Formulation of a Class of Solvable Standard Quadratic Congruence of Composite Modulus- an Odd Prime Positive Integer Multiple of Seven

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 study, a standard *quadratic congruence* of composite modulus-an odd prime positive- integer multiple of seven, is formulated. Formulae are established successfully and are tested and found true with suitable examples. No need to use *Chinese Remainder Theorem*. Formulation is the merit of the paper.**

***Keywords*: Chinese Remainder Theorem, Composite modulus, Quadratic Congruence.**

INTRODUCTION

Here, in this paper, another standard quadratic congruence of **composite modulus**- an odd prime positive- integer multiple of seven, is considered for formulation. I have formulated a lot of standard quadratic congruence of composite modulus earlier. I had successfully tried my best to formulate all those **quadratic congruence**; even some congruence are remained to formulate. Here I consider one such standard quadratic congruence yet not formulated. It is of the type: $x^2 \equiv a^2 (mod\ 7p)\ with\ (a^2, 7p) = 1, p \neq 7$, p being a positive odd prime integer.

LITERATURE- REVIEW

I have gone through different books on Number Theory and peeped into the literature of mathematics. It is very pathetic and panic for me that no formulation has been found for the said congruence; only the use of **Chinese Remainder Theorem [1]** is discussed. Koshy had made a small bold attempt to consider the congruence of composite modulus **[4]** but no other mathematician do. They all discussed the congruence of prime modulus only. No perfect attempt had been taken for standard quadratic congruence of composite modulus. No one had attempted to do anything for the students' sake. They all used the very popular method called "CRT". NO one even had attempted to improve the literature of quadratic congruence of composite modulus.

NEED OF MY RESEARCH

The use of Chinese Remainder Theorem is not a fare method for the students in examination. It takes a long time. Students are always ready to get rid of such method and want to feel comfortable when solving such quadratic congruence. It is only possible if the problem is formulated. I have tried my best to formulate the problem. This is the need of my research.

PROBLEM-STATEMENT

The problem is to formulate the standard quadratic congruence $x^2 \equiv a^2\ (mod\ 7p), p \neq 7,$

with $(a^2,\ 7p) = 1,$ p being an odd positive prime integer. Such congruence always has four solutions **[3].** Here, I have tried my best to establish the formula for solutions of the said congruence.

ANALYSIS & RESULT (Formulation)

Consider the congruence $x^2 \equiv b\ (mod\ 7p)$.

If $b = a^2, then\ we\ have\ the\ congruence\ x^2 \equiv a^2\ (mod\ 7p)$.

Otherwise, it can be written as $x^2 \equiv b + k.7p = a^2\ (mod\ 7p)$ for some positive integer k **[2].**

It is of the type $x^2 \equiv a^2\ (mod\ 7p)$.

Then its two obvious solutions are $x \equiv 7p \pm a \equiv a, 7p - a\ (mod\ 7p)$.

We search for other two solutions as under:

Now, consider $x = \pm(2p \pm a)$

Then, $x^2 = (2p \pm a)^2 = 4p^2 \pm 4pa + a^2 = a^2 + 4p(p \pm a) = a^2 + 4p.7m,\ \ if\ p \pm a = 7m.$

Thus the other two solutions are:

$\boldsymbol{x \equiv \pm(2p \pm a)\ (mod\ 7p)}$, **if** $\boldsymbol{p \pm a = 7m}$.

Also, consider $x = \pm(p \pm a)$

Then, $x^2 = (p \pm a)^2 = p^2 \pm 2pa + a^2 = a^2 + p(p \pm 2a) = a^2 + p.7m,\ \ if\ p \pm 2a = 7m.$

Therefore, **two other solutions are** $\boldsymbol{x \equiv \pm(p \pm a)\ (mod\ 7p),\ \ if\ p \pm 2a = 7m}$.

Also, for $x \equiv \pm(3p \pm a)\ (mod\ 7p)$, we have $x^2 \equiv (3p \pm a)^2$

$$= 9p^2 \pm 6pa + a^2$$

$$= a^2 + 3p(3p \pm 2a)$$

$$= a^2 + 3p.7m,\ \ if\ 3p \pm 2a = 7m$$

$$\equiv a^2\ (mod\ 7p)$$

Thus, if $\boldsymbol{3p \pm 2a = 7m, then\ x \equiv 3p \pm a\ (mod\ 7p)\ are\ the\ other\ two\ solutions}$.

Also, for $x \equiv \pm(4p \pm a)\ (mod\ 7p)$, we have $x^2 \equiv (4p \pm a)^2$

$$= 16p^2 \pm 8pa + a^2$$

$$= a^2 + 8p(2p \pm a)$$

$$= a^2 + 8p.7m,\ \ if\ 2p \pm a = 7m$$

$$\equiv a^2\ (mod\ 7p)$$

Thus, if $\boldsymbol{2p \pm a = 7m, then\ x \equiv 4p \pm a\ (mod\ 7p)\ are\ the\ other\ two\ solutions}$.

But, if $(a, 7p) \neq 1$, then the congruence has only two obvious solutions. Because then, if

$a^2 = 7k, then\ ultimately,\ p \pm a \neq 7m.$ Hence, the second pair of solutions is not possible. And the said congruence must have the obvious pair of solutions.

ILLUSTRATIONS

Consider the congruence $x^2 \equiv 23\ (mod\ 77)$……..[**Taken from internet**].

It can be written as $x^2 \equiv 23 + 77 = 100 = 10^2\ (mod\ 7.11)\ with\ p = 11\ \&\ a = 10$ [2].

Thus, the congruence is of the type $x^2 \equiv a^2\ (mod\ 7p)$

Then, $x \equiv 7p \pm a\ = 77 \pm 10\ (mod\ 77) \equiv 10, 67\ (mod\ 77)$ are the two obvious solutions

Also, $(a^2, 7p) = (10, 77) = 1$. So, other two solutions exist.

These two solutions are:

$As\ p + a = 11 + 10 = 21 = 7.3 = 7m$

Thus, $x \equiv \pm(2p + a) = \pm(22 + 10) = \pm 32 = 32, 45(mod\ 77)$ are the other two solutions.

Therefore, the said congruence under considerations has four solutions

$$\boldsymbol{x \equiv 10, 67;\ 32, 45\ (mod\ 77).}$$

Consider the congruence $x^2 \equiv 30\ (mod\ 91)$

It can be written as $x^2 \equiv 30 + 91 = 121 = 11^2\ (mod\ 7.13)\ with\ p = 13.$

Thus, the congruence is of the type $x^2 \equiv a^2\ (mod\ 7p)$

Then, $x \equiv a, 7p - a\ (mod\ 7p) = 11, 91 - 11\ (mod\ 91) \equiv 11, 80\ (mod\ 91)$ are the two obvious solutions

For the other two solutions, we see that

$p + 2a = 13 + 2.11 = 35 = 7.5,$

Hence, $x \equiv \pm(p + a) \equiv \pm(13 + 11) = \pm 24 = 24, 67(mod\ 91)$

Therefore, the said congruence under considerations has four solutions

$$\boldsymbol{x \equiv 11, 80; 24, 67\ (mod\ 91)}.$$

Consider the congruence $x^2 \equiv 9\ (mod\ 35)$

It can be written as $x^2 \equiv 3^2\ (mod\ 7.5)\ with\ p = 5.$

Thus, the congruence is of the type $x^2 \equiv a^2\ (mod\ 7p)$

Then, $x \equiv a, 7p - a\ (mod\ 7p) = 3, 35 - 3\ (mod\ 35) \equiv 3, 32\ (mod\ 35)$ are the two obvious solutions

For the other two solutions, we see that

$3p \pm 2a = 3.5 \pm 2.3 = 15 + 6 = 7.3,$

Hence, $x \equiv \pm(3p + a) \equiv \pm(15 + 3) = \pm 18 = 18,\ 17\ (mod\ 35)$

Therefore, the said congruence under considerations has four solutions

$$\boldsymbol{x \equiv 3, 32; 17, 18\ (mod\ 35)}.$$

Consider one more example as per need: $x^2 \equiv 49\ (\text{mod}\ 161)$

It can be written as $x^2 \equiv 7^2\ (\text{mod}\ 7.23)$

It is of the type $x^2 \equiv a^2\ (mod\ 7p) with\ p = 23\ \&\ a = 7.$

Its two obvious solutions are $x \equiv 7p \pm a = 161 \pm 7 = \boldsymbol{7, 154\ (mod\ 161)}$.

Also for other two solutions, we see that $(a^2, 7p) = (49, 161) \neq 1$

Hence other two solutions do not exist and hence $\boldsymbol{x \equiv 7, 154\ (mod 161)}$ are the other two solutions.

CONCLUSION

Therefore, we conclude that the congruence under consideration $x^2 \equiv a^2 (mod\ 7p)\ with\ (a, 7p) = 1$ has four incongruent solutions given by:

Two obvious solutions are $\boldsymbol{x \equiv 7p \pm a = a, 7p - a\ (mod\ 7p)}$.

And other two solutions are in the followings:

If $\boldsymbol{p \pm 2a = 7m, then}$ **two other solutions are** $\boldsymbol{x \equiv \pm(p \pm a)(mod\ 7p)}$.

If $\boldsymbol{p \pm a = 7m,\ then\ x \equiv \pm(2p \pm a)\ (mod\ 7p)}$ **are the other two solutions**

If $\boldsymbol{3p \pm 2a = 7m, then\ x \equiv \pm(3p \pm a)\ (mod\ 7p)\ are\ the\ other\ two\ solutions}$.

But if $\boldsymbol{(a, 7p) \neq 1, then\ the\ congruence\ have\ only\ two\ obvious\ solutions}$.

MERIT OF THE PAPER

In this paper, a class of standard quadratic congruence of composite modulus- an odd positive integer multiple of seven, is formulated. First time, a formula is established. No need to use Chinese Remainder Theorem. This is the merit of the paper.

REFERENCES

[1]Burton David M, *Elementary Number Theory*, Seventh Indian edition, Mc Graw Hill(Pvt) Ltd.
[2] Roy B M , *Discrete Mathematics & Number Theory*, First edition, Das Ganu Prakashan, Nagpur (INDIA)
[3] Zuckerman at el, An Introduction to The Theory of Numbers, fifth edition, Wiley student edition, INDIA, 2008.
[4]Koshy Thomas, Elementary Number Theory with Applications, Second edition, Academic press, Indian Print, 2009.