RP-77: AN ALGORITHMIC FORMULATION OF SOLVING LINEAR CONGRUENCE OF PRIME AND COMPOSITE MODULUS OF DEGREE ONE

Prof. B M Roy

Head
Department of Mathematics
Jagat Arts, Commerce & I H P Science College, Goregaon
Dist. Gondia, M. S., INDIA. Pin: 441801
(Affiliated to R T M Nagpur University, Nagpur)

***Abstract*: In this paper, various methods of solving a linear congruence of prime modulus is discussed. It is also found that when modulus is comparatively large, then the existed methods become impractical and finding solutions is not easy. But the proposed method gives the solutions easily in a short time. The proposed method is time-saving. Formulation makes the finding solutions easy. This is the merit of the paper.**

***Keywords*: Division algorithm, Euclidean algorithm, linear congruence, Modular Inverse, Prime modulus, Residue system.**

INTRODUCTION

A congruence of the type: $ax \equiv b\ (mod\ m)\ with\ a \not\equiv 0\ (mod\ m)$, is called a linear congruence of degree one [3]. If m is a composite positive integer, then the congruence is called linear congruence of composite modulus but if $m = p$, a prime positive integer, then it is called a linear congruence of prime modulus. Some linear congruence have unique solution and some has many solutions and some others have no solutions [1].

$e.g. 20x \equiv 4\ (mod\ 30)$ has no solution. This proves that the solvability condition is must for solving linear congruence.

Linear congruence is an essential part of Elementary Number Theory and it is studied with great interest. A system of linear congruence is solved by using the famous theorem, known as Chinese Remainder Theorem (CRT) [3].

LITERATURE-REVIEW

Linear congruence is a part of study in number Theory. Some methods are mentioned for solutions in the author's Book &in the book of Zukerman [2] & [3]. Residue- method is a popular simple method of finding solutions. $e.g. Consider\ the\ congruence$:

$2x \equiv 3\ (mod\ 5)$. By residue- method, it is seen that

$x \equiv 4\ (mod\ 5)\ is\ a\ solution\ of\ the\ linear\ congruence.$

But sometimes this method becomes impractical, when modulus is comparatively large. $e.g.\ Consider\ the\ congruence$: $8x \equiv 10\ (mod\ 40)$.

The residue method is not suitable here. It takes a long time.

Then another method, known as G.C.D. method is used. In some problems, this method is also becomes time-consuming.

Sometimes the method also become impractical.

$e.g. Consider\ \ 23x \equiv 12\ (mod\ 1001)$ & $140x \equiv 133\ (mod\ 301)$.

Here finding g. c. d. orally is not possible. Sometimes, finding the initial solution is difficult.

NEED OF RESEARCH

But there also exists some linear congruence which cannot be solved with an ease using above methods.

$e.g.$ The congruence $97x \equiv 807(mod\ 1001)$. It cannot be solved with an ease. It takes a long time.

Sometimes it become nearly impossible to use those methods for solutions when the modulus is comparatively large. Here is the need of a new simple time - saving method.

It will increase the interest of the readers so many times. This is the need of the research.

To overcome this difficulty, the author proposed a very simple method for solutions in a short time.

PROBLEM-STATEMENT

Here the problem is:

"$To\ find\ the\ solutions\ of\ the\ linear\ congruence\ of\ degree\ one$:

$\boldsymbol{ax \equiv b\ (mod\ m)\ with\ a \not\equiv o\ (mod\ m)}$,

$when\ m\ is\ comparatively\ large, either\ prime\ or\ composite\ integer$".

METHODS OF SOLVING LINEAR CONGRUENCE

Here the methods are described in short**.**

Method-I (RESIDUE METHOD)

It is well-known that the members of residues of the modulus are the solutions of the congruence. It is called the residue- method of solving the linear congruence. Solutions can be obtained by finding the residues and testing the members for solutions by Trial & Error method one by one [2], [3].

$e.g.$ Consider the linear congruence: $5x \equiv 4\ (mod\ 6)$.

The non-zero residues of 6 are 1, 2, 3, 4, 5.

It is seen that $x \equiv 2\ (mod\ 6)$ is the only solution.

But if the modulus is comparatively large, then this method becomes time-consuming and the residue method does not work well.

Method-II: (Inversion method):

Consider the congruence: $ax \equiv b\ (mod\ m)$.

If there exists c such that $ac \equiv 1\ (mod\ m)$, then multiplying the congruence by c, one get $acx \equiv bc\ (mod\ m) i.e.\ x \equiv bc\ (mod\ m)$. Here c is the modular inverse of a.

$e.g.$ Consider the congruence $3x \equiv 2\ (mod\ 11)$.

It is seen that $3.4 \equiv 1\ (mod\ 11)$ giving $c = 4$.

Then the unique solution is $x \equiv bc\ (mod\ m)$

$\equiv 2.4 = 8\ (mod\ 11)$.

$\boldsymbol{Note}$: Consider the congruence $13x \equiv 2\ (mod\ 39)$. Residue system of 39 has 38 members. Definitely, the method is time-consuming. The residue method is not suitable here. But one interesting thing is that this congruence has no solution. Even are trying for solutions. What a ridiculous thing!! So, we must test the congruence for solvability. So we need a method with **solvability condition.**

Method –III: (G. C. D. Method)

Consider the congruence $ax \equiv b\ (mod\ m)$. If $(a, m) = g\ \&\ g|b$, then linear congruence is solvable; otherwise, not. If the congruence is solvable, then it has g-solutions given by:

$$x \equiv \left(\frac{b}{g}\right) x_0 + \left(\frac{m}{g}\right) t\ \ (mod\ m)\ \ with\ \ 0 \le t \le g - 1\ [2]\ \&\ [3].$$

If $g = 1$, then the congruence has **unique solution** $\boldsymbol{x \equiv bx_0\ (mod\ m)}$ **whenever** x_0 is a solution of $\left(\frac{a}{g}\right) x \equiv 1\ \left(mod\ \frac{m}{g}\right) i.e.\ ax \equiv 1\ (mod\ m)$.

$e.g.$ Consider the linear congruence $12x \equiv 30\ (mod\ 45)$.

Here, $a = 12,\ b = 30,\ m = 45$.

Then, $(a, m) = (12, 45) = 3\ and\ we\ see\ that\ 3|30\ i.e.\ g|b$.

Thus the congruence is solvable and has $g = 3$ solutions.

These are given by

$x \equiv \left(\frac{b}{g}\right)x_0 + \left(\frac{m}{g}\right)t \ (mod\ m)\ with\ 0 \le t \le g-1.$

$\equiv \left(\frac{30}{3}\right)x_0 + \left(\frac{45}{3}\right)t\ (mod\ 45)\ with\ t = 0,1,2.$

$\equiv 10x_0$+45t (mod 45) with $t = 0,1,2.$

For x_0, $consider\ the\ congruence\ \left(\frac{a}{g}\right)x \equiv 1\ \left(mod\ \frac{m}{g}\right)$

$i.e.\left(\frac{12}{3}\right)x \equiv 1\ \left(mod\ \frac{45}{3}\right)$

$i.e.\ 4x \equiv 1\ (mod\ 15).$

Its has unique solution $x \equiv 4\ (mod\ 15)$. So, here, $x_0 = 4$.

Then, all the solutions are $x \equiv 10.4 + 15t\ (mod\ 45) with\ t = 0,1,2$

$\equiv 40 + 0; 40 + 15; 40 + 30\ (mod\ 45)$

$\equiv 40, 55, 70\ (mod\ 45)$

$\equiv 40, 10, 25\ (mod\ 45).$

Now consider the congruence $140x \equiv 133\ (mod\ 301)$ with $a = 140, b = 133, m = 301$.

As m is very large, Residue Method fails. In g.c.d. method, $(a,m) = (140, 301) = 7$.

How can one guess that $g = 7$?

Here is the difficulty.

Now x_0 is given by $20x \equiv 1\ (mod\ 43)$ with $x_0 = 28$.

Here is one more difficulty. How one can guess that $x \equiv 28\ (mod\ 43)\ is\ a\ solution\ of\ the\ congruence$? It is a time-consuming problem.

To overcome these difficulties**,** the proposed method is used and it works well [2].

So, we need the proposed method to overcome the two serious difficulties:

[1] To find g. c. d. of a & m $i.e.(a,m) = g$;

[2] To find $x_0\ \ i.e.\ to\ solve\ \left(\frac{a}{g}\right)x \equiv 1\ \left(mod\ \frac{m}{g}\right)$.

Here is one more example: $23x \equiv 12\ (mod\ 1001)$. It is also a time-consuming problem. So, readers must use the above methods. They are in search of a suitable method.

ALGORITHMIC PROPOSED METHOD

Consider the linear congruence $ax \equiv b\ (mod\ m)$; m being comparatively large.

To find g, one can use Euclidean Algorithm, a repeated use of division algorithm [2] & [3]:

After obtaining g, express it as $g = ax_0 + my_0$ using above steps and find x_0.

Algorithmic steps are as under:

1) Given the congruence: $ax \equiv b\ (mod\ m)$ with m comparatively large, find a, b, m.
2) Find g. c. d g of a & m $i.e.\ g = (a,m)$ using Euclidean Algorithm.
3) If g | b, then congruence is solvable and has g- incongruent solutions.
4) Find a solution x_0 from $g = ax_0 + my_{0,}$ using Euclidean Algorithm.
5) Find all the required solutions $x \equiv \left(\frac{b}{g}\right)x_0 + \left(\frac{m}{g}\right)t\ (mod\ m)\ with\ 0 \le t \le g-1.$

FORMULATION OF SPECIAL CUBIC CONGRUENCE OF PRIME MODULUS:

Here the author wishes to provide a formula for the solutions of linear congruence of degree one. Let us consider the congruence $ax \equiv b\ (mod\ p), p\ being\ prime\ integer$.

Let $(a,p) = 1$. Then using Fermat's theorem: $a^{p-1} \equiv 1\ (mod\ p)$.

Multiplying the given congruence by a^{p-2}:

$a^{p-2}.ax \equiv a^{p-2}.b\ (mod\ p)\ i.e.\ \ a^{p-1}x \equiv a^{p-2}.b\ (mod\ p)$

$i.e.\ x \equiv a^{p-2}.b\ (mod\ p)$.

This is the unique solution of the congruence $ax \equiv b\ (mod\ p)\ if\ \ (a,p) = 1$and is always solvable. This formula is more useful when a & p are moderately large.

ILLUSTRATIONS

Let us consider a linear congruence of prime modulus:$17x \equiv 53\ (mod\ 97)$.

It is of the type:$ax \equiv b\ (mod\ m)\ \ with\ a = 17, b = 53,\ \ m = 97$.

To find (a,m), we use Euclidean Algorithm.

Using division algorithm repeatedly, we get:

$$97 = 17.5 + 12$$

$$17 = 12.1 + 5$$

$$12 = 5.2 + 2$$

$$5 = 2.2 + 1$$

$$2 = 1.2 + 0$$

Then it can be seen that $(a,p) = (17,97) = 1 = g$ & $1|53\ \ i.e.\ g|b$.

So, the congruence is solvable & as g=1, it has only one solution.

Now, from the above equations we get

$1 = 5 - 2.2$

$= 5 - (12 - 5.2).2$

$= 5 - 12.2 + 5.4$

$= 5.5 - 12.2$

$= (17 - 12).5 - 12.2$

$= 17.5 - 12.5 - 12.2$

$= 17.5 - 12.7$

$= 17.5 - (97 - 17.5).7$

$= 17.5 - 97.7 + 17.35$

$= 17.40 - 97.7$

Therefore, $x_0 = 40$

Then $x_1 = x_0.b = 40.53 = 2120 \equiv 83\ (mod\ 97)$.

This is the required unique solution.

Here is one more example: $23x \equiv 12\ (mod\ 1001)\ \ with\ a = 23,\ \ b = 12,\ \ m = 1001$.

Then, $(a,m) = (23,1001) = 1$, using Euclidean Algorithm. Then, we get $x_0 = -87$.

Then the unique solution is $x \equiv bx_0\ (mod\ m)$

$$\equiv 12.(-87) = -1044 + 2.1001 = \mathbf{958}\ (\boldsymbol{mod}\ \mathbf{1001}).$$

Similarly, $93x \equiv 4\ (mod\ 97)$ can be solved easily using this method with solution

$x \equiv 96\ (mod\ 97)$.

Consider the congruence $3x \equiv 2\ (mod\ 11)$.

Here $a = 3, b = 2, p = 11 \ with \ (a, p) = (3, 11) = 1$. Therefore, the congruence is solvable and has a unique solution.

As p is small, $Inversion\ method$ formula is suitable.

The solution is given by $x \equiv a^{p-2}.b \ (mod\ p)$

$$\equiv 3^{11-2}.2 \ (mod\ 11)$$

$$\equiv 3^{9}.2 \ (mod\ 11)$$

$$\equiv 4.2 \ (mod\ 11)$$

$$\equiv 8 \ (mod\ 11).$$

CONCLUSION

Thus, it can be concluded from this discussion that the linear congruence of composite & prime modulus of degree one can be solved very easily using Euclidean algorithm, when other methods fails and when modulus is comparatively large.

This is the merit of the paper. It makes solving the linear congruence simple & easy.

REFERENCES

[1] Burton David M., 2012, *Elementary Number Theory*, Mc Graw Hill Education (India) Private Limited, Chennai, ISBN: 978-1-25-902576-1.
[2] Roy B. M., 2016, *Discrete Mathematics & Number Theory*, Das Ganu Prakashan Nagpur, (India), ISBN: 978-93-84336-12-7.
[3] Zuckerman H. S., at el, 1960, "*An Introduction to The Theory of Numbers*", 5/e, Wiley India (Pvt) Ltd, ISBN: 978-81-265-1811-1.