RP-57: Formulation of Solutions of Standard Quadratic Congruence of Even Composite Modulus-a product of Two Powered Odd Primes in Two Special Cases

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 paper, the author considered a very special type of standard quadratic congruence of even composite modulus- a product of two powered odd primes in two special cases for formulation of its solutions. The formulation discovered is justified and verified by solving some suitable examples. No need to use Chinese remainder Theorem.**

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

INTRODUCTION

Here, a standard quadratic congruence of even composite modulus- a product of two powered odd primes in two special cases, is discussed and formulated. It is of the type: $x^2 \equiv a^2 \pmod{2^r p^m q^n}$, p being a positive prime integer & m, n, r positive integers. Such type of standard quadratic congruence is not formulated earlier.

LITERATURE REVIEW

In different books on Number Theory, no formulation is found for the said congruence. Much had been written on standard quadratic congruence of prime modulus. A short discussion is given by Thomas Koshy [1]. He used Chinese Remainder Theorem for solutions.

In this paper, the author took the opportunity of formulating the congruence for solutions. The author formulated many standard quadratic congruence of composite modulus [2], [3], [4], [5], [6], [7], [8]. In this sequence of formulation the author found this present quadratic congruence unformulated and hence it is considered.

NEED OF RESEARCH

The literature of mathematics do not show any formulation of solutions of the said congruence except the Chinese Remainder Theorem (CRT). It is a very lengthy procedure. It is not a good method for readers. It is time-consuming and to have remedy, formulation is necessary. This is the need of my research.

PROBLEM-STATEMENT

Here the problem is-"To formulate the solutions of the standard quadratic congruence of even composite modulus of the type: $x^2 \equiv a^2 \pmod{2^r p^m q^n}$

with p an odd prime & m, n, r positive integer in two special cases:

Case-I: $a = p$,

Case-II: $a = q$.

ANALYSIS & RESULTS

Here the author wishes to discuss the existed method in brief.

Solution by Existed Method

Consider the case-I. Let $a = p$.

In the existed method, to apply CRT, the congruence under consideration is split into individual congruence as:

$$x^2 \equiv p^2 \pmod{2^r} \dots\dots\dots\dots\dots\dots (1)$$

$$x^2 \equiv p^2 \pmod{p^m} \dots\dots\dots\dots\dots\dots\dots\dots (2)$$

$$x^2 \equiv p^2 \pmod{q^n} \dots\dots\dots\dots\dots\dots\dots\dots\dots (3).$$

The congruence (1) has four solutions if $r \geq 3$.

The congruence (2) has exactly p-solutions and the congruence (3) has exactly two solutions.

So, the congruence under consideration must have 4.p.2= 8p solutions [2].

These solutions can be obtained by solving the individual congruence separately and the common solutions are obtained nu using CRT.

Now consider the case-II.

Let $a = q$. As in above, the individual congruence are:

$$x^2 \equiv q^2 \pmod{2^r} \dots\dots\dots\dots\dots\dots (1)$$

$$x^2 \equiv q^2 \pmod{p^m} \dots\dots\dots\dots\dots\dots\dots\dots (2)$$

$$x^2 \equiv q^2 \pmod{q^n} \dots\dots\dots\dots\dots\dots\dots\dots\dots (3)$$

The congruence (1) has four solutions, if $r \geq 3$.

The congruence (2) each has exactly two solutions and the congruence (3) has exactly q- solutions.

So, the congruence under consideration must have 4.2.q = 8q solutions [1].

These solutions can be obtained by solving the individual congruence separately and the common solutions are obtained nu using CRT.

Formulation of Solutions

Consider the congruence: $x^2 \equiv a^2 \pmod{2^r p^m q^n}$.

Case-I: $a = p$.

Let us consider that $a = p$.

Consider $x \equiv 2^{r-1}p^{m-1}q^n k \pm p \pmod{2^r p^m q^n}$

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

$$\equiv (2^{r-1}p^{m-1}q^n k)^2 \pm 2.\, 2^{r-1}p^{m-1}q^n k.\, p + p^2 \pmod{2^r p^m q^n}$$

$$\equiv (2^{r-1}p^{m-1}q^n k)^2 \pm 2^r p^m q^n k + p^2 \pmod{2^r p^m q^n}$$

$$\equiv 2^r p^m q^n k(2^{r-2}p^{m-2}q^n k \pm 1) + p^2 \pmod{2^r p^m q^n}$$

$$\equiv p^2 \pmod{2^r p^m q^n}$$

But for $k = 2p$, the congruence has the same solution as for $k = 0$.

Thus, the solutions are $x \equiv 2^{r-1}p^{m-1}q^n k \pm p \pmod{2^r p^m q^n}; k = 0, 1, 2, \dots, (2p-1)$.

These are 4p-solutions of the congruence.

The remaining 4p-solutions, consider

$x \equiv \pm(2p^{m-1}q^n k \pm p) \pmod{2^r p^m q^n}$

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

$$\equiv (2p^{m-1}q^n k)^2 \pm 2.2p^{m-1}q^n k.\, p + p^2 \pmod{2^r p^m q^n}$$

$$\equiv (2p^{m-1}q^n k)^2 \pm 4p^m q^n k + p^2 \pmod{2^r p^m q^n}$$

$$\equiv 4p^m q^n k(p^{m-2}q^n k \pm 1) + p^2 \pmod{2^r p^m q^n}$$

$$\equiv 2^2 p^m q^n.\, 2^{r-2}t + p^2 \pmod{2^r p^m q^n}, \text{ if } p^{m-2}q^n k \pm 1 = 2^{r-2}t.$$

$$\equiv 2^r p^m q^n t + p^2 \pmod{2^r p^m q^n}$$

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

Thus, $x \equiv \pm(2p^{m-1}q^n k \pm p) \pmod{2^r p^m q^n}$; if $p^{m-2}q^n k \pm 1 = 2^{r-2}t$ gives the remaining solutions.

Case-II: $a = q$.

Let us consider that $a = q$.

Consider $x \equiv 2^{r-1}p^m q^{n-1}k \pm q \pmod{2^r p^m q^n}$

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

$\equiv (2^{r-1}p^m q^{n-1}k)^2 \pm 2.\, 2^{r-1}p^m q^{n-1}k.\, q + q^2 \pmod{2^r p^m q^n}$

$\equiv (2^{r-1}p^m q^{n-1}k)^2 \pm 2^r p^m q^n k + q^2 \pmod{2^r p^m q^n}$

$\equiv 2^r p^m q^n k(2^{r-2}p^m q^{n-2}k \pm 1) + q^2 \pmod{2^r p^m q^n}$

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

But for $k = 2q$, the solution is the same as for $k = 0$.

Thus, $x \equiv 2^{r-1}p^m q^{n-1}k \pm q \pmod{2^r p^m q^n}$ gives the $4q -$ solutions.

For the remaining solutions, consider

$x \equiv (2p^m qk \pm q) \pmod{2^r p^m q^n}$.

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

$\equiv (2p^m q^{n-1}k)^2 \pm 2.\, 2p^m q^{m-1}k.\, q + q^2 \pmod{2^r p^m q^n}$

$\equiv (2p^m q^{n-1}k)^2 \pm 4p^m q^n k + q^2 \pmod{2^r p^m q^n}$

$\equiv 4p^m q^n k(p^m q^{n-2}k \pm 1) + q^2 \pmod{2^r p^m q^n}$

$\equiv 2^2 p^m q^n.\, 2^{r-2}t + q^2 \pmod{2^r p^m q^n}$, **if** $k(p^m q^{n-2}k \pm 1) = 2^{r-2}t$.

$\equiv 2^r p^m q^n t + q^2 \pmod{2^r p^m q^n}$

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

Thus, $x \equiv \pm(2p^m q^{n-1}k \pm q) \pmod{2^r p^m q^n}$; if $k(p^m q^{n-2}k \pm 1) = 2^{r-2}t$ gives the remaining solutions.

ILLUSTRATIONS BY FORMULATION

Example-I:

Consider the congruence: $x^2 \equiv 9 \pmod{3600}$.

It can be written as $x^2 \equiv 3^2 \pmod{16.9.25}$ i.e. $x^2 \equiv 3^2 \pmod{2^4.3^2.5^2}$

It is of the type $x^2 \equiv a^2 \pmod{2^r p^m q^n}$ with $p = 3, q = 5$ & $a = 3$.

It has exactly $8p = 8.3 = 24$ solutions.

Its twelve solutions are given by:

$x \equiv 2^{r-1}p^{m-1}q^n k \pm q \pmod{2^r p^m q^n}$; $k = 0, 1, 2, \ldots\ldots\ldots, 2p-1$.

$\equiv 2^{4-1}3^1 5^2 k \pm 3 \pmod{2^4.3^2.5^2}$; $k = 0, 1, 2, 3, 4, 5$.

$\equiv 2^3.3^1.5^2 k \pm 3 \pmod{16.9.25}$

$\equiv 600k \pm 3 \pmod{3600}$

$\equiv 0 \pm 3; 600 \pm 3; 1200 \pm 3; 1800 \pm 3; 2400 \pm 3; 3000 \pm 3 \pmod{3600}$.

$\equiv 3, 3597; 597, 603;\ 1197, 1203;\ 1797, 1803; 2397, 2403; 2997, 3003 \pmod{3600}$

The other twelve solutions are given by

$x \equiv \pm(2p^{m-1}q^n k \pm q) \pmod{2^r p^m q^n}$; **if** $k(p^{m-2}q^n k \pm 1) = 2^{r-2}t$.

$\equiv \pm(2.3.25k \pm 3) \pmod{2^4.5^2 3^2}$

$\equiv \pm(150k \pm 3) \pmod{3600}$; **if** $25k \pm 1 = 4t$.

For k = 1, one have $25 - 1 = 24 = 4.6$

So, x $\equiv \pm(150 - 3) \pmod{2^r p^m q^n}$

$\equiv \pm 147$ **(mod 3600)**

$\equiv 147, 3453 \pmod{3600}$.

Also for k = 3, one have $25.3 + 1 = 76 = 4.19$

So, x $\equiv \pm(450 + 3) \pmod{3600}$

$\equiv \pm 453 \pmod{3600}$

$\equiv 453, 3147 \pmod{3600}$.

Also for k = 5, one have $25.5 - 1 = 124 = 4.31$

So, x $\equiv \pm(750 - 3) \pmod{3600}$

$\equiv \pm 747 \pmod{3600}$

$\equiv 747, 2853 \pmod{3600}$.

Also for k = 7, one have $25.7 + 1 = 176 = 4.44$

So, x $\equiv \pm(1050 + 3) \pmod{3600}$

$\equiv \pm 1053 \pmod{3600}$

$\equiv 1053, 2547 \pmod{3600}$.

Also for $k = 9, one\ have\ 25.9 - 1 = 224 = 4.56$

So, $x \equiv \pm(1350 - 3) \pmod{3600}$

$\equiv \pm 1347 \pmod{3600}$

$\equiv 1347, 2253 \pmod{3600}$.

Also for $k = 11, one\ have\ 25.11 + 1 = 276 = 4.69$

So, $x \equiv \pm(1650 + 3) \pmod{3600}$

$\equiv \pm 1653 \pmod{3600}$

$\equiv 1653, 1947 \pmod{3600}$.

Thus, the other twelve solutions are

$x \equiv 147, 3453;\ 453, 3147;\ 747, 2853;\ 1053, 2547;$

$1347, 2253; 1653, 1947 \pmod{3600}$.

Therefore, these are the twenty four solutions of the congruence.

***Example − II*:**

Consider the congruence: $x^2 \equiv 25 \pmod{3600}$.

It can be written as $x^2 \equiv 5^2 \pmod{16.9.25} i.e. x^2 \equiv 5^2 \pmod{2^4.3^2.5^2}$

It is of the type $x^2 \equiv p^2 \pmod{2^r p^m q^n} with\ p = 3, q = 5\ \&\ a = 5$.

It has exactly $8p = 8.5 = 40$ **solutions. Its twenty solutions are given by:**

$x \equiv 2^{r-1} p^m q^{n-1} \mathrm{k} \pm q \pmod{2^r p^m q^n}; k = 0, 1, 2, \ldots\ldots\ldots, 2q - 1.$

$\equiv 2^{4-1} 3^2 5^1 k \pm 5 \pmod{2^4.3^2.5^2}; k = 0, 1, 2, 3, \ldots\ldots\ldots, 8, 9.$

$\equiv 2^3.3^2.5^1 k \pm 5 \pmod{16.9.25}$

$\equiv 360k \pm 5 \pmod{3600}$

$\equiv 0 \pm 5; 360 \pm 5; 720 \pm 5; 1080 \pm 5; 1440 \pm 5; 1800 \pm 5;$

$2160 \pm 5; 2520 \pm 5; 2880 \pm 5; 3240 \pm 5 \ (mod\ 3600)$.

$\equiv 5, 3595; 355, 365;\ 715, 725;\ 1075, 1085; 1435, 1445; 1795, 1805;$

$2155, 2165; 2515, 2525; 2875, 2885; 3235, 3245 (mod\ 3600)$

The other twenty solutions are given by

$x \equiv \pm(2p^m q^{n-1} k \pm q)\ (mod\ 2^r p^m q^n); if\ k(p^m q^{n-2} k \pm 1) = 2^{r-2} t.$

$\equiv \pm(2.9.5k \pm 5)\ (mod\ 2^4 . p^2 q^2)$

$\equiv \pm(90k \pm 5)\ (mod\ 3600); if\ 9k \pm 1 = 4t.$

For $k = 1, one\ have\ 9 - 1 = 8 = 4.2$

So, $x \equiv \pm(90 - 5)\ (mod\ 2^r p^m q^n)$

$\equiv \pm 85$ **(mod 3600)**

$\equiv 85, 3515\ (mod\ 3600)$.

Also for $k = 3, one\ have\ 9.3 + 1 = 28 = 4.7$

So, $x \equiv \pm(270 + 5)\ (mod\ 3600)$

$\equiv \pm 275\ (mod\ 3600)$

$\equiv 275, 3325\ (mod\ 3600)$.

Also for $k = 5, one\ have\ 9.5 - 1 = 44 = 4.11$

So, $x \equiv \pm(450 - 5)\ (mod\ 3600)$

$\equiv \pm 445\ (mod\ 3600)$

$\equiv 445, 3155\ (mod\ 3600)$.

Also for $k = 7,\ 9.7 + 1 = 64 = 4.16$

So, $x \equiv \pm(630 + 5)(mod\ 3600)$

$\equiv \pm 635\ (mod\ 3600)$

$\equiv 635, 2965\ (mod\ 3600)$

Also, for $k = 9, one\ have\ 81 - 1 = 80 = 4.20$

So, $x \equiv \pm(810 - 5)(mod\ 3600)$

$\equiv \pm 805$

$\equiv 805, 2795\ (mod\ 3600)$

Also for $k = 11,\ 9.11 + 1 = 100 = 4.25$

So, $x \equiv \pm(990 + 5)(mod\ 3600)$

$\equiv \pm 995\ (mod\ 3600)$

$\equiv \pm 995, 2605\ (mod\ 3600)$

Also, for $k = 13,\ 9.13 - 1 = 116 = 4.29$

So, $x \equiv \pm(1170 - 5)\ (mod\ 3600)$

$\equiv \pm 1165\ (mod\ 3600)$

$\equiv 1165, 2435\ (mod\ 3600)$

Also, for $k = 15,\ 9.15 + 1 = 136 = 4.34$

So, $x \equiv \pm(1350 + 5)\ (mod\ 3600)$

$\equiv \pm 1355\ (mod\ 3600)$

$\equiv 1355, 2245\ (\mathbf{mod}\ 3600)$

Also, for k $= 17,\quad 9.17 - 1 = 152 = 4.38$

So, $x \equiv \pm(1520 - 5)\ (\mathbf{mod}\ 3600)$

$\equiv \pm 1515\ (\mathbf{mod}\ 3600)$

$\equiv 1515, 2085\ (\mathbf{mod}\ 3600)$

Also, for k $= 19,\quad 9.19 + 1 = 172 = 4.43$

So, $x \equiv \pm(1720 + 5)\ (\mathbf{mod}\ 3600)$

$\equiv \pm 1725\ (\mathbf{mod}\ 3600)$

$\equiv 1725, 1875\ (\mathbf{mod}\ 3600)$

Thus, the other twenty solutions are

$x \equiv 85, 3515; 275, 3325; 445, 3155; 635, 2965; 805, 2795$

995, 2605; 1165, 2435; $1355, 2245; 1515, 2085; 1725, 1875\ (\mathbf{mod}\ 3600)$

Therefore, these are the forty solutions of the congruence.

CONCLUSION

In this paper, finding solutions of a class of standard quadratic congruence of even composite modulus- a product of two powered odd prime in two special cases is formulated and compared with the existed method using CRT. Formulation gives solutions in less time.

REFERENCES

[1] Zuckerman at el, An Introduction to The Theory of Numbers, fifth edition, Wiley student edition, INDIA, 2008.

[2] Koshy Thomas, Elementary Number Theory with Applications, second edition, Indian Print, 2009.

[3] Roy B M, Formulation of a special type of standard quadratic congruence of composite modulus- a product of two powered odd primes, International Journal of Trend in Scientific Research and Development (IJTSRD), ISSN: 2456-6470, Vol-04, Issue-04, May-Jun-20.

[4] Roy B M, Formulation of solutions of a class of standard quadratic congruence modulo a multiple of power of an odd prime, International Journal of Engineering Technology Research & Management (IJETRM), ISSN: 2456-9348, Vol-04, Issue-05, May-20.

[5] 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 prime, International Journal of Scientific Research and Engineering Development (IJSRED), ISSN: 2581-7175, Vol-03, Issue-03, May-20.

[6] Roy B M, Formulation of solutions of standard quadratic congruence of even composite modulus-a product of twice an odd prime and power of another odd prime, International Journal for Research Trends and Innovations (IJRTI), ISSN: 2456-3315, Vol-05, Issue-05, May-20.

[7] Roy B M, Formulation of standard quadratic congruence of even composite modulus- a prime multiple of a powered odd prime, International Journal of Science & Engineering Development Research (IJSDR), ISSN: 2455-2631, Vol-05, Issue-05, May-20.

[8] Roy B M, Formulation of solutions of a standard quadratic congruence of even composite modulus –a product of powered odd prime with eighth multiple of another odd prime, International Journal of Scientific Research and Engineering Development (IJSRED), ISSN: 2581-7175, Vol-03, Issue-03, June-20.