Maher Rusho

1 November, 2022

A Case Study Of Special Types Of Congruences And It's Solution

Maher Ali Rusho

Abstract :

Number Theory is one of the major part of any kind of national and international Math Olympiad . And Numbers are also the base of Mathematics .Without it Math is meaningless . Famous Mathematician like Terence Tao , Ramanujan , Gregory Perelman were inspired by numbers especially number theory from their early childhood and for this they came into mathematics field . But because of our traditional math curriculum „ there is no Number Theory portion . I feel sorrow with thus that Many child don't like math because the Math books never make interest on them . . And the silly thing is in the national curriculum of Bangladesh People go through Number Theory in their Undergraduate or M.SC level !! To make interest in Mathematics to the general people , the math curriculum must be changed . . It would be nice if elementary student starts their Math journey through number theory , then we will get more mathematicians in near-future , because Mathematicians in needed to shape the future world . I am going to write this paper to Advance Math Olympiad Student who has a bit of knowledge of everything in Number theory , But it will be useful to an undergraduate student also . Happy Problem Solving!

Key - Words : Linear Congruence , congruence modulo of functional equation and it's solution , Chinese remainder theorem , theory of equations

Linear Congruences

Theorem :1

If (a,n)=1 , then the linear congruences $ax \equiv b(modn)$ has a unique solution (mod n) . The solution in X is $X \equiv ba^{\Phi}(n) - 1$.

Theorem :2

If (a,n)=g , where g>1 , then the congruence ax≡b(mod n)

1)has no root if g doesn't divide b.

2) exactly g incongruent roots g/b ,

The roots are

$x0, x0 + n/g, x0 + 2n/g, - - - - - x0 + (g-1)n/g$

Where xo is the unique root of $a/g * x \equiv b/g(modn/g)$. Remember one thing . If in an congruent solution you want to multiply a constant term , you don't need to multiply in the modulo term in the equation e.g $ax \equiv b(modn)$ can be multiply by c a constant it become $cax \equiv b(modn)$. But if you have to divide the congruent you have to divide the modulo part . And to understand this statement see example of theorem 2 ,2

Let's dive into some example , because understanding math doesn't mean understanding it's theory , you must have to solve the problems also for proper understanding

Solve the congruence 5x≡7 (mod 8) by using the the Euler Theorem

Given that (5,8)=1

Therefore the given equation has a unique solution . From this the solution is $x \equiv ba^{\Phi(n)-1}$

Here $a=5$, $b=7$, $n=8$, $\Phi(8)-1 = 3$

Now apply equation

$x \equiv 7 * 5^3 \pmod 8$

$=> x \equiv 875 \pmod 8$

$-> x \equiv 3 \pmod 8$

Similar type of problem

Solve $15x \equiv 6 \pmod n$

Here $(15,21)=3$ and $3/6$. So , it has 3 roots , now

$15x \equiv 6 \pmod{21}$

=> divide by 3 it become

$5x \equiv 2 \pmod 7$

$14x + x \equiv 6 \pmod 7$

/ so our first solution is $x_0 = 6$, then another solutions will be from theorem 2,2 13 and 20

So solution is 6,13,20(ans)

Chinese theorem in Number theory

Chinese theorem is contagious theorem like covid-19 , but it is useful !! So we can touch it or use it , I am not going to go to tell the

theory , I will see you some examples and you will understand it in a natural way ,

Solve his congruent and find it's least solution

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

Let's define a variable $m = m_1 m_2 m_3 = 3*5*7$, and let assume $M_1 = m/m_1 = 35$, $M_2 = M/m_2 = 21$, $M_3 = m/m_3$

Step 1 :

$M_1 x_1 \equiv 1 \pmod{m_1}$

$=> 35 x_1 \equiv 1 \pmod 3$

$=> x_1 \equiv 2 \pmod 3$

Step 2 :

$M_2 x_2 \equiv 1 (\text{mode } m_2)$

$21 x_2 \equiv 1 \pmod 5$

$=> x_2 \equiv 1 \pmod 5$

Then The least solution is

$x \equiv M_1 x_1 a + M_2 x_2 + m_3 X_3 \pmod{m\ 3*5*7}$

$x \equiv 233 \pmod{105}$

$x \equiv 23 \pmod{105}$

If we don't understand this then repeat this solution .

Congruences of Higher Degree with Prime Modulo

With prime modulo p , the general form of a congruence is

f(x) = $a0x^n + - - - - + an(mod p)$

All of it 's solution obtain by substituting all the integers of a complete residue system modulo p for x in (1) . For this purpose , we do the following steps .

1) if some coefficients of f(x) are greater than p , we reduce them to less than p . Also if the degree of f(x) is not less than p, can obtain r(x) such that

2) f(x)=(x^p-x)q(x)+r(x)

3) Where the degeee of r(x) is less than p . We educe f(x) to r(x) such that

4) f(x)≡r(x)(mod p)

5) By using x^p ≡x(mod p) . The incongruent solutions of f(x) and r(x) identical . Here the problem of solving (1)becomes that of r(x)≡0 (mod p)

6) The last step is if f(x)≡f1(x0f29x) (mod p) . Then to solve f1(x) ≡0(mod p) and f2(x) ≡0(mod p)

Conclusion

In this paper we have discussed some technique of solving difficult type of congruent modulo . That will be very useful when solving Olympiad number theory problem , Our aim of Rusho's Education plant is to make math Olympiad and other olympiad easy for you . So if enjoy hen you can read this articles also : https://rusho.org/my-research-paper:2

Reference :

The Theory Of numbers (prof.Dr.Fazlur Rahman)

Advance theory of numbers

Number theory and it';s application : https://books.google.com.bd/books?id=cVuyzgEACAAJ&dq=advance+theory+of+number+bangladesh+book&hl=en&sa=X&ved=2ahUKEwiAv8729Iz7AhVI1jgGHQWSBEkQ6AF6BAgHEAI

https://books.google.com.bd/books?id=m59lEAAAQBAJ&pg=PA936&dq=advance+theory+of+number+bangladesh+book&hl=en&sa=X&ved=2ahUKEwiAv8729Iz7AhVI1jgGHQWSBEkQ6AF6BAgDEAI#v=onepage&q=advance%20theory%20of%20number%20bangladesh%20book&f=false

https://artofproblemsolving.com/wiki/index.php/Category:Olympiad_Number_Theory_Problems