INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume 4, Issue 3)

Available online at: www.ijariit.com

A new method of finding solutions of a solvable standard quadratic congruence of comparatively large prime modulus

B. M. Roy

roybm62@gmail.com

Jagat Arts Commerce Indraben Hariharbhai Patel Science College,

Gondia, Vidharbha, Maharashtra

ABSTRACT

In this paper, a new method of finding solutions of salvable standard quadratic congruence of a comparatively large prime modulus is described. A comparative study was made by solving numerical problems using existed and proposed methods. The merits and demerits of both the methods are also discussed.

Keywords: *Congruence, Divisibility, Prime modulus, Quadratic congruence.*

1. INTRODUCTION

Divisibility is a fundamental concept of Number Theory and a congruence is nothing more than a statement about divisibility and expressed in a convenient notation.

The theory of congruence was introduced by Carl Friedrich Gauss (1777-1855) in his book DisquisitionesArithmeticae [1].

2. STATEMENT OF DIVISION ALGORITHM [1]

If an integer ‘a’ is divided by a non-zero positive integer ‘p’, then there always exists a unique integer ‘q’, called quotient and a unique integer ‘r’, called remainder with the condition r≥0 but r<p.

Mathematically we can write: a=pq+r, 0≤r<p. …….(1)

3. DIVISION ALGORITHM IN CONGRUENCE NOTATION

Statement (1) can also be written as: a-r=pq i.e. p| a-r

We write this as: a≡r (mod p)……(2)

and read as: ’a’ is congruent to ‘r’ modulo ‘p’.

i.e. Dividend ≡ Remainder (modulo divisor).

Here ‘modulo’ is abbreviated as ‘mod’.

(2) is the new form of (1) in congruence notation.

4. QUADRATIC CONGRUENCE AND SOLUTIONS

If 'a' is replaced by x^2in (2), then the congruence becomes x^2≡r (mod p) ……..(3)

and is called a standard quadratic congruence. A solution of (3) is the value of unknown x that satisfies the congruence (3). To find the solution of congruence (3) literally means to find a perfect square which when divided by a positive integer p gives the remainder

r. We know that the square of two different integers is the same perfect square and hence we can say that every quadratic congruence has at least two solutions. If the modulus p is a prime positive integer, then the quadratic congruence has exactly two incongruent solutions [2].

5. EXISTED METHOD

To find the solution of x^2≡a (mod p)…….(4)

We find a perfect square b^2which is congruent to 'a' modulo 'p'.

We solve the congruence (4) by the existed method described below assuming that p is a positive prime integer.

If 'a' is a perfect square i.e.a=b^2, then the congruence is: x^2≡b^2 (mod p) and it has exactly two solutions given by x≡±b (mod p) i.e. x≡b,-b (mod p) i. e. x≡b,p-b (mod p).

If 'a' is not a perfect square, then we add 'p' to 'a' to get x^2≡a+p (mod p). If (a+p) is a perfect square, then the congruence becomes x^2≡b^2 (mod p) with solutions x≡±b (mod p).

If a+p is not a perfect square, then we again add 'p' to a+p to get a+2p. If a+2p is not a perfect square, we add p again to get a+3p.We proceed in this way to get a+kp , which is a perfect square.

Thus, x^2≡a (mod p)

≡a+kp (mod p)for some finite k

≡b^2 (mod p)

We add "kp" {which is congruent to zero modulo prime p} to 'a' to get a+kp=b^2 for certain positive integer k.

Then congruence becomes: x^2≡a+kp (mod p) and hence x^2≡b^2 (mod p)

The solutions are then given byx≡±b (mod p)i.e.x≡b,p-b (mod p).

6. ILLUSTRATIONS

1) Consider the congruence x^2≡23 (mod 43).

23 is not a perfect square. So we add 43 to get x^2≡23+43=66 (mod 43).

66 is not a perfect square. So we add 43 to 66 to get x^2≡66+43=109 (mod 43).

Proceeding in this way we get

x^2≡23+43=66+43=109+43=152+43=195+43=238+43=281+43=324=〖18〗^2 (mod 43) .

Thus we get x^2≡〖18〗^2 (mod 43).

Hence solutions are: x≡±18 (mod 43) i.e. x≡18,43-18 (mod 43)i.e. x≡18,25 (mod 43)

Consider the congruence: x^2≡48 (mod 503)

As in above, we get: x^2≡48+ 503+503+⋯..+503=48+503.12=6048=〖78〗^2 (mod 503)

Hence solutions are: x≡78,425 (mod 503).

7. DRABACKS OF EXISTED METHOD

The method has serious drawbacks and hence the method is not preferred. Sometimes it becomes impractical. To find the solution of the congruence x^2≡a (mod p), one has to find a perfect square b^2 which is congruent to 'a' modulo p i.e. b^2≡a (mod p). So one can go on testing every perfect square and has to find that prefect square which is congruent to a. Here lies the difficulty!!

In this existed method, one has to check at every step whether the number obtained is a perfect square or not. (i.e.for every value of k, one has to check a+kp is a perfect square or not) .

We have to prepare a list of perfect squares and test everyone to get the required congruent number 'a' modulo p. It will be boring and time-consuming.

This takes more time to get the solutions. Sometimes it becomes a boring task.

8. PROBLEM STATEMENT

To find the solutions of a standard quadratic congruence x^2≡a (mod p) where p is a prime positive integer, using a very simple method in comparatively less time, proposed by the author and may be called

"PERFECT-SQUARE-METHOD".

9. PROPOSED PERFECT- SQUARE METHOD

our aim is to find a quick and simple procedure. For that, we use a popular mathematical formula: a^2+2a+1=〖(a+1)〗^2.

Considering this formula as a^2+(2a+1)=〖(a+1)〗^2, we get an algorithm to find all the successive perfect squares.

So, for the congruence x^2≡a (mod p), we find a perfect square nearest to p but greater than p. Let it be b^2.If it is not congruent to a, then adding 2b+1 to b^2, we get 〖(b+1)〗^2. Then adding 2b+3 to 〖(b+1)〗^2 we get 〖(b+2)〗^2 and so on.

Thus, the series becomes

b^2+(2b+1)+(2b+3)+(2b+5)+⋯……+(2b+q)≡a(mod p)

for a finite odd positive integer q. Then x≡±((q+1)/2) are the two incongruent solutions.

10. ILLUSTRATIONS

Solve the congruence x^2≡43 (mod 97)

Solution: Given congruence is x^2≡43 (mod 97).

Here a=43 p=97.

Perfect square nearest to 97 and greater than 97 is 100=〖10〗^2.

Then
100+(2.10+1)=121≡24+(2.10+3)=47+(2.10+5)=72+(2.10+7)=99≡2+(2.10+9)=31+(2.10+11)=62+(2.10+13)=95+(2.10+15)=130≡33+2.10+17)=70+(2.10+19)=109≡12+(2.10+21)=53+(2.10+23)=96+(2.10+25)=141≡44+(2.10+27)=91+(2.10+29)=140≡43 (mod 97)

It can also be written as

100+21=121≡24+23=47+25=72+27=99≡2+29=31+31=62+33=95+35=130≡33+37=70+39=109≡12+41=53+43=96+45=141≡44+47=91+49=140≡43 (mod 97).

Then the solutions are

x≡±((49+1)/2)=±25 (mod 97) i.e. x≡25,-25 (mod 97) i.e.x≡25,72 (mod 97).

Consider another congruencex^2≡52 (mod 101). It can be shown that its solutions are

x≡±31 (mod 101) i.e. x≡31,70 (mod 101) with q=61.

11. MERIT OF PROPOSED METHOD

1) This method takes less time to get the required Solutions.

2) One need not test for perfect square at every step as in existed method.

3) The calculation is simple and smooth.

4) Numbers never become larger than the modulus.

12. CONCLUSION

In this paper, a new method of solving solvable standard quadratic congruence of the comparatively large prime modulus of the type x^2≡a (mod p) is discussed. It is found that the proposed method is very simple, interesting, time-saving and easily calculable. A comparison is made by solving the same problem using both the method existed and proposed.

13. REFERENCES

[1] Burton David M., "Elementary Number Theory", Indian edition, Mc Graw Hill Education (India)Pvt Ltd.
[2] Niven I., Zuckerman H. S., Montogomery H. L. (1960, Reprint 2008), "An Introduction to the theory of Numbers", 5/e, Wiley India (Pvt) Ltd.

[3] Roy B. M., "Discrete Mathematics & Elementary Number Theory, 1/e, Jan. 2016, Das GanuPrakashan, Nagpur, India.
[4] Thomas Koshy, "Elementary Number Theory with Applications", 2/e, Academic Press.

