SIMULTANEOUS DIOPHANTINE EQUATIONS AND CONSISTENCY

T. Srinivasa Rao, Asst. Professor, AKNU, Rajahmundry, A.P., India.

Dr. Thamma Koteswara Rao	***D.Vasubabu***	***Dr.B.Venkateswarlu***
Asst.Professor, Humanities	***Asst.Professor, Dept. of Math***	***Asst. Professor, Dept. of Math***
UCE, JNTU, Narsaraopeta	***Krishna University***	***Vikram Simhapuri University***
A.P., India	***Machilipatnam, AP***	***College, Kavali, A.P., India***

Key Words: linear congruences, greatest common divisor (GCD), Relatively prime, incongruent solutions, Euclidean ring, Euclidean algorithm, Division Algorithm, determinant, Augmented matrix, reduction of matrix, modular (mod)

***Introduction*:**
A Euclidean domain R in which a, b &$m \neq 0$, the division algorithm can be rephrased as $ax \equiv b \; mod \; m$ holds for every $x \in E$ whenever $gcd(a, m) = p|b$ for some p in E. extending the role of x to more variables, this will become a Diophantine equation whose solutions can be one or more depending on the greatest common divisor 'gcd' of a and b. this is summarized in the theorem following. As the method of augmented matrix to solve a system of non-homogeneous linear equations, in the case of system of Diophantine equations also, the augmented matrix model under the Gauss elimination technique has been introduced. The three variable Diophantine equations or the system of linear congruences are solved and a generalization has been brought out to a finite number of variables or in particular n variables.

Abstract: Euclidean algorithm and Division algorithm are used to bring out a solution for the linear congruence and the necessary and sufficient condition for a congruence relation to possess a solution is extended to the system of congruences and unlike Chinese reminder theorem, those followed the Gauss elimination method and the conditions for possessing the solutions for the linear system have been explored.

Discussion 1:
Definition: A system of n congruence relations in n variables all are congruent modulo m is said to be consistent if they have at least one solution set.

Theorem: a linear Diophantine equation $ax + by = c$ has a solution if and only if $d\,|c$ where $d =$ gcd (a, b). …… 1.1
That is, if x_0, y_0 are integers or forming a solution to the Diophantine equation, then all other solutions are $x = x_0 + \left(\frac{b}{d}\right)t; y = y_0 - (\frac{a}{d})t$ for some integer t.
$d = \gcd(a, b) \Rightarrow a = dp, b = dq, p, q \epsilon \mathbb{Z}$
$ax_0 + b\,y_0 = c \Rightarrow d(px_0 + dq\,y_0) = c \Rightarrow d|c$ …… 1.2

The linear Diophantine equation $ax + by = c$ has a solution if and only if $\gcd(a, b) = d\,|c$. If x_0, y_0 is one solution of this equation, then all other solutions are of the form $x = x_0 + \left(\frac{b}{d}\right)t; y = y_0 + \left(\frac{a}{d}\right)t$ for an arbitrary integer t.
To get the 1st solution of the Diophantine equation, let us apply the Euclidean algorithm and find p and q such that $d = ap + bq$ where p and q bear the opposite signs. Since d

 https://doi.org/10.5281/zenodo.15047204

divides c, suppose $\frac{c}{d} = k$, then it can explicitly be written as $dk = akp + bkq$ or $c = ax_0 + by_0$ solves the Diophantine equation. …… 1.3

Euclidean algorithm & Division algorithm: if a and b are elements in a Euclidean ring R, then there exists two elements q and r in R and gcd $(a, b) = d$ such that $d = ax + by$ for some elements x and y in R obtained through a sequence of division algorithms applications between a and b in which the last non zero residue is d.
$a = bq_1 + r_1$, either $r_1 = 0$ or $d(r_1) < d(b)$ and $q_1, r_1 \epsilon$ R
But, $r_1 \neq 0 \Longrightarrow$
$b = r_1q_2 + r_2$ and $q_2, r_2 \epsilon$ R, $r_2 \neq 0 \Longrightarrow$
$r_1 = r_2q_3 + r_3$ and $q_3, r_3 \epsilon$R, $r_3 \neq 0 \Longrightarrow$
$\dots\dots\dots\dots\dots\dots$
$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}$ and $q_3, r_3 \epsilon$R, $r_{n-1} \neq 0 \Longrightarrow$
$r_{n-2} = r_{n-1}q_n + r_n$, and $q_n, r_n \epsilon$R, $r_n \neq 0 \Longrightarrow$
$r_{n-1} = r_nq_{n+1} + r_{n+1}$ where $r_{n+1} = 0$ and $q_{n+1}, r_{n+1} \epsilon$ R
While $r_{n+1} = 0$, it follows r_n is the last non zero remainder in the division algorithm procedure exists in R which is the greatest common divisor of a and b.
Going backwards to the above procedure as

$$\begin{aligned} d = r_n &= r_{n-2} - r_{n-1}q_n \\ &= r_{n-2}(1 + q_{n-1}q_n) - r_{n-3}q_n \\ &= (r_{n-4} - r_{n-3}q_{n-2})(1 + q_{n-1}q_n) - r_{n-3}q_n \\ &= (1 + q_{n-1}q_n)r_{n-4} - (q_{n-2} + q_{n-2}q_{n-1}q_n + q_n)r_{n-3} \\ &\dots\dots\dots\dots\dots \\ &= K_1b - K_2a \quad \text{where } K_1 \& K_2 \epsilon R \text{ in view of (1.3).} \end{aligned}$$

$Kd = (KK_1)a + (-KK_2)b$ or $ax + by = c$ forming the Diophantine equation.
So, a Diophantine equation $ax + by = c$ has a solution when $c = Kd$ for some integer K.
Once the Diophantine equation is established, then it can otherwise be written in the form $ax - c = b(-y)$ or $|ax - c$.
See that y already bears a negative sign in the above procedure and so, $-y = s$ a positive integer. This division leads to the definition (1.18).
So, a linear congruence $ax \equiv c \; mod \; b$ if and only if the Diophantine equation $ax + by = c$ has a solution.
In particular, if $\gcd(a, b) = n|c$, then there will be n incongruent solutions modulo.
They are $x_0, x_0 + \frac{b}{n}, x_0 + \frac{2b}{n}, \dots, x_0 + \frac{(n-1)b}{n}$ forming the reduced residue system. …… 1.4
Note that if $\gcd(a, b) = 1$ then there is a unique solution to $ax \equiv c \; mod \; b$ leading to $ax \equiv 1 mod \; b$ has the solution called the inverse of $a \; mod \; b$. …… 1.5

Theorem: the system of linear congruences
$ax + by \equiv r \; mod \; n$
$cx + dy \equiv s \; mod \; n$ has unique solution $modulo \; n$ whenever $\gcd(ad - bc, n) = 1$……1.6

A linear Diophantine equation leads to the linear congruence.
For a suitable element $x \epsilon$R, if $m|ax - b$ for some a, b & $m \neq 0$ in R, then we say that the linear congruence $ax \equiv b \; mod \; m$ has the solution $x \epsilon$R (the Euclidean ring of integers)

Elimination method of solving the system of linear congruences a Gauss perspective:

 https://doi.org/10.5281/zenodo.15047204

$a_{11}x_1 + a_{12}x_2 + a_{13}x_3 \equiv b_1 mod\ m$ 1.6.1
$a_{21}x_1 + a_{22}x_2 + a_{23}x_3 \equiv b_2 mod\ m$ 1.6.2
$a_{31}x_1 + a_{32}x_2 + a_{33}x_3 \equiv b_3 mod\ m$ 1.6.3

To satisfy the basic condition of a congruence relation to possess a solution in each of the above three relations,
$\gcd(a_{11}, a_{12}, a_{13}, m)\ |b_1; \gcd(a_{21}, a_{22}, a_{23}, m)|b_2; \gcd(a_{31}, a_{32}, a_{33}, m)\ |b_3$ simultaneously. Then it may be continued in the following lines.
$(a_{11}x_1 + a_{12}x_2 + a_{13}x_3)a_{23} \equiv b_1a_{23} mod\ m$
$(a_{21}x_1 + a_{22}x_2 + a_{23}x_3)a_{13} \equiv b_2a_{13} mod\ m$
These equations give
$a_{11}a_{23} - a_{21}a_{13} = c_{11}; a_{12}a_{23} - a_{13}a_{22} = c_{12};\ d_1$ such that
$c_{11}x_1 + c_{12}x_2 \equiv d_1 mod\ m$ 1.6.4
Similarly,
$(a_{11}x_1 + a_{12}x_2 + a_{13}x_3)a_{33} \equiv b_1a_{33} mod\ m$ 1.6.5
$(a_{31}x_1 + a_{32}x_2 + a_{33}x_3)a_{13} \equiv b_3a_{13} mod\ m$ 1.6.6
From these, taking
$a_{11}a_{33} - a_{31}a_{13} = c_{21}; a_{12}a_{33} - a_{13}a_{32} = c_{22};\ b_1a_{33} - b_3a_{13} = d_2$ leading to
$c_{21}x_1 + c_{22}x_2 \equiv d_2 mod\ m$ 1.6.7
Further, to isolatex_2,
$(c_{11}x_1 + c_{12}x_2)c_{22} \equiv d_1c_{22} mod\ m$ 1.6.8
$(c_{21}x_1 + c_{22}x_2)c_{12} \equiv d_2c_{12} mod\ m$ 1.6.9
From these, putting $c_{11}c_{22} - c_{21}c_{12} = e_1; d_1c_{22} - d_2c_{12} = f_1$
$e_1x_1 \equiv f_1 mod\ m$ 1.6.10
Observe that
$e_1 = (a_{11}a_{23} - a_{21}a_{13})(a_{12}a_{33} - a_{13}a_{32}) - (a_{11}a_{33} - a_{31}a_{13})(a_{12}a_{23} - a_{13}a_{22}) \neq 0$ and $f_1 = (a_{12}a_{33} - a_{13}a_{32})(b_1a_{23} - b_2a_{13}) - (a_{12}a_{23} - a_{13}a_{22})(b_1a_{33} - b_3a_{13})$
This congruence relation (1.6.10) has a solution if and only if
$\gcd(e_1, m) = g_1$ and $g_1|f_1$ by (1.3).
$x_1^{(1)} = x_1$ is one solution obtained as in theorem (1.3), then $x_1^{(2)} = x_1^{(1)} + \frac{m}{g_1}$;
$x_1^{(3)} = x_1' + \frac{2m}{g_1}$; ...,..., $x_1^{(g_1-1)} = x_1^{(1)} + \frac{(g_1-1)m}{g_1}$ is the set of other solutions of (1.6.10) forming the reduced residue system modulo m or (1.5) holds.
...... 1.6.11
(1.6.4) and (1.6.7) now become $h_{1i}x_2 \equiv j_{1i}\ mod\ m, 1 \le i \le g_1 - 1$ 1.6.12
These $g_1 - 1$ congruence relations have solutions $x_{2i}^{(1)} = x_2$ if and only if $g_{2i} = \gcd(h_{1i}, m)|j_{1i}, 1 \le i \le g_1 - 1$
Another set of reduced residue system modulo m for each $1 \le i \le g_1 - 1$ that satisfy (1.6.12) is $x_{2k}^{(2)} = x_{2k}^{(1)} + \frac{2m}{g_{2i}}$; ...,...; $x_{2k}^{(g_{2i}-1)} = x_{2k}^{(1)} + \frac{(g_{2i}-1)m}{g_{2i}}$ whenever $x_{2k}^{(1)}$ is one solution, $1 \le k \le g_{2i} - 1$ 1.6.13
(1.6.11) and (1.6.13) jointly allow $(g_{2i} - 1)(g_1 - 1)$ linear congruences of the form $r_{1t}x_3 \equiv s_{1t}\ mod\ m; 1 \le t \le (g_{2i} - 1)(g_1 - 1); 1 \le i \le g_1 - 1$ 1.6.14
This linear congruence has a solution if and only if $g_{3u} = \gcd(r_{1t}, m)\ |s_{1t}$;
$1 \le t \le (g_{2i} - 1)(g_1 - 1); 1 \le i \le g_1 - 1$
The incongruent solutions (1.6.11) and (1.6.14) exist only in the case of
$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = 0$ and otherwise there is the unique solution suitable from the available incongruent solutions.

 https://doi.org/10.5281/zenodo.15047204

$5x + 8y + 12z \equiv 1 \, mod \, 14$
$9x + 3y + 11z \equiv 9 \, mod \, 14$
$6x + 12y + 13z \equiv 9 \, mod \, 14$ …… 1.6.15
This system can immediately be reduced to
$3x + 10y \equiv 1 \, mod \, 14$
$9x + 5y \equiv 4 \, mod \, 14$
This results in $11y \equiv 13 \, mod \, 14$ whose unique solution is $y = 5$
On substitution, another relation $3x \equiv 7 \, mod \, 14$ results in $x = 7$
Using these in any of the given relations, it follows $12z \equiv 10 \, mod \, 14$ which has its first solution $z = 2$ and the incongruent solution $z = 9$
But, the determinant of the coefficient matrix is not zero leading to a unique solution. This is satisfied by $x = 7; y = 5; z = 9$ as the unique solution.

2. Augmented matrix method to solve the linear system of Congruences in Gauss perspective:
$a_{11}x_1 + a_{12}x_2 + a_{13}x_3 \equiv b_1 mod \, m$ …… 2.1
$a_{21}x_1 + a_{22}x_2 + a_{23}x_3 \equiv b_2 mod \, m$ …… 2.2
$a_{31}x_1 + a_{32}x_2 + a_{33}x_3 \equiv b_3 mod \, m$ …… 2.3

$$\left\langle \begin{array}{ccc|c} a_{11} & a_{12} & a_{13} & b_1 \\ a_{21} & a_{22} & a_{23} & b_2 \\ a_{31} & a_{32} & a_{33} & b_3 \end{array} \right\rangle \equiv \mathbf{0} \, mod \, m$$

$$\left. \begin{array}{l} a_{11}R_2 - a_{21}R_1 \\ a_{11}R_3 - a_{31}R_1 \end{array} \right) \approx$$

$$\left\langle \begin{array}{ccc|c} a_{11} & a_{12} & a_{13} & b_1 \\ a_{11}a_{21} - a_{21}a_{11} & a_{11}a_{22} - a_{21}a_{12} & a_{11}a_{23} - a_{21}a_{13} & a_{11}b_2 - a_{21}b_1 \\ a_{11}a_{31} - a_{31}a_{11} & a_{11}a_{32} - a_{31}a_{12} & a_{11}a_{33} - a_{31}a_{13} & a_{11}b_3 - a_{31}b_1 \end{array} \right\rangle$$
$\equiv \mathbf{0} \, mod \, m$

$$\approx \left\langle \begin{array}{ccc|c} a_{11} & a_{12} & a_{13} & b_1 \\ 0 & c_{22} & c_{23} & d_2 \\ 0 & c_{32} & c_{33} & d_3 \end{array} \right\rangle \equiv \mathbf{0} \, mod \, m \qquad [3]$$

where $c_{22} = a_{11}a_{22} - a_{21}a_{12}; c_{23} = a_{11}a_{23} - a_{21}a_{13}; c_{32} = a_{11}a_{32} - a_{31}a_{12}$
$c_{33} = a_{11}a_{33} - a_{31}a_{13}; d_2 = a_{11}b_2 - a_{21}b_1;\ d_3 = a_{11}b_3 - a_{31}b_1$
Again performing $c_{22}R_3 - c_{32}R_2) \approx$

$$\approx \left\langle \begin{array}{ccc|c} a_{11} & a_{12} & a_{13} & b_1 \\ 0 & c_{22} & c_{23} & d_2 \\ 0 & 0 & e_{33} & f_3 \end{array} \right\rangle \equiv \mathbf{0} \, mod \, m \text{ where } e_{33} = c_{22}c_{33} - c_{32}c_{23} \text{ and}$$

$f_3 = c_{22}d_3 - c_{32}d_2$ …… 2.4
The given system of linear congruences has unique solution provided $\gcd(e_{33}, m) \,|f_3$. Otherwise, the congruence system is inconsistent.
On the other hand, if $e_{33} = 0$ & $f_3 = km$ for some integer k, then the system has incongruent solutions.
If $e_{33} \neq 0, m \nmid e_{33}$ & $f_3 = 0$, then $z_1 = \mathrm{k} \in \mathbb{Z}$; are the infinitely many solutions
$z = z_1 + \frac{rf_3}{\gcd(e_{33},m)}$ ……2.5
and $c_{22}y \equiv (d_2 - c_{23}k) mod \, m$ …… 2.6
This again has the solution provided $\gcd(c_{22}, m) \,| d_2 - c_{23}km$

 https://doi.org/10.5281/zenodo.15047204

Otherwise, the congruence system is inconsistent.

If $\gcd(c_{22}, m) > 1$, then there will be $\gcd(c_{22}, m)$ number of incongruent solutions $y = y_1 + \frac{nd_2}{\gcd(c_{22},m)}$,$1 \leq n \leq \gcd(c_{22}, m)$ for (2.6.) 2.7

Using (2.5) and (2.7) in (2.1), it gives

$$a_{11}x \equiv \left(b_1 - a_{12}\left[y_1 + \frac{nd_2}{\gcd(c_{22},m)}\right] - a_{13}\left[z_1 + \frac{rf_3}{\gcd(e_{33},m)}\right]\right) mod\ m \qquad \text{...... 2.8}$$

This congruence has a solution if and only if

$$\gcd(a_{11}, m)\ |(b_1 - a_{12}\left[y_1 + \frac{nd_2}{\gcd(c_{22},m)}\right] - a_{13}\left[z_1 + \frac{rf_3}{\gcd(e_{33},m)}\right])$$

If $\gcd(a_{11}, m) = 1$, then (1.6.5) has unique solution x_1.

If $\gcd(a_{11}, m) > 1$, there will be $x = x_1 + \frac{tb_1}{\gcd(a_{11},m)}$; $1 \leq t \leq \gcd(a_{11}, m)$

...... 2.9

Note that $ax \equiv b\ mod\ p_1$; $ax \equiv b\ mod\ p_2$ where p_1 and p_2 are relatively prime (1.6), then $ax \equiv b\ mod\ p_1p_2$ 2.10

The above results can be extended to n simultaneous congruences.

References:

1. On congruences for the traces of powers of some matrices
AV Zarekya – Proceedings of Steklov Institute of Mathematics, 2008 – Springer
2. The solutions of a system of linear congruences
RC Hildner – 1930 – etd.ohiolink.edu
3. A method of congruent type for linear systems with conjugate normal coefficient matrices
M Ghasemi Kamalvand, KD ikramov – Computational Mathematics and Mathematical Physics 49, 203 – 216, 2009
4. Congruences of a square matrix and its transpose
RA Horn, VV Sergeichuk, Linear Algebra and its Applications, 2004, Elsevier
5. Linear congruences in a general arithmetic
HL Olson – Annals of Mathematics, 1926 – JSTOR

6. https://arxiv.org/pdf/math/0702488

 https://doi.org/10.5281/zenodo.15047204