RP-139: Reformulation of solutions of standard quadratic congruence of composite modulus- a product of two different odd primes and four

Prof. B. M. Roy

Head, Dept. of Mathematics
Jagat Arts, Commerce & I H P Science College, Goregaon (Gondia)
(Affiliated to RTM Nagpur University)

***Abstract*: In this paper, a reformulation of solutions of a solvable standard quadratic congruence of composite modulus-a product of two different odd primes and four is considered for study. The solutions are reformulated. It is found that the formula is very simple, easy to remember and takes less time in comparison to the existed method. Formula is also illustrated using the numerical examples.**

***Keywords*: Chinese Remainder Theorem (CRT), even composite modulus, Quadratic Congruence.**

INTRODUCTION

The author had formulated this congruence in 2018 with a different formulation [1].
But after a self-review of the formulation, it is felt that the previous formulation requires reformulation. So, the author considers the same congruence for the reformulation here.
The congruence $x^2 \equiv a \ (mod\ p), p\ an\ odd\ prime$ is a standard quadratic congruence of prime modulus in an unknown x. The values of x that satisfy the congruence are the solutions of it. The standard quadratic congruence of prime modulus has exactly two solutions [2]. If p is replaced by m, a composite positive integer, then the congruence is called a congruence of composite modulus. It has at least two solutions [3].
Here the author wishes to consider the congruence:
$x^2 \equiv a \ (mod\ m)$ of composite modulus.
If $m = 4pq$, then the congruence becomes: $x^2 \equiv a \ (mod\ 4pq)$.

PROBLEM STATEMENT

Here the problem is-
"To reformulate the solutions of the standard quadratic congruence of composite modulus of the type:

$$x^2 \equiv a \ (mod\ 4pq) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

$where\ p, q$ are distinct positive odd primes".

EXISTED METHOD:

The existed method is popularly known as Chinese Remainder Theorem (CRT) method.
Consider the congruence under consideration (1).
It can be split into three individual congruence.
These standard quadratic congruence can be solved separately to get solutions.
As "every solvable quadratic congruence of positive odd prime modulus has exactly two solutions, solving those**, eight common solutions** can be obtained using Chinese Remainder Theorem. This method has some serious demerits. To overcome these demerits, a simple, easy and time-saving method is required. $i.e.$ Formulation of solutions must be required. The author already formulated many standard quadratic congruence of composite modulus [4], [5], [6]. Here is one more.

ANALYSIS & RESULT (REFORMULATION)

Consider the congruence $x^2 \equiv a \ (mod\ 4pq)$.
Case-I: $Let\ a \neq p;\ a \neq q$.
If $a = b^2$, then the congruence becomes: $x^2 \equiv b^2 \ (mod\ 4pq)$.
If $a \neq b^2$, then we add "$m.4pq$" to a to get $a + m.4pq\ with\ such\ an\ m\ such\ that$
$a + m.4pq = b^2$ [3].
For the solutions, consider, $x \equiv 2pqk \pm b \ (mod\ 4pq)$.
Then, $x^2 \equiv (\ 2pqk \pm b\ )^2 \ (mod\ 4pq)$

$$\equiv (2pqk)^2 \pm 2.2pqk.b + b^2 \ (mod\ 4pq)$$
$$\equiv 4p^2q^2k^2 \pm 4pqkb + b^2 \ (mod\ 4pq)$$
$$\equiv 4pqk(pqk \pm b) + b^2 \ (mod\ 4pq)$$
$$\equiv b^2 \ (mod\ 4pq).$$

Therefore, $x \equiv 2pqk \pm b \ (mod\ 4pq)$ gives the solutions of the congruence under consideration.
But for$k = 2$, the solutions reduces to $x \equiv 2pq.2 \pm b \ (mod\ 4pq)$

$\equiv 4pq \pm b\ (mod\ 4pq)$
$\equiv 0 \pm b\ (mod\ 4pq)$

These are the same solutions as for $k = 0$.
Also for $k = 3$, the solutions reduces to $x \equiv 2pq.3 \pm b\ (mod\ 4pq)$
$\equiv 2pq(2+1) \pm b(mod\ 4pq)$
$\equiv (4pq + 2pq) \pm b\ (mod\ 4pq)$
$\equiv (0 + 2pq) \pm b\ (mod\ 4pq)$
$\equiv 2pq \pm b\ (mod\ 4pq)$

These are the same solutions as for $k = 1$.
Thus, all the solutions are $x \equiv 2pqk \pm b\ (mod\ 4pq); k = 0, 1$.
This gives four of the eight solutions of the congruence.
For the remaining four solutions, consider $x \equiv \pm(2pk \pm b)\ (mod\ 4pq)$.
Then, $x^2 \equiv \{\pm(2pk \pm b)\}^2\ (mod\ 4pq)$
$\equiv 4p^2k^2 \pm 2.2pk.b + b^2\ (mod\ 4pq)$
$\equiv 4pk(pk \pm b) + b^2\ (mod\ 4pq)$
$\equiv 4p\ .k\ (pk \pm b) + b^2\ (mod\ 4pq)$
$\equiv 4p(qt)$, if k.$(pk \pm b) = qt, for\ an\ integer\ t$
$\equiv 4pqt + b^2\ (mod\ 4pq)$
$\equiv b^2\ (mod\ 4pq)$.

Thus, the other four solutions are given by:
$x \equiv \pm(2pk \pm b), \quad if\ k.(pk \pm b) = qt, for\ some\ positive\ integer\ t.$
Therefore, the congruence $x^2 \equiv b^2(mod\ 4pq)$ has eight solutions; the four are given by
$x \equiv 2pqk \pm b\ (mod\ 4pq)$.
Other four solutions are $x \equiv \pm(2pk \pm b)(mod\ 4pq),\ when\ k(pk \pm b) = qt,$
$for\ positive\ integer\ t.$

Case-II: $a = p\ or\ q$.
In this case the congruence becomes $x^2 \equiv p^2\ (mod\ 4pq);\ x^2 \equiv q^2\ (mod\ 4pq)$.
Then it can be clearly seen that the congruence must have four incongruent solutions.
It is seen that $x \equiv 2pqk \pm b\ (mod\ 4pq)$ satisfy the congruence and hence give the solutions of the congruence. It gives the required four solutions for$k = 0, 1$.

ILLUSTRATIONS

We illustrate the methods by giving an example and solving the congruence by both the methods.

Example-1: Consider $x^2 \equiv 49\ (mod\ 60)$ with $60 = 4.3.5$ and so $p = 5, q = 3$.
It can be written as: $x^2 \equiv 7^2(mod\ 60)$
It is of the type: $x^2 \equiv a^2(mod\ 4pq)$
It has eight solutions. The four are given by
$x \equiv 2pqk \pm a\ (mod\ 4pq); k = 0, 1.$
$\equiv 2.3.5k \pm 7\ (mod\ 4.3.5)$
$\equiv 30k \pm 7\ (mod\ 60)$
$\equiv 0 \pm 7; 30 \pm 7\ (mod\ 60)$
$\equiv 7, 53; 23, 37\ (mod\ 60)$
Other four solutions are given by $x \equiv \pm(2pk \pm b)(mod\ 4pq),\ if\ k.(pk \pm b) = qt$
$for\ some\ integer\ t.$
So, $x \equiv \pm(2.5.k \pm 7)\ (mod\ 60), if\ 5k \pm 7 = 3t.$
$i.e.\ x \equiv \pm(10k \pm 7)(mod\ 60)\ if\ 5k \pm 7 = 3t.$
But $5.1 + 7 = 12 = 3.4\ giving\ k = 1$.
Thus, other two solutions are $x \equiv \pm(10.1 + 7) = \pm 17\ (mod\ 60)$
$i.e. x \equiv 17, 43\ (mod\ 60)$.
Also, $5.2 - 7 = 3 = 3.1\ giving\ k = 2$.
Then, other two solutions are $x \equiv \pm(10.2 - 7) = \pm 13\ (mod\ 60)$
$i.e.\ x \equiv 13, 47\ (mod\ 60)$.
Therefore, all the solutions are $x \equiv 7, 53; 17, 43; 13, 47; 23, 27\ (mod\ 60)$.
These are the same solutions obtained as in above by existed method but easily and in comparatively less time.

Example-2: Consider the congruence $x^2 \equiv 36\ (mod\ 140)$.
It can be written as $x^2 \equiv 6^2\ (mod\ 4.5.7)$.
It is of the type $x^2 \equiv a^2\ (mod\ 4.pq)\ with\ p = 5, q = 7, a = 6$.
It has eight solutions. The four are given by
$x \equiv 2pqk \pm a\ (mod\ 4pq); k = 0, 1.$
$\equiv 2.5.7k \pm 6\ (mod\ 4.5.7)$
$\equiv 70k \pm 6\ (mod\ 140)$

$\equiv 0 \pm 6; 70 \pm 6\ (mod\ 140)$
$\equiv 6, 134; 64, 76\ (mod\ 140)$
Other four solutions are given by
$x \equiv \pm(2pk \pm b)(mod\ 4pq),\ if\ k.(pk \pm b) = qt\ ,\ for\ some\ integer\ t.$
So, $x \equiv \pm(2.5.k \pm 6)\ (mod\ 140), if\ 5k \pm 6 = 7t.$
But also for $k = 3,\ 5.3 + 6 = 21 = 7.3$
$So,\ x \equiv \pm(10.3 + 6)\ (mod\ 140)$
$\equiv \pm 36(mod\ 140$
$\equiv 36, 104\ (mod\ 140).$
But for $k = 4,\ 5.4 - 6 = 14 = 7.2$
$So,\ x \equiv \pm(10.4 - 6)\ (mod\ 140)$
$\equiv \pm 34\ (mod\ 140$
$\equiv 34, 106\ (mod\ 140).$
The solutions are given by $x \equiv 6, 134; 64, 76; 34, 106; 36, 104$ (mod 140).
$\equiv 6, 34, 36, 64, 76, 104, 106, 134\ (mod\ 140).$

Example-3: consider the congruence $x^2 \equiv 49\ (mod\ 140)$.
It can be written as $x^2 \equiv 7^2\ (mod\ 4.5.7)$.
It is of the type $x^2 \equiv q^2\ (mod\ 4pq)$. Its four solutions are given by
$x \equiv 2pqk \pm a\ (mod\ 4pq); k = 0, 1.$
$\equiv 2.5.7k \pm 7\ (mod\ 4.5.7)$
$\equiv 70k \pm 7\ (mod\ 140).$
$\equiv 0 \pm 7; 70 \pm 7\ (mod\ 140)$
$\equiv 7, 133; 63, 77\ (mod\ 140).$
These are the required four solutions.

CONCLUSION

Therefore, it is concluded that for $a \neq p, a \neq q$, the congruence under consideration has eight solutions; four are given by $x \equiv 2pqk \pm a\ (mod\ 4pq); k = 0, 1$. The other four solutions are given by $x \equiv \pm(2pk \pm b)(mod\ 4pq),\ if\ k.(pk \pm b) = qt\ ,\ for\ some\ integer\ t$. But for
$a = p\ or\ a = q$, the congruence has exactly four solutions given by
$x \equiv 2pqk \pm a\ (mod\ 4pq); k = 0, 1.$
Thus a simpler, less time-consuming new method of finding solutions (directly) of a solvable quadratic congruence of even composite modulus is developed.

Merits of proposed method:

This formulation is very simple and easier. It takes less time to get the solutions of the congruence. We need not use the Chinese Remainder Theorem which is a time-consuming method. The formulation solves the problem directly $i.e.$ solves the quadratic congruence without expliting into standard quadratic congruence of prime modulus.

REFERENCES

[1] Roy B M, *Formulation of solutions of standard quadratic congruence of even composite modulus as a product of two odd primes & four*, International Journal of Recent Innovation in Academic Research (IJRIAR), ISSN: 2635-3040, Vol-02, Issue-02, June-18.
[2] Niven I., Zuckerman H. S., Montgomery H. L. (1960, Reprint 2008), *"An Introduction to The Theory of Numbers"*, 5/e, Wiley India (Pvt) Ltd.
[3] Koshy Thomas, *Elementary Number Theory with Applications*, 2/e, Academic press.
[4] Roy B M, *Formulation of solutions of standard quadratic congruence of even composite modulus- a product of power of an odd prime & four times of another odd primes*, International Journal of Scientific Research & Engineering Development (IJSRED), ISSN: 2581-7175, Vol-03, Issue-03, May-20.
[5] Roy B M, *Formulation of solutions of standard quadratic congruence of even composite modulus- a product of twice an odd prime &power of another odd prime* (IJRTI), ISSN: 2456-3315, Vol-05, Issue-05, May-20.
{6] Roy B M, *Solving a standard quadratic congruence of composite modulus modulo a product of two different odd primes in two special cases*, International Journal of Scientific Research & Engineering Development (IJSRED), ISSN: 2581-7175, Vol-03, Issue-04, Jul-Aug-20.