International Journal of
Mathematics And its Applications
ISSN: 2347-1557

Int. J. Math. And Appl., **11(1)**(2023), 125–130
Available Online: http://ijmaa.in

Solving System of Linear Congruences - Flow charts

K. Suvarna[1,*], P. V. Prasada Rao[2]

[1]*Department of Mathematics, D. K. Government College for Women (A), Nellore, Andhra Pradesh, India*
[2]*Department of Mathematics, University College, V.S. University, Kavali, Andhra Pradesh, India*

Abstract

Euclidean algorithm and Division algorithm for solving the system of linear congruence and fixing the necessary and sufficient condition for the system of congruence relation to possess a solution is established for any number of variables other than the Chinese reminder theorem, that continued on the basis of Gauss elimination method/Gauss Seidel method have been explored in the paper titled simultaneous Diophantine equations and consistency. The approach has been given a algorithm in the present discussion.

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

1. Introduction

A Euclidean domain R in which $a, b \& m \neq 0$, the division algorithm can be rephrased as $ax \equiv b \bmod m$ holds for every $x \in E$ whenever $\gcd(a, m) = p \mid b$ 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.

*Corresponding author (tsr.math@aknu.edu.in)

2. Main Results

Discussion 1

Definition 2.1. *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 2.2. *A linear Diophantine equation $ax + by = c$ has a solution if and only if $d \mid c$ where*

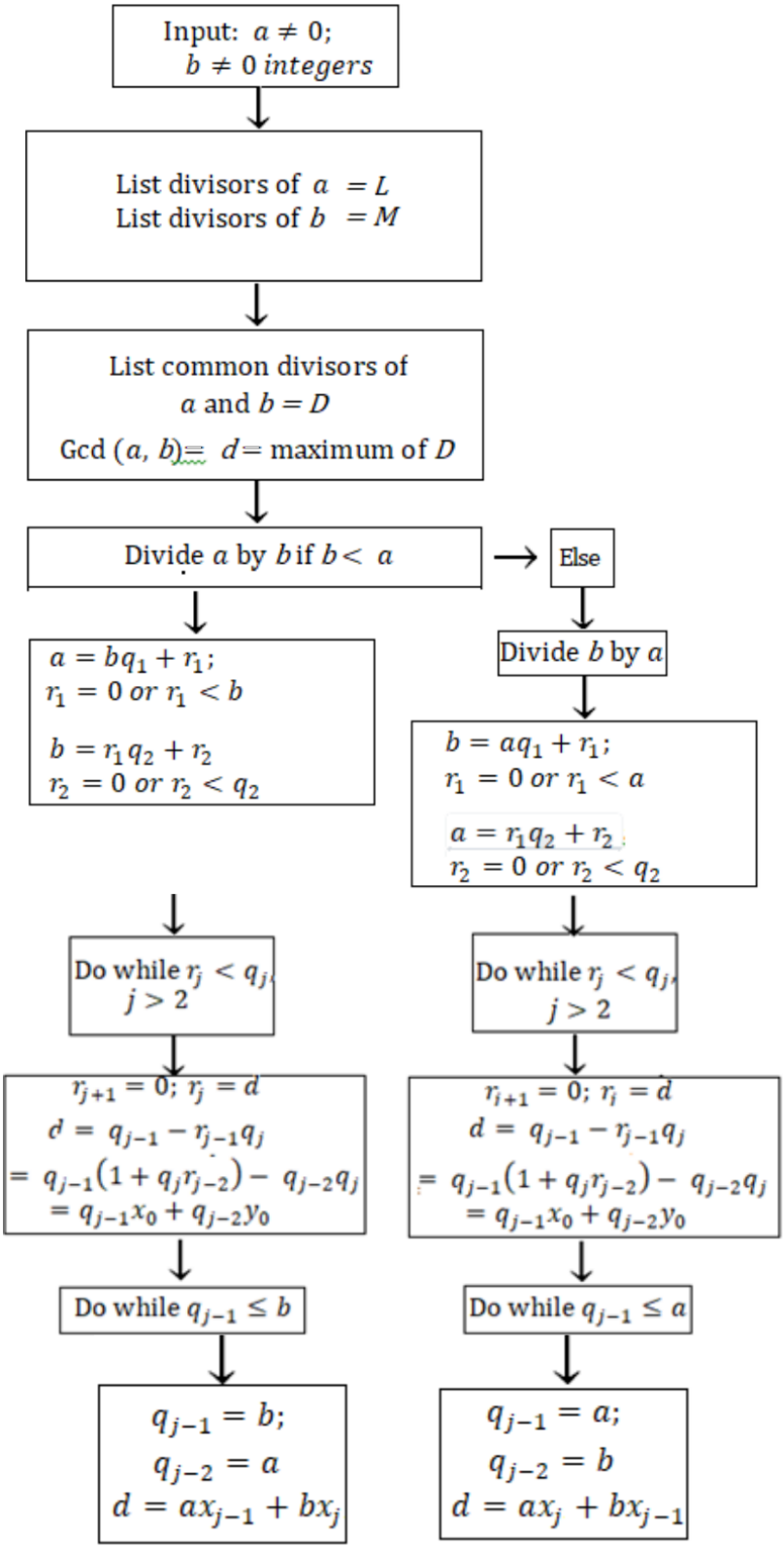
$$d = \gcd(a, b) \tag{1}$$

That is, if x_0, y_0 are integers or forming a solution to the Diophantine equation, then all other solutions are $x = x_0 + \left(\frac{b}{d}\right) t; y = y_0 - \left(\frac{a}{d}\right) t$ for some integer t.

$$\begin{gathered} d = \gcd(a, b) \Rightarrow a = dp, b = dq, p, q \in \mathbb{Z} \\ ax_0 + by_0 = c \Rightarrow d\,(px_0 + dqy_0) = c \Rightarrow d \mid c \end{gathered} \tag{2}$$

The linear Diophantine equation $ax + by = c$ has a solution if and only if $\gcd(a, b) = d \mid c$. 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 1^{st} 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 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.

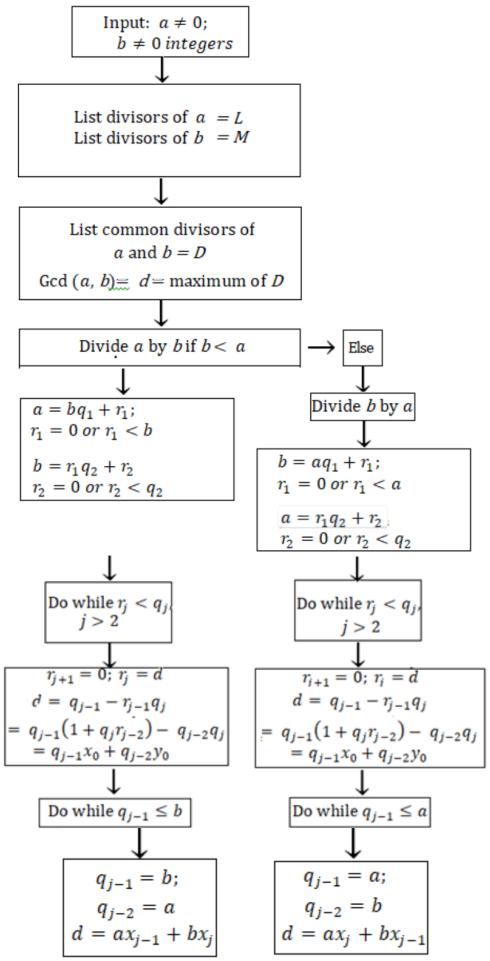
Flow chart 1: writing the greatest common divisor GCD d of a and b as a linear combination $d = ax_{j-1} + bx_j$ when $b < a$ and $d = ax_j + bx_{j-1}$ when $b > a$



2.1 Discussion 2

The gcd of a and b is d, when m divides d, there is a solution to the linear congruence $ax \equiv b \bmod m$ from the introduction. So, $\frac{m}{d} = k$ for some integer k that is used to increase the congruence relation $d = ax + by$ as $m = akx + bky$ in which a, k, y are known. So, x is obtained from this relation which is the solution of the congruence.

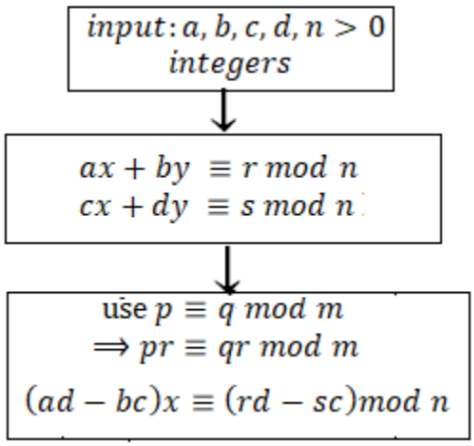
Flow chart 2:

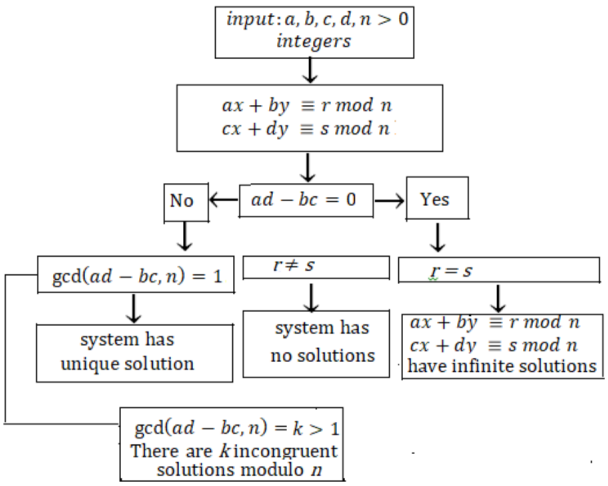


Discussion 3

The discussion 1 and 2 are used to extend the argument to 2 congruences in 2 variables and putting the conditions $ad - bc \neq 0$ into it as the necessary condition, the two variable congruence relations can be reduced to one variable congruence. Using the flow chart 2, the one variable congruence can be solved which in turn help to evaluate the other variable.

Flow chart 3:

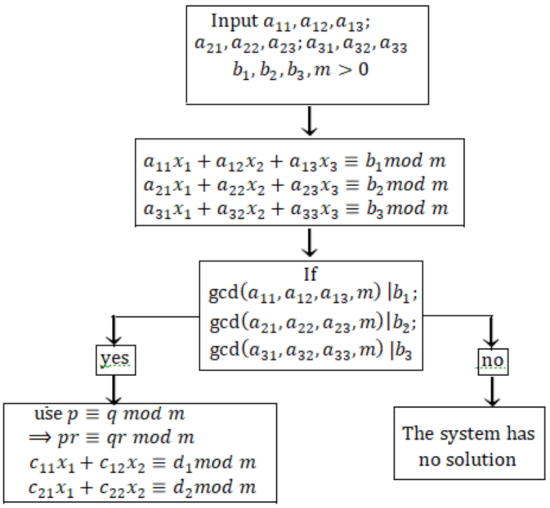




Discussion 4

Extending the above discussion to the three variable system of three linear congruences and putting the necessary conditions, the three variable congruences can be reduced to two variable congruences and using the discussion 3 that can be solved in the said necessary conditions, this new system again can be reduced to one variable congruence that ultimately can be solved using the necessary condition in discussion 2. So, in the retreating manner, the remaining two variables can be found.

Flow chart 4:



References

[1] A. V. Zarelua, *On congruences for the traces of powers of some matrices*, Proceedings of Steklov Institute of Mathematics, 236(2008), 78-98.

[2] R. C. Hildner, The solutions of a system of linear congruences, (1930).

[3] M. Ghasemi Kamalvand and Kh. D. Ikramov, *A method of congruent type for linear systems with conjugate-normal coefficient matrices*, Computational Mathematics and Mathematical Physics, 49(2009), 203-216.

[4] Roger A. Horn and Vladimir V. Sergeichuk, *Congruences of a square matrix and its transpose*, Linear Algebra and its Applications, 389(2004), 347-353.

[5] Horace L. Olson, *Linear Congruences in a General Arithmetic*, Annals of Mathematics, 28(1/4)(1926 - 1927), 237-244. .