[*Roy* et al., 5(5): May, 2018*]

ISSN: 2349-5197
Impact Factor: 3.765

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

FORMULATION OF SOLUTIONS OF STANDARD QUADRATIC CONGRUENCE OF EVEN COMPOSITE MODULUS

Prof. B. M. Roy
Head, Dept. of Mathematics, Jagat Arts, Commerce & I H P Science college, Goregaon (Gondia).
Affiliated to RTM Nagpur University (INDIA)

DOI: 10.5281/zenodo.1254399

Keywords: Chinese Remainder Theorem, even composite modulus, Quadratic Congruence.

Abstract
In this paper, a formula for finding solutions of a solvable standard quadratic congruence of even composite modulus as a product of two different primes is established. It solves the problem directly. It saves time of calculation. Formulation is the merit of the paper

Introduction
A congruence $x^2 \equiv a \ (mod\ m)$ is a standard quadratic congruence in an unknown x.
If m is a prime positive integer, then the congruence is called a congruence of prime modulus. If m is a composite integer, then the congruence is called a standard quadratic congruence of composite modulus. Here we consider the congruence $x^2 \equiv a \ (mod\ 2pq)$and has four incongruent solutions [2].

Need of research
The congruence under consideration can be solved by using Chinese Remainder Theorem; it takes a long time to find all the solutions. It is not a fair method for students. No formulation is found in the literature of mathematics. Here lies the need of this research. I tried my best to formulate the congruence and the effort is presented in this paper.

Problem-statement
Formulation of a solvable standard quadratic congruence of even composite modulus:
$x^2 \equiv a \ (mod\ 2pq)$ ……………………………………………………………………………………..(1)
$where\ p, q$ are distinct positive odd primes with $q < p$.

Discussion of existed method [2]
Consider the congruence (1).
It can be explit into three congruence:
$x^2 \equiv 1 \ (mod\ 2)$ ……………………………….………….(i)
$x^2 \equiv a \ (mod\ p)$ ……………………………………………(ii)
$x^2 \equiv a \ (mod\ q)$ ……………………………………………..(iii)

These standard quadratic congruence can be solved separately to get solutions:
$x \equiv 1 \ \ (mod\ 2)$ ……………………………………….(iv)
$x \equiv c,\ d \ \ (mod\ p)$ …………………………………..….(v)
$x \equiv e,\ f \ \ (mod\ q)$ ………………………………..…..(vi)

as "every solvable quadratic congruence of positive odd prime modulus has exactly two solutions [2].

Solving these**, four solutions** can be obtained using **Chinese Remainder Theorem.**

Demerits of the proposed method:
Definitely, use of "Chinese Remainder Theorem" is a time-consuming calculation. It sometimes becomes a boring task because it is complicated.

Discussion of Proposed method (Formulation)

Consider the congruence (1).
If $a = b^2$, then the congruence becomes $x^2 \equiv b^2 (mod\ 2pq)$.

Two obvious solutions of the congruence are: $x \equiv 2pq \pm b\ (mod\ 2pq)$.
$i.e.\ \ x \equiv 2pq + b,\ 2pq - b\ \ (mod\ 2pq)\ \ i.e.\ x \equiv b,\ \ 2pq - b\ \ (mod\ \ 2pq)$.

Thus, b is a solution of $x^2 \equiv b^2(mod\ 2pq)$.

If $a \neq b^2$,then we add "$2kpq$" to a to get $a + 2kpq\ with\ such\ a\ k\ such\ that\ a + 2kpq = b^2$.

Then, the two obvious solutions are as before.

Now, for the other two solutions let $x = \pm(2pk \pm b)$,
we have

$$x^2 = \{\pm(2pk \pm b)\}^2$$
$$= 4p^2k^2 \pm 4pkb + b^2$$
$$= b^2 + 4pk(pk \pm b)$$
$$= b^2 + 4p(qt)$$
$$= b^2 + 2t(2pq)\ ,\ \text{if } k(pk\ \pm b) = qt, for\ an\ integer\ t.$$
$$\equiv b^2\ \ (mod\ 2pq),\ \text{if } k(pk\ \pm b) = qt.$$

Thus, the other two solutions are given by:

$$x \equiv \pm(2pk \pm b),\qquad if\ k(pk \pm b) = qt, for\ some\ positive\ integer\ t.$$

Therefore, the congruence $x^2 \equiv b^2(mod\ 2pq)$ has two obvious solutions
$x \equiv \pm b\ (mod\ 2pq)$; and other solutions are $x \equiv \pm(2pk \pm b)(mod\ 2pq)$,
$when\ k(pk \pm b) = qt, for\ positive\ integer\ t.$

Illustration of method by an Example

Consider the congruence: $x^2 \equiv 4\ (mod\ 42)$. Here, $42 = 2.3.7\ with\ p = 7, q = 3$.
Thus, the congruence is of the type: $x^2 \equiv a\ (mod\ 2pq)$.

Solution by existed Method:
Consider $x^2 \equiv 4\ (mod\ 42)$.
We see that $42 = 2.3.7$

So, the congruence can be explit into the following congruence:

$$x^2 \equiv 4\ (mod\ 2)\quad i.e.\ x^2 \equiv 0\ (mod\ 2)\ giving\ solutions\ \ x \equiv 0\ (mod\ 2)$$
$$x^2 \equiv 4\ (mod\ 3)\quad i.e.\ x^2 \equiv 1\ \ (mod\ 3)\ giving\ solutions\ x \equiv 1, 2\ (mod\ 3)$$
$$x^2 \equiv 4\ (mod\ 7)\quad i.e. x^2 \equiv 4\ (mod\ 7)\ giving\ solutions\ x \equiv 2, 5\ \ (mod\ 7)$$

We consider the congruence for Chinese remainder Theorem.

Thus, we have $x \equiv 0\ (mod\ 2)$; $x \equiv 1, 2\ (mod\ 3)$; $x \equiv 2, 5\ \ (mod\ 7)$.
So, $a_1 = 0;\ \ a_2 = 1\ \ or\ \ 2;\ \ \ a_3 = 2\ \ or\ \ 5;\ \ m_1 = 2;\ \ m_2 = 3;\ \ m_3 = 7.$
We have, $M = [2, 3, 7] = 42;\ M_1 = 21;\quad M_2 = 14;\quad M_3 = 6.$
Now, $M_1x \equiv 1\ (mod\ m_1)\ \ i.e. 21x \equiv 1\ (mod\ 2)\ \ i.e.\ x \equiv 1\ (mod\ 2) giving\ x_1 = 1.$

$$M_2x \equiv 1\ (mod\ m_2)\quad i.e. 14x \equiv 1\ (mod\ 3)\quad i.e.\ x \equiv 2\ (mod\ 3) giving\ x_2 = 2.$$
$$M_3x \equiv 1\ (mod\ m_3)\quad i.e. 6x \equiv 1\ (mod\ 7)\quad i.e.\ x \equiv -1\ (mod\ 7) giving\ x_3 = -1.$$

The common solutions are given by $x_0 \equiv a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3(mod\ M)$.
Putting values one must get $x_0 \equiv 2, 40; 16, 26\ (mod\ 42)$**[calculations not shown].**

Isn't a time-consuming method??

Solution by Formulation:

Consider $x^2 \equiv 4\ (mod\ 42)$.

It can be written as: $x^2 \equiv 4 = 2^2 (mod\ 42)$ giving solutions $x \equiv \pm 2\ (mod\ 42)$
$i.e.\ x \equiv 2, 40\ \ (mod\ 42)$. Therefore, $b = 2$ is a solution.

Other two solutions are given by $x \equiv \pm(2pk \pm b)(mod\ 2pq),\ if\ k(pk \pm b) = qt, for\ some\ integer\ t.$
So, $x \equiv \pm(2.7.k \pm 2)(mod\ 42),\ if\ k(7k \pm 2) = 3t$
$i.e.\ x \equiv \pm(14k \pm 2)\ \ (mod\ 42)\ if k(\ 7k \pm 2) = 3t.$

But $1.(7.1 + 2) = 9 = 3.3\ giving\ k = 1$

Thus, other two solutions are $x \equiv \pm(14.1 + 2) = \pm 16\ (mod\ 42)\ i.e. x \equiv 16, 26\ (mod\ 42)$.
Therefore, all the solutions are $x \equiv 2, 40; 16, 26\ (mod\ 42)$.

These are the same solutions obtained as in above by existed method but easily and in comparatively less time.

Conclusion

Thus a simpler, less time-consuming new method of finding solutions (directly) of a solvable quadratic congruence of even composite modulus of the type $x^2 \equiv a^2\ (mod\ 2pq)\ \ with\ p, q\ are\ odd\ primes,$ is developed.No need to use Chinese Remainder Theorem. ***This is the merit of this paper***.

References

[1] Niven I., Zuckerman H. S., Montgomery H. L. (1960, Reprint 2008), "An Introduction to The Theory of Numbers", 5/e, Wiley India (Pvt) Ltd.
[2] Koshy Thomas, Elementary Number Theory with Applications, 2/e, Academic press.
[3] Burton David, Elementary number theory, 7/e, Mac Graw Hill.
[4] Roy B. M., Discrete Mathematics & Number Theory, 1/e, Das Ganu Prakashan, Nagpur, INDIA.