iJETRM
International Journal of Engineering Technology Research & Management

RP-118: A REVIEW & RE-FORMULATION OF THE SOLUTIONS OF A STANDARD QUADRATIC CONGRUENCE OF EVEN COMPOSITE MODULUS-A POWER OF AN ODD PRIME

Prof. B M Roy
M. Sc. (mathematics); Hon. Ph. D., Hon. D. Sc.
Head, Dept. of Mathematics
Jagat Arts, Commerce & I H P Science college, Goregaon,
Dist- GONDIA (M.S), India, Pin-441801
(Affiliated to RTM Nagpur University, Nagpur)

ABSTRACT
In this paper, a standard quadratic congruence of even composite modulus-a power of an odd prime, is reviewed and reformulated. It is a review and reformulation of the author's previously published paper- "Formulation of Solutions of a Special Class of Standard Quadratic Congruence of Even Composite Modulus". The formulae established are tested true by citing numerical examples for different cases. Formulation is the merit of the paper. No need to use the preferred Chinese Remainder Theorem.

Keywords:
Composite modulus, Prime integer, Quadratic congruence, Reformulation.

INTRODUCTION

The author has formulated many standard quadratic congruence of prime and composite modulus. Here is another quadratic congruence considered for the formulation of its solutions. It is found that a little attempt had been made for formulation of the solutions of the congruence. Readers preferred to use Chinese Remainder Theorem to solve the congruence, which takes a long time. For the time saving purpose, the author has tried his best to formulate the congruence and his efforts are presented in this paper.

REVIEW OF LITERATURE

It is known that the congruence $x^2 \equiv a^2 \ (mod\ 2^m), m \geq 3$ has exactly 4- solutions,
if $a \equiv 1 \ (mod\ 8)$[1].
The congruence $x^2 \equiv a^2 \ (mod\ p^n)$ with $n \geq 1$& p odd prime, has exactly two solutions [1].
Then the congruence $x^2 \equiv a^2 \ (mod 2^m.p^n)$ has (2). (4) = 8 solutions for odd a $i.e.$
$a \equiv 1 \ (mod\ 8)$[1].
But if a≠1 (mod 8) $i.e. if\ a\ is\ even\ integer, then$ nothing is said about the solutions of the congruence.
Also, it was not mentioned what happened if $a = p, a = 2p.$
The author found that such types of congruence are solvable and need some formulation.
Here the author wishes to consider all such cases for its formulation.

NEED OF THIS REFORMULATION

No direct formula is found in the literature of mathematics; but only a method is mentioned i. e. Chinese Remainder Theorem. It takes a long time to find all the solutions [2]. We need a time-saving method or formulation. Also, author's previous formulation needs reformulation. There author didn't consider these cases. This is the need of the research. The author wished to formulate the congruence for the benefit the readers / students in different case.

PROBLEM STATEMENT

"To review and re-formulate the congruence: $x^2 \equiv a^2$ (mod $2^m.p^n$), $m \geq 4$, p being an odd prime integer in four cases:
Case-I: when a is odd positive integer and $a = p$,

iJETRM
International Journal of Engineering Technology Research & Management

Case-II: when a is odd positive integer and a$\neq p$,

Case-III: when a is even positive integer and $a = 2p$;

Case-IV: when a is even positive integer and $a \neq 2p$.

ANALYSIS & RESULT

Case-I:

Let a be odd positive integer and $a = p$.

For the solutions, consider $x = 2^{m-1}p^{n-1}k \pm a; n \geq 2, k = 0, 1, 2, 3, \ldots\ldots\ldots$

Then $x^2 = (2^{m-1}.p^{n-1}k \pm a)^2$

$$- 2^{2m-2}.p^{2n-2}k^2 \pm 2.2^{m-1}.p^{n-1}k.a + a^2$$
$$= 2^m.p^{n-1}k\{2^{m-2}p^{n-1}k \pm a\} + a^2$$
$$= 2^m.p^nk\{2^{m-2}p^{n-2}k \pm 1\} + a^2; \ if\ a = p.$$
$$\equiv a^2 \ (mod\ 2^m.p^n)$$, if a is odd positive integer & a = p.

Thus, $x \equiv 2^{m-1}p^{n-1}.k \pm a \ (\mathrm{mod}\ 2^mp^n)$ are the solutions for $k = 0, 1, 2, 3, \ldots\ldots$

But if $k = 2p$, then $x = 2^{m-1}p^{n-1}.2p \pm a$

$$= 2^mp^n \pm a$$
$$\equiv \pm a \ (mod\ 2^mp^n)$$, which is the same solution as for $k = n$.

For $k = 2p + 1$, it can be easily seen that the solution is the same as for $k = 1$.

Therefore, it can be concluded that the congruence has $2(2p) = 4p$ solutions as for a single value of k, the congruence has exactly two solutions.

Thus, all the solutions can be given by

$x \equiv 2^{m-1}p^{n-1}.k \pm a \ (\mathrm{mod}\ 2^mp^n); k = 0,1, \ldots\ldots, (p-1).$

Case-II: Let a be odd positive integer and $a \neq p$.

Consider $x \equiv 2^{m-1}p^nk \pm a \ (mod\ 2^mp^n); n > 1, k = 0, 1, 2, \ldots\ldots\ldots$

Then $x^2 \equiv (2^{m-1}p^n.k \pm a)^2$

$$\equiv 2^{2m-2}p^{2n}k^2 \pm 2.2^{m-1}p^nka + a^2$$
$$\equiv 2^mp^nk\,(2^{m-2}p^nk \pm a) + a^2$$
$$\equiv a^2 \ (mod\ 2^mp^n)$$

Thus, $x \equiv 2^{m-1}p^nk \pm a \ (mod\ 2^mp^n)$ are the solutions of the congruence.

But for $k = 2, x \equiv 2^{m-1}p^n.2 \pm a \equiv 2^mp^n \pm a \equiv \pm a \ (mod\ 2^mp^n)$which are the same solutions for $k = 0$. For other higher values of k, the solutions repeats.

Thus, $k = 0, 1$ gives four solutions of the congruence. But, as per [2], the congruence must have eight solutions. Therefore, other four solutions yet remains to formulate.

For the other four solutions of the congruence consider: $x \equiv \pm(2kp^n \pm a) \ (mod\ 2^mp^n)$

Therefore, $x^2 \equiv (2kp^n \pm a)^2 \ (mod\ 2^mp^n)$

$$\equiv 4k^2p^{2n} \pm 2.2kp^n.a + a^2$$
$$\equiv 4k^2p^{2n} \perp 4kp^n.a + a^2$$
$$\equiv 4kp^n(kp^n \pm a) + a^2$$
$$\equiv 4p^nk(kp^n \pm a) + a^2;$$
$$\equiv 2^mp^nt + a^2, \ if\ k(kp^n \pm a) = 2^{m-2}t.$$
$$\equiv a^2 \ \ (mod\ 2^mp^n)$$

Thus other four solutions are $x \equiv \pm(2kp^n \pm a) \ (mod\ 2^mp^n)$.

iJETRM
International Journal of Engineering Technology Research & Management

Therefore, the congruence has exactly eight solutions.

Case-III: Let a be even positive integer and $a = 2p$.

Then, consider $x = (2^{m-2}.p^{n-1}k \pm a) \pmod{2^m.p^n}$; $n \geq 2, k = 0, 1, 2, 3, 4, 5, \ldots\ldots\ldots$

Then, $x^2 \equiv (2^{m-2}p^{n-1}k \pm a)^2 \equiv 2^{2m-4}p^{2n-2}k^2 \pm 2.2^{m-2}.p^{n-1}k.a + a^2$

$\equiv 2^{m-1}.p^{n-1}k\{2^{m-3}.p^{n-1}k \pm a\} + a^2$

$\equiv 2^{m-1}.p^{n-1}k\{2pt\} + a^2$, if $a = 2p$,

$\equiv 2^m.p^n.kt + a^2$

$\equiv a^2 \pmod{2^m.p^n}$

Thus, $x \equiv (2^{m-2}.p^{n-1}k \pm a) \pmod{2^m.p^n}$ are the solutions, if $a = 2p$, an even integer.

But if $k = 4p, then\ x = (2^{m-2}.p^{n-1}.4p + a)$

$= (2^m p^n \pm a)$

$\equiv \pm a \pmod{2^m.p^n}$ which is the same solutions as for $k = 0$.

Similarly, for $k = 4p + 1, 4p + 2, \ldots\ldots$ the same solutions repeats as for $k = 1, 2$.

Therefore, the above congruence has 8p solutions as for every value of

$a, the\ congruence\ has\ exactly\ two$ solutions.

Thus, for a =2p, the congruence has 8p solutions.

These are: $x \equiv (2^{m-2}.p^{n-1}k \pm a) \pmod{2^m.p^n}; m > 4, k = 0, 1, 2, \ldots\ldots\ldots, 4p - 1.$

Case-IV:

Let a be even positive integer and $a \neq 2p$.

Then, consider $x \equiv (2^{m-2}.p^n k \pm a) \pmod{2^m.p^n}; k = 0, 1, 2, 3, 4, 5, \ldots\ldots\ldots$

Then, $x^2 \equiv (2^{m-2}p^n k \pm a)^2 \equiv 2^{2m-4}p^{2n}k^2 \pm 2.2^{m-2}.p^n k.a + a^2$

$\equiv 2^{m-1}.p^n k\{2^{m-3}.p^n k \pm a\} + a^2$

$= 2^{m-1}.p^n k\{2t\} + a^2$, if a is even.

$\equiv 2^m.p^n.k + a^2$

$\equiv a^2 \pmod{2^m.p^n}$

Thus, $x \equiv (2^{m-2}.p^n k \pm a) \pmod{2^m.p^n}$ are the solutions, if a is even integer.

But if $k = 4, then\ x = (2^{m-2}.p^n.4 \pm a)$

$-(2^m p^n \pm a)$

$\equiv \pm a \pmod{2^m.p^n}$ which is the same solutions as for $k = 0$.

Similarly, for $k = 5, 6, 7, 8 \ldots\ldots$ The same solutions repeats as for $k = 1, 2, 3, 0$.

Therefore, the above congruence has eight solutions if a is even integer and the solutions are

$x \equiv (2^{m-2}.p^n k \pm a) \pmod{2^m.p^n}$.

ILLUSTRATIONS

(1) Consider the congruence $x^2 \equiv 25 \pmod{400}$

Here, $400 = 16.25 = 2^4.5^2\ with\ m = 4; n = 2\ and\ p = a = 5$.

The congruence can be written as $x^2 \equiv 5^2 \pmod{2^4.5^2}\ \ with\ a = p = 5, an\ odd\ integer$.

Thus the congruence has 2 (2p) = 2(2.5) = 20 solutions given by

$x \equiv (2^{m-1}.p^{n-1}.k \pm a) \pmod{2^m.p^n}; k = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.$

$x \equiv (2^3.5.k \pm 5) \pmod{2^4.5^2}$

$\equiv (40k \pm 5) \pmod{400}; k = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.$

$\equiv 0 \pm 5; 40 \pm 5; 80 \pm 5; 120 \pm 5; 160 \pm 5; 200 \pm 5; 240 \pm 5; 280 \pm 5; 320 \pm 5;$

iJETRM
International Journal of Engineering Technology Research & Management

$360 \pm 5\ (mod\ 400)$.
$\equiv 2, 398; 35, 45; 75, 85;\ 115, 125; 155, 165; 195, 205; 235, 245;$
$275, 285; 315, 325;\ 355, 365\ (mod\ 400)$
These are the twenty solutions of the congruence.

(2) Consider the congruence $x^2 \equiv 9\ (mod\ 400)$
Here, $400 = 16.25 = 2^4.5^2\ with\ m = 4, n = 2, and\ p = 5, a = 3; a \neq p.$
The congruence can also be written as: $x^2 \equiv 3^2 (mod\ 2^4.5^2)\ \ with\ a = 3, an\ odd\ integer$
Thus the congruence has eight solutions.
Four solutions are given by

$$x = 2^{m-1}p^n k \pm a\ (mod\ 2^m.p^n); k = 0, 1.$$
$$\equiv 2^3 5^2 k \pm 3\ (mod\ 2^m.p^n);$$
$$\equiv (200k \pm 3); k = 0, 1.$$
$$\equiv \mathbf{0} \pm 3;\ 200 \pm 3\ (mod\ 400)$$
$$\equiv \mathbf{3, 397}; \mathbf{203, 197}\ (\text{mod } 400).$$

Other four solutions are given by
$$x \equiv\ +(2kp^n + a\ (mod\ 2^m p^n)$$
$$\equiv \pm(2k.25 \pm 3)\ \ (mod\ 400\ )$$
$$\equiv \pm(50k \pm 3)\ \ (mod\ 400); \text{ if } k(kp^n \pm a) = k(25k \pm 3) = 2^{4-2}t$$
$$\equiv \pm(50k \pm 3)\ \ (mod\ 400); \text{ if } k(kp^n \pm a) = k(25k \pm 3) = 4t$$
$$\equiv \pm(50 + 3);\ \pm(150 - 3)\ \ (mod\ 400); \text{ if } \ k = 1, 6$$
$$\equiv \pm 53;\ \pm 147\ \ (mod\ 400);$$
$$\equiv 53, 347; 147, 253\ (mod\ 400).$$

Thus all the eight solutions are: $\boldsymbol{x \equiv 03, 397; 203, 197;\ 53, 347; 147, 253 (mod\ 400).}$

Let us consider another example. $x^2 \equiv 25\ (mod\ 96)$. Here $25 \equiv 1\ (mod\ 8)$.
and $96 = 32.3 = 2^5.3^1\ with\ n = 5\ and\ p = 3.$
The congruence can also be written as $x^2 \equiv 5^2 (mod\ 2^5.3^1)\ \ with\ a = 5\ and\ a \neq p.$
Thus, the congruence has eight solutions.
The four solutions are given by

$$x \equiv \left(2^{m-1}.p^n.k \pm a\right)\ \ (mod\ 2^m.p^n); k = 0, 1.$$
$$\equiv \left(2^{5-1}.3^1.k \pm 5\right)\ \ \left(mod\ 2^5.3^1\right)$$
$$\equiv\ 48k \pm 5\ \ (mod\ 96)$$
$$\equiv \pm 5; 48 \pm 5\ (mod\ 96)$$
$$\equiv 5, 91; 43, 53\ \ (mod\ 96).$$

Other four solutions are given by $x \equiv \pm(2kp^n \pm \mathrm{a}),\ \text{if } \mathrm{k}(\mathrm{kp}^n \pm \mathrm{a}) = 2^{m-2}\mathrm{t}$
$$\equiv \pm(2k.3 \pm 5),\quad if\ k(k.3 \pm 5) = 2^3 t = 8t$$
$$\equiv \pm(6k \pm 5),\quad if\ \ k(3k \pm 5) = 8t$$

Here, it can be seen that for $k = 1,\ \ 1(3.1 + 5) = 8;$
hence the solutions are $x \equiv \pm(6 + 5) - \pm 11 - 11, 85.$
Also for $k = 7,\ \ 7(3.7 - 5) = 7.16 = 8t,$ the solutions are $x \equiv \pm(42 - 5) = \pm 37 = 37, 59.$
Thus all the required solutions are: $\boldsymbol{x = 5, 91; 43, 53;\ 11, 85;\ 37, 59\ (mod\ 96).}$

Consider the congruence $x^2 \equiv 36\ (mod 288)$

iJETRM
International Journal of Engineering Technology Research & Management

It can be written as $x^2 \equiv 6^2 \ (mod 32.9) i.e. x^2 \equiv 6^2 \ (mod 2^5.3^2)$
Here, $p = 3, a = 6 = 2.3 = 2p$.
The congruence has $8p = 8.3 = 24$ solutions, given by

$$x \equiv 2^{m-2}p^{n-1}k \pm a \ (mod\ 2^m p^n); k = 0, 1, 2, \ldots\ldots\ldots, 4p-1.$$
$$= 2^{5-2}3^{2-1}k \pm 6 \ (mod\ 2^5 3^2)$$
$$\equiv 2^3 3^1 k \pm 6 \ (mod\ 32.9)$$
$$\equiv 24k \pm 6 \ (mod\ 288); k = 0, 1, 2, \ldots\ldots., 11.$$
$$\equiv 0 \pm 6; 24 \pm 6; 48 \pm 6; 72 \pm 6; 96 \pm 6; 120 \pm 6;$$
$$144 \pm 6; 168 \pm 6; 192 \pm 6; 216 \pm 6; 240 \pm 6; 264 \pm 6 \ (mod\ 288)$$

≡6, 282; 18, 30; 42, 54; 66, 78; 90, 102; 114, 126; 138, 150; 162, 174; 186, 198; 210, 222; 234, 246; 258, 270 $(mod\ 288)$
These are the required 24 solutions.
Similarly, the congruence $x^2 \equiv 100 \ (mod\ 800)$ must have 40 solutions.

CONCLUSION

Thus, the solutions of the standard quadratic congruence of composite modulus of the type:
$x^2 \equiv a^2 \ (mod\ 2^m.p^n)$, with p a prime integer, is formulated in four different cases.
The established formulae are tested by solving some examples. It is a very quick method to find all the solutions. One need not use the Chinese Remainder Theorem but the established author's formulation.

MERIT OF THE PAPER

The review and reformulation of author's previous paper is done. A new formulation is developed and discussed fully. It is a corrective-measure of the previous paper. This is the merit of the paper.

REFERENCE

[1] Koshy, Thomas; Elementary Number Theory with Applications; 2/e; 2009, Academic press.
[2] Niven, I.; Zuckerman H S.; Montgomery H L. An Introduction to the Theory of Numbers; 5/e; 2008, WSE.
[3] Roy B M, *A New method of finding solutions of a solvable standard quadratic congruence of comparatively large prime modulus*, International Journal of Advanced research, Ideas and Innovations in Technology (IJARIIT), ISSN: 2454-132X, Vol-04, Issue-03, May-18.
[4] Roy B M, *Formulation of solutions of some classes of standard quadratic congruence of composite modulus as a product of prime-power integer by two and four*, International Journal of Research Trends and Innovation (IJRTI), ISSN: 2456-3315, Vol-03, Issue-05, May-18.
[5] Roy B M, *Formulation of solutions of standard quadratic congruence of even composite modulus as a product of two odd primes and four*, International Journal of Research Innovation in Academic Research (IJRIAR), ISSN: 2635-3040, Vol-02, Issue-02, Jun-18
[6] Roy B M, *Formulation of standard quadratic congruence of even composite modulus*, International Journal of International Journal of Scientific development and research (IJSDR), ISSN: 2455-2631, Vol-03, Issue-08, Ahg-18.
[7] Roy B M, *An algorithmic formulation of solving standard quadratic congruence of prime power modulus*, International Journal of Advanced research, Ideas and Innovations in Technology (IJARIIT), ISSN: 2454-132X, Vol-04, Issue-06, Nov-Dec-18.
[8] Roy B M, *Formulation of a class of solvable standard quadratic congruence of even composite modulus*, International Journal of Research Trends and Innovation (IJRTI), ISSN: 2456-3315, Vol-04, Issue-03, Mar-19.
[9] Roy B M, *Formulation of solutions of a special standard quadratic congruence of composite modulus-an even multiple of power of an odd positive integer*, International Journal of Advanced research, Ideas and Innovations in Technology (IJARIIT),, ISSN: 2454-132X, Vol-05, Issue-05, Sep-Oct-19.