail: smarand@unm.edu

In this article we determine several theorems and methods for solving linear congruences and systems of linear congruences and we find the number of distinct solutions. Many examples of solving congruences are given.

§1. Properties for solving linear congruences.

Theorem 1. The linear congruence \( a_1 x_1 + \ldots + a_n x_n \equiv b \pmod{m} \) has solutions if and only if \((a_1,\ldots,a_n,m)\mid b\).

Proof:

\[ a_1 x_1 + \ldots + a_n x_n \equiv b \pmod{m} \iff a_1 x_1 + \ldots + a_n x_n - my = b \]

is a linear equation which has solutions in the set of integer numbers \(\iff (a_1,\ldots,a_n,-m)\mid b \iff (a_1,\ldots,a_n,m)\mid b \).

If \( m = 0 \), \( a_1 x_1 + \ldots + a_n x_n \equiv b \pmod{0} \iff a_1 x_1 + \ldots + a_n x_n = b \) has solutions in the set of integer numbers \(\iff (a_1,\ldots,a_n)\mid b \iff (a_1,\ldots,a_n,0)\mid b \).

Theorem 2. The congruence \( ax \equiv b \pmod{m} \), \( m \neq 0 \), with \((a,m)=d\mid b\), has \(d\) distinct solutions.

The proof is different of that from the number’s theory courses: \( ax \equiv b \pmod{m} \iff ax - my = b \) has solutions in the set of integer numbers; because \((a,m)=d\mid b\) it results: \( a = a_1 d, \quad m = m_1 d, \quad b = b_1 d \) and \((a_1,m_1)=1\), \( a_1 dx - m_1 dy = b_1 d \iff a_1 x - m_1 y = b_1 \). Because \((a_1,m_1)=1\) it results that the general solution of this equation is \( \begin{cases} x = m_1 k_1 + x_0 \\ y = a_1 k_1 + y_0 \end{cases} \), where \( k_1 \) is a parameter and \( k_1 \in \mathbb{Z} \), and where \( (x_0,y_0) \) constitutes a particular solution in the set of integer numbers of this equation; \( x = m_1 k_1 + x_0, \quad k_1 \in \mathbb{Z}, \quad m_1, x_0 \in \mathbb{Z} \Rightarrow x \equiv m_1 k_1 + x_0 \pmod{m} \). We’ll assign values to \( k_1 \) to find all the solutions of the congruence.

It is evident that \( k_1 \in \{0,1,2,\ldots,d-1,d+1,\ldots,m-1\} \) which constitutes a complete system of residues modulo \( m \).

(Because \( ax \equiv b \pmod{m} \iff ax \equiv b \pmod{-m} \), we suppose \( m > 0 \).)

Let \( D = \{0,1,2,\ldots,d-1\}; \quad D \subseteq M, \quad \forall \alpha \in M, \quad \exists \beta \in D: \alpha \equiv \beta \pmod{d}\mid m_1 \)

(because \( D \) constitutes a complete system of residues modulo \( d \)).

It results that \( am_1 = \beta m_1 \pmod{m_1} \); because \( x_0 = x_0 \pmod{m_1} \), it results: \( m_1 \alpha + x_0 \equiv m_1 \beta + x_0 \pmod{m} \).
Therefore \( \forall \alpha \in M, \exists \beta \in D : m_\alpha \alpha + x_\beta \equiv m_\beta + x_\alpha (\mod m) \); thus \( k_1 \in D \).

\( \forall \gamma, \delta \in D, \gamma \neq \delta (\mod d) \mid m_1 \Rightarrow \gamma m_1 \neq \delta m_1 (\mod dm_1) ; m_1 \neq 0 \). It results that \( m_\gamma \gamma + x_\delta \equiv m_\delta + x_\gamma (\mod m) \) is false, that is, we have exactly \( \text{card} D = d \) distinct solutions.

**Remark 1.** If \( m = 0 \), the congruence \( ax \equiv b (\mod 0) \) has one solution if \( a \mid b \); otherwise it does not have solutions.

**Proof:**

\( ax \equiv b (\mod 0) \iff ax = b \) has a solution in the set of integer numbers \( \iff a \mid b \).

**Theorem 3.** (A generalization of the previous theorem)

The congruence \( a_1 x_1 + \ldots + a_n x_n \equiv b (\mod m) \), \( m_1 \neq 0 \), with \((a_1, \ldots, a_n, m) = d \mid b \) has \( d \cdot |m|^{-1} \) distinct solutions.

**Proof:**

Because \( a_1 x_1 + \ldots + a_n x_n \equiv b (\mod m) \iff a_1 x_1 + \ldots + a_n x_n \equiv b (\mod m) \), we can consider \( m > 0 \).

The proof is done by induction on \( n \) the number of variables.

For \( n = 1 \) the affirmation is true in conformity with theorem 2.

Suppose that it is true for \( n - 1 \). Let’s proof that it is true for \( n \).

Let the congruence with \( n \) variables \( a_1 x_1 + \ldots + a_n x_n \equiv b (\mod m) \), \( a_1 x_1 + \ldots + a_{n-1} x_{n-1} \equiv b - a_n x_n (\mod m) \). If we consider that \( x_n \) is fixed, the congruence \( a_1 x_1 + \ldots + a_{n-1} x_{n-1} \equiv b - a_n x_n (\mod m) \) is a congruence with \( n - 1 \) variables. To have solutions we must have \((a_1, \ldots, a_{n-1}, m) = d \mid b - a_n x_n \iff b - a_n x_n \equiv 0 (\mod \delta) \).

Because \( \delta \mid m \Rightarrow \frac{m}{\delta} \in \mathbb{Z} \), therefore we can multiply the previous congruence with \( \frac{m}{\delta} \). It results that

\[
\frac{m a_n}{\delta} x_n \equiv \frac{m b}{\delta} (\mod \frac{m}{\delta})
\]

(*)

which has \( \left( \frac{m a_n}{\delta}, \frac{m}{\delta} \right) = \frac{m}{\delta} (a_n, \delta) = \frac{m}{\delta} (a_n, (a_1, \ldots, a_{n-1}, m)) = \frac{m}{\delta} (a_1, \ldots, a_{n-1}, a_n, m) \frac{m}{\delta} \cdot d \) distinct solutions for \( x_n \). Let \( x_0 \) be a particular solution of the congruence (*). It results that \( a_1 x_1 + \ldots + a_{n-1} x_{n-1} \equiv b - a_n x_n^0 (\mod m) \) has, conform to the induction’s hypothesis, \( \delta \cdot m^{n-2} \) distinct solutions for \( x_n^0 \) where \( \delta = (a_1, \ldots, a_{n-1}, m) \).

Therefore the congruence \( a_1 x_1 + \ldots + a_{n-1} x_{n-1} + a_n x_n \equiv b (\mod m) \) has \( \frac{m}{\delta} \cdot d \cdot \delta \cdot m^{n-2} = \frac{m}{\delta} \cdot d \cdot m^{n-1} \) distinct solutions for \( x_n^0 \) and \( x_n \).

§2. A Method for Solving Linear Congruences

Let’s consider the congruence \( a_1 x_1 + \ldots + a_n x_n \equiv b (\mod m), m \neq 0 \),
\(a_i \equiv a'_i (\text{mod } m)\) and \(b \equiv b' (\text{mod } m)\) with \(0 \leq a'_i, \ b \leq m - 1\) (we made the nonrestrictive hypothesis \(m > 0\)). We obtain:

\[a_i x_i + \ldots + a_n x_n \equiv b (\text{mod } m) \iff a'_i x_i + \ldots + a'_n x_n \equiv b' (\text{mod } m),\]

which is a linear equation; when it is resolved in \(\mathbb{Z}\) it has the general solution:

\[x_i = \alpha_{i1} k_1 + \ldots + \alpha_{in} k_n + \gamma_i, \quad \ldots \]

\[x_n = \alpha_{n1} k_1 + \ldots + \alpha_{nm} k_n + \gamma_n, \quad y = \alpha_{n+1,1} k_1 + \ldots + \alpha_{n+1,n} k_n + \gamma_{n+1}, \]

\(k_j\) being parameters \(\in \mathbb{Z}, \ j = 1, n, \ \alpha_{ij}, \gamma_i \in \mathbb{Z},\) constants, \(i = 1, n + 1, \ j = 1, n\).

Let’s consider \(\alpha_{ij} = \alpha_{ij}' (\text{mod } m)\) and \(\gamma_i = \gamma_i' (\text{mod } m)\) with \(0 \leq \alpha_{ij}'\), \(\gamma' \leq m - 1\); \(i = 1, n + 1, \ j = 1, n\).

Therefore

\[x_i = \alpha_{i1}' k_1 + \ldots + \alpha_{in}' k_n + \gamma_i' (\text{mod } m) \quad \ldots \quad x_n = \alpha_{n1}' k_1 + \ldots + \alpha_{nm}' k_n + \gamma_n' (\text{mod } m)\]

\(k_j\) being parameters \(\in \mathbb{Z}, \ j = 1, n, \ \alpha_{ij}, \gamma_i \in \mathbb{Z},\) constants, \(i = 1, n + 1, \ j = 1, n\).

Let’s consider \((\alpha_{ij}, \ldots, \alpha_{ij}, m) = d_j, \ j = 1, n\). We’ll prove that for \(k_j\) it would be sufficient to only give the values \(0, 1, 2, \ldots, \frac{m}{d_j} - 1\); for \(k_j = \frac{m}{d_j} - 1 + \beta'\) with \(\beta' \geq 1\) we obtain

\[k_j = \frac{m}{d_j} + \beta\] with \(\beta \geq 0; \ \beta', \beta \in \mathbb{Z}.\)

\[\alpha_{ij}' k_j = \alpha_{ij}' d_j k_j = \alpha_{ij}' m + \alpha_{ij}' d_j \beta \equiv \alpha_{ij}' d_j \beta (\text{mod } m);\]

we denoted \(\alpha_{ij}' = \alpha_{ij}' d_j\) because \(d_j | \alpha_{ij}'.\)

We make the notation \(m = d_j m_j, \ m_j = \frac{m}{d_j}.\)

Let’s consider \(\eta \in \mathbb{Z}, \ 0 \leq \eta \leq m - 1\) such that \(\eta = \alpha_{ij}' d_j \beta (\text{mod } d_j m_j);\) it results \(d_j | \eta.\)

Therefore \(\eta = d_j \gamma\) with \(0 \leq \gamma \leq m_{j-1}\) because we have that

\[d_j \gamma \equiv \alpha_{ij}' d_j (\text{mod } d_j m_j),\]

which is equivalent to \(\gamma \equiv \alpha_{ij}' \beta (\text{mod } m_j).\)

Therefore \(\forall k_j \in \mathbb{N}, \ \exists \gamma \in \{0, 1, 2, \ldots, m_{j-1}\}: \alpha_{ij}' k_j \equiv d_j \gamma (\text{mod } m);\)

analogously, if the parameter \(k_j \in \mathbb{Z}.\) Therefore \(k_j\) takes values from \(0, 1, 2, \ldots\) to at most \(m_j - 1; \ j = 1, n.\)

Through this parameterization for each \(k_j\) in (**), we obtain the solutions of the linear congruence. We eliminate the repetitive solutions. We obtain exactly \(d_j | m_j\) distinct solutions.

**Example 1.** Let’s resolve the following linear congruence:
\[2x + 7y - 6z \equiv -3 \pmod{4}\]

Solution: \(7 \equiv 3 \pmod{4}, -6 \equiv 2 \pmod{4}, -3 \equiv 1 \pmod{4}\).

It results that \(2x + 3y + 2z \equiv 1 \pmod{4}\); \((2, 3, 2, 4) = 111\) therefore the congruence has solutions and it has \(1 \cdot 4^{3-1} = 16\) distinct solutions.

The equation \(2x + 3y + 2z - 4t = 1\) resolved in integer numbers, has the general solution:

\[
\begin{align*}
  x & = 3k_1 - k_2 - 2k_3 - 1 \equiv 3k_1 + 3k_2 + 2k_3 + 3 \pmod{4} \\
  y & = -2k_1 + 1 \equiv 2k_1 + 1 \pmod{4} \\
  z & = k_2 \pmod{4}
\end{align*}
\]

\(k_j\) are parameters \(\in \mathbb{Z}, j = 1, 3\).

(We did not write the expression for \(t\), because it doesn’t interest us).

We assign values to the parameters. \(k_j\) takes values from 0 to at most \(m_j - 1\);

\(k_3\) takes values from 0 to \(m_3 - 1 = \frac{m}{d_3} - 1 = \frac{4}{2} - 1 = 1\);

\[
k_3 = 0 \Rightarrow \begin{cases} 
  x \equiv 3k_1 + 3k_2 + 3 \pmod{4} \\
  y \equiv 2k_1 + 1 \pmod{4} \\
  z \equiv k_2 \pmod{4}
\end{cases}
\]

\[
k_3 = 1 \Rightarrow \begin{pmatrix} 
  3k_1 + 3k_2 + 1 \\
  2k_1 + 1 \\
  k_2
\end{pmatrix}
\]

\(k_1\) takes values from 0 to at most 3.

\[
k_1 = 0 \Rightarrow \begin{pmatrix} 
  3k_2 + 3 \\
  1 \\
  k_2
\end{pmatrix}, \quad \begin{pmatrix} 
  3k_2 + 1 \\
  1 \\
  k_2
\end{pmatrix}; \quad k_1 = 1 \Rightarrow \begin{pmatrix} 
  3k_2 + 2 \\
  3 \\
  k_2
\end{pmatrix}, \quad \begin{pmatrix} 
  3k_2 \\
  3 \\
  k_2
\end{pmatrix};
\]

for \(k_2 = 2\) and 3 we obtain the same expressions as for \(k_1 = 1\) and 0.

\(k_2\) takes values from 0 to at most 3.

\[
k_2 = 0 \Rightarrow \begin{pmatrix} 
  3 \\
  1 \\
  0
\end{pmatrix}, \quad \begin{pmatrix} 
  1 \\
  1 \\
  0
\end{pmatrix}, \quad \begin{pmatrix} 
  2 \\
  0 \\
  0
\end{pmatrix}; \quad k_2 = 2 \Rightarrow \begin{pmatrix} 
  1 \\
  3 \\
  2
\end{pmatrix}, \quad \begin{pmatrix} 
  0 \\
  3 \\
  2
\end{pmatrix};
\]

\[
k_2 = 1 \Rightarrow \begin{pmatrix} 
  1 \\
  1 \\
  1
\end{pmatrix}, \quad \begin{pmatrix} 
  1 \\
  1 \\
  1
\end{pmatrix}, \quad \begin{pmatrix} 
  3 \\
  3 \\
  3
\end{pmatrix}; \quad k_2 = 3 \Rightarrow \begin{pmatrix} 
  1 \\
  1 \\
  3
\end{pmatrix}, \quad \begin{pmatrix} 
  0 \\
  3 \\
  3
\end{pmatrix}, \quad \begin{pmatrix} 
  2 \\
  3 \\
  3
\end{pmatrix};
\]

which represent all distinct solutions of the congruence.
Remark 2. By simplification or amplification of the congruence (the division or multiplication with a number \( \neq 0, 1, -1 \)), which affects also the module, we lose solutions, respectively foreign solutions are introduced.

Example 2.

1) The congruence \( 2x - 2y \equiv 6 \pmod{4} \) has the solutions
\[
\begin{pmatrix}
3 \\
0
\end{pmatrix}, \begin{pmatrix}
1 \\
0
\end{pmatrix}, \begin{pmatrix}
0 \\
1
\end{pmatrix}, \begin{pmatrix}
2 \\
1
\end{pmatrix}, \begin{pmatrix}
1 \\
2
\end{pmatrix}, \begin{pmatrix}
3 \\
2
\end{pmatrix}, \begin{pmatrix}
2 \\
3
\end{pmatrix}, \begin{pmatrix}
0 \\
3
\end{pmatrix};
\]

2) If we would simplify by 2, we would obtain the congruence \( x - y \equiv 3 \pmod{2} \), which has the solutions \( \begin{pmatrix}
1 \\
0
\end{pmatrix}, \begin{pmatrix}
0 \\
1
\end{pmatrix} \); therefore we lose solutions.

3) If we would amplify with 2, we would obtain the congruence \( 4x - 4y \equiv 12 \pmod{4} \), which has the solutions:
\[
\begin{pmatrix}
3 \\
0
\end{pmatrix}, \begin{pmatrix}
5 \\
0
\end{pmatrix}, \begin{pmatrix}
7 \\
0
\end{pmatrix}, \begin{pmatrix}
1 \\
1
\end{pmatrix}, \begin{pmatrix}
4 \\
1
\end{pmatrix}, \begin{pmatrix}
6 \\
1
\end{pmatrix}, \begin{pmatrix}
0 \\
1
\end{pmatrix}, \begin{pmatrix}
2 \\
1
\end{pmatrix}, \begin{pmatrix}
3 \\
2
\end{pmatrix}, \begin{pmatrix}
6 \\
2
\end{pmatrix}, \begin{pmatrix}
0 \\
2
\end{pmatrix}, \begin{pmatrix}
2 \\
3
\end{pmatrix}, \begin{pmatrix}
4 \\
3
\end{pmatrix}, \begin{pmatrix}
6 \\
3
\end{pmatrix}, \begin{pmatrix}
1 \\
4
\end{pmatrix}, \begin{pmatrix}
3 \\
4
\end{pmatrix}, \begin{pmatrix}
5 \\
4
\end{pmatrix}, \begin{pmatrix}
0 \\
5
\end{pmatrix}, \begin{pmatrix}
2 \\
5
\end{pmatrix}, \begin{pmatrix}
4 \\
5
\end{pmatrix}, \begin{pmatrix}
6 \\
5
\end{pmatrix}, \begin{pmatrix}
1 \\
6
\end{pmatrix}, \begin{pmatrix}
3 \\
6
\end{pmatrix}, \begin{pmatrix}
5 \\
6
\end{pmatrix}, \begin{pmatrix}
7 \\
6
\end{pmatrix}, \begin{pmatrix}
2 \\
7
\end{pmatrix}, \begin{pmatrix}
4 \\
7
\end{pmatrix}, \begin{pmatrix}
6 \\
7
\end{pmatrix}, \begin{pmatrix}
0 \\
7
\end{pmatrix};
\]

therefore we introduce foreign solutions.

Remark 3. By the division or multiplication of a congruence with a number which is prime with the module, without dividing or multiplying the module, we obtain a congruence which has the same solutions with the initial one.

Example 3. The congruence \( 2x + 3y \equiv 2 \pmod{5} \) has the same solutions as the congruence \( 6x + 9y \equiv 6 \pmod{5} \) as follows:
\[
\begin{pmatrix}
0 \\
1
\end{pmatrix}, \begin{pmatrix}
2 \\
1
\end{pmatrix}, \begin{pmatrix}
3 \\
2
\end{pmatrix}, \begin{pmatrix}
4 \\
3
\end{pmatrix}, \begin{pmatrix}
0 \\
4
\end{pmatrix}.
\]

§2. PROPERTIES FOR SOLVING SYSTEMS OF LINEAR CONGRUENCES.

In this paragraph we will obtain some interesting theorems regarding the systems of congruences and then a method of solving them.

Theorem 1. The system of linear congruences:
\[
\begin{align*}
a_1x_1 + \ldots + a_nx_n & \equiv b \pmod{m_i}, \quad i = 1, r,
\end{align*}
\]
has solutions if and only if the system of linear equations:
\[
\begin{align*}
a_1x_1 + \ldots + a_nx_n &= b, \\
&\quad i = 1, r,
\end{align*}
\]
The system of congruences \( a_i x \equiv b_i \pmod{m_i} \), \( m_i \neq 0 \), \( i = 1, r \) admits solutions if and only if: \( (a_i, m_i) \mid b_i \), \( i = 1, r \) and \( (a_j, m_j) \mid a_j b_j - a_j b_i \), \( i, j = 1, r \).

**Proof:**

\[ \forall i = 1, r, \quad a_i x \equiv b_i \pmod{m_i} \iff \forall i = 1, r, \quad a_i x = b_i + m_i y_i, \quad y_i \text{ being unknowns } \in \mathbb{Z}; \] these Diophantine equations, taken separately, have solutions if and only if \( (a_i, m_i) \mid b_i \), \( i = 1, r \).

\[ \forall i, j = 1, r, \quad \text{from: } a_i x = b_i + y_i m_i \mid a_j \quad \text{and} \quad a_j x = b_j + y_j m_j \mid a_i, \quad \text{we obtain:} \]

\[ a_i a_j \cdot x = a_i b_j + a_j m_i y_i = a_j b_i + a_j m_i y_j, \quad \text{Diophantine equations which have solution if and only if} \]

\( (a_j, m_j) \mid a_i b_j - a_j b_i, \quad i, j = 1, r. \)

**Consequence.** (We obtain a simpler form for the theorem from p. 20 of [1]). The system of congruences \( x \equiv b_i \pmod{m_i}, \quad m_i \neq 0, \quad i = 1, r \) has solutions if and only if

\[ (m_i, m_j) \mid b_i - b_j, \quad i, j = 1, r. \]

**Proof:**

From theorem 2, \( a_i = 1, \quad \forall i = 1, r \) and \( (1, m_i) = 1 \mid b_i, \quad i = 1, r. \)

**§4. METHOD FOR SOLVING SYSTEMS OF LINEAR CONGRUENCES**

Let’s consider the system of linear congruences:

\[ a_{i1} x_1 + a_{i2} x_2 + \ldots + a_{in} x_n \equiv b_i \pmod{m_i}, \quad i = 1, r \]

the system’s matrix rank being \( r < n, \quad a_{ij}, b_i, m_i \in \mathbb{Z}, \quad m_i \neq 0, \quad i = 1, r, \quad j = 1, n. \)

According to §1 from this chapter, we can consider:

\[
0 \leq a_{ij} \leq |m_i| - 1, \quad 0 \leq b_i \leq |m_i| - 1, \quad \forall i = 1, r, \quad j = 1, n.
\]

From the theorem 1 and the remark 1 it results that, to solve this system of congruences is equivalent with solving in integer numbers the system of equations:

\[ a_{i1} x_1 + \ldots + a_{in} x_n - m_i y_i = b_i, \quad i = 1, r, \]

the system’s matrix rank being \( r < n. \)

Using the algorithm from [2], we obtain the general solution of this system:
\[
\begin{align*}
\begin{cases}
  x_1 &= \alpha_1 k_1 + \ldots + \alpha_{i-1} k_{i-1} + \alpha_i k_i + \beta_i, \\
  x_n &= \alpha_1 k_1 + \ldots + \alpha_{n-1} k_{n-1} + \alpha_n k_n + \beta_n, \\
  y_1 &= \alpha_{n+1} k_1 + \ldots + \alpha_{n+i-1} k_{n+i-1} + \alpha_{n+i} k_{n+i} + \beta_{n+i}, \\
  y_r &= \alpha_{n+r+1} k_1 + \ldots + \alpha_{n+r+n} k_{n+r+n} + \beta_{n+r+n},
\end{cases}
\end{align*}
\]
\[\alpha_{hj}, \beta_h \in \mathbb{Z} \text{ and } k_j \text{ are parameters } \in \mathbb{Z} .\]

Let’s consider \( m = \{m_1, \ldots, m_r\} > 0 \); because the variables \( y_1, \ldots, y_r \) don’t interest us, we’ll retain only the expressions of \( x_1, \ldots, x_n \).

Therefore:

(5) \[ x_i = \alpha_i k_1 + \ldots + \alpha_i k_i + \beta_i, \quad i = 1, n \]
and again we can suppose that

(**) \[ 0 \leq \alpha_{hj} \leq m - 1, \quad 0 \leq \beta_h \leq m - 1, \quad h = 1, n, \quad j = 1, n. \]

We have: \( x_i \equiv \alpha_i k_1 + \ldots + \alpha_i k_i + \beta_i (\text{mod } m), \quad i = 1, n \). Evidently \( k_j \) takes the values of at most the integer numbers from 0 to \( m - 1 \). Conform to the same observations from §1 from this chapter, for \( k_j \) it is sufficient to give only the values \( 0, 1, 2, \ldots, \frac{m}{d_j} - 1 \) where

(***) \[ d_j = \left( \alpha_{ij}, \ldots, \alpha_{nj}, m \right), \text{ for any } j = 1, n. \]

By the parameterization of \( k_1, \ldots, k_n \) in (5) we obtain all the solutions of the system of linear congruence (1); \( k_j \) takes at most the values \( 0, 1, 2, \ldots, \frac{m}{d_j} - 1 \); we eliminate the repeating solutions.

**Remark 2.** The considerations (*) and (**), and (***) have the roll of making the calculation easier, to reduce the computational volume. This algorithm of solving the linear congruence works also without these considerations, but it is more difficult.

**Example.** Let’s solve the following system of linear congruences:

(6) \[ \begin{cases}
  3x + 7y - z \equiv 2 (\text{mod } 2) \\
  5y - 2z \equiv 1 (\text{mod } 3)
\end{cases} \]

**Solution:** The system of linear congruences (6) is equivalent with:

(7) \[ \begin{cases}
  x + y + z \equiv 0 (\text{mod } 2) \\
  2y + z \equiv 1 (\text{mod } 3)
\end{cases} \]

which is equivalent with the system of linear equations:

(8) \[ \begin{cases}
  x + y + z - 2t_1 = 0 \\
  2y + z - 3t_2 = 1
\end{cases} \]

\( x, \ y, \ z, \ t_1, \ t_2 \) unknowns \( \in \mathbb{Z} \)

This has the general solution (see [2]):
\[
\begin{align*}
  x & = -2k_1 + 2k_2 + 3k_3 + 1 \\
  y & = k_1 - 3k_3 - 1 \\
  z & = k_1 \\
  t_1 & = k_2 \\
  t_2 & = k_3
\end{align*}
\]

where \( k_1, k_2, k_3 \) are parameters \( \in \mathbb{Z} \).

The values of \( t_1 \) and \( t_2 \) don’t interest us; \( m = [2, 3] = 6 \). Therefore:

\[
\begin{align*}
  x & \equiv 4k_1 + 2k_2 + 3k_3 + 1 \pmod{6} \\
  y & \equiv k_1 + 3k_3 + 5 \pmod{6} \\
  z & \equiv k_1 \pmod{6}
\end{align*}
\]

\( k_3 \) takes values from 0 to \( 6 \) \((3, 3, 0, 6) - 1 = 1 \); \( k_2 \) from 0 to 2; \( k_1 \) from 0 to at most 5.

\[ k_3 = 0 \Rightarrow \begin{cases} 
  x \equiv 4k_1 + 2k_2 + 1 \pmod{6} \\
  y \equiv k_1 + 5 \pmod{6} \\
  z \equiv k_1 \pmod{6}
\end{cases} \]

\[ k_3 = 1 \Rightarrow \begin{cases} 
  4k_1 + 2k_2 + 4 \\
  k_1
\end{cases} \]

\[ k_2 = 0, 1, 2 \Rightarrow \begin{cases} 
  4k_1 + 1 \\
  k_1 + 5 \\
  k_1 + 2 \\
  k_1
\end{cases} \]

\[ k_1 = 0, 1, 2, 3, 4, 5 \Rightarrow \]

\[
\begin{pmatrix}
  1 & 4 & 3 & 0 & 5 & 2 & 5 & 2 & 1 & 4 & 3 & 0 \\
  5 & 2 & 5 & 2 & 0 & 3 & 0 & 3 & 0 & 3 & 0 \\
  0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\
  3 & 0 & 5 & 2 & 1 & 4 & 1 & 4 & 3 & 0 & 5 & 2 \\
  1 & 4 & 1 & 4 & 2 & 5 & 2 & 5 & 2 & 5 & 2 \\
  2 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 3 & 3 \\
  5 & 2 & 1 & 4 & 3 & 0 & 3 & 0 & 5 & 2 & 1 & 4 \\
  3 & 0 & 3 & 0 & 4 & 1 & 4 & 1 & 4 & 1 & 4 & 1 \\
  4 & 4 & 4 & 4 & 4 & 5 & 5 & 5 & 5 & 5 & 5 & 5
\end{pmatrix}
\]

which constitute the 36 distinct solutions of the system of linear congruences (6).

**REFERENTES:**


[Published in “Gamma”, Year X, Nos. 1-2, October 1987.]