RP-141: Another formulation of standard quadratic congruence of composite modulus Modulo a Prime-multiple of a prime- power Integer

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)

***Abstract*: In this paper, the author considered a standard quadratic congruence of composite modulus modulo a prime multiple of a prime-power integer for formulation of its solutions. Previously it was formulated by the author but in a different way. After a rigorous study, the author succeed to find another formulation of the congruence for its solutions. Such a congruence always has exactly four solutions. The formulation is tested and verified by solving different numerical examples. The solutions can now be obtained in a short time. No need to use CRT. This is the merit of the paper.**

***Keywords*: Composite Modulus, Formulation, Standard Quadratic Congruence.**

INTRODUCTION

The author already has formulated the standard quadratic congruence of composite modulus- a product of two different odd primes in different cases [1] & [2]. Here in this paper, the author considers a generalisation of these papers and wishes to formulate the said congruence: $x^2 \equiv a \ mod \ p^n q); p, q \ being \ different \ odd \ primes$.

PROBLEM-STATEMENT: Here the problem is

"The formulation of the standard quadratic congruence of composite modulus of the type:

$$x^2 \equiv a \ mod \ p^n q); p, q \ being \ different \ odd \ primes."$$

LITERATURE-REVIEW

The congruence under consideration was not formulated by earlier mathematicians. The readers used to apply CRT to get the solutions [3], [4], [5]. It is a long procedure. It is much complicated and time-consuming. The readers also faced difficulty to solve the individual congruence.

Previously it was formulated by the author in two special cases as $when \ a = p^2$ & $a = q^2$.

The congruence $x^2 \equiv p^2 \ mod \ p^n q)$ has exactly $2p -$ incongruent solutions, given by

$x \equiv p^{n-1}qk \pm p \ (mod \ p^n q); k = 0, 1, 2, \dots \dots \dots (p-1)$.

Also, the congruence $x^2 \equiv q^2 \ mod \ p^n q)$ has exactly $2 -$ incongruent solutions, given by $x \equiv p^n qk \pm p \ (mod \ p^n q); k = 0$.

ANALYSIS & RESULT

Consider the congruence $x^2 \equiv a \ mod \ p^n q)$.

Case-I:

If $a = b^2$, then the congruence reduces to: $x^2 \equiv b^2 \ mod \ p^n q)$.

Its two obvious solutions are given by $x \equiv \pm b \ (mod \ p^n q)$.

For the remaining two solutions, consider $x \equiv \pm(p^n k \pm b) \ mod \ p^n q)$.

Then $x^2 \equiv (p^n k \pm b)^2 \ (mod \ p^n q)$

$$\equiv (p^n k)^2 \pm 2.p^n k.b + b^2 \ (mod \ p^n q)$$

$$\equiv p^n k(p^n k \pm 2b) + b^2 \ (mod \ p^n q), if \ k(p^n k \pm 2b) = qt.$$

$$\equiv p^n.qt + b^2 \ (mod \ p^n q)$$

$$\equiv b^2 \ (mod \ p^n q).$$

Therefore, $x \equiv \pm(p^n k \pm b)\ mod\ p^n q),\ if\ k(p^n k \pm 2b) = qt$, satisfies the congruence and hence gives two required solutions of the congruence for a value of k.

If $a \neq b^2, then\ it\ can\ be\ expressed\ so\ as: a + l.p^n q = b^2\ (mod\ p^n q)$.

Case-II: Let $b = p$.

Then the congruence reduces to the form $x^2 \equiv p^2\ (mod\ p^n q)$

For the solutions, consider $x \equiv p^{n-1}qk \pm p\ (mod\ p^n q)$

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

$\equiv (p^{n-1}qk)^2 \pm 2.p^{n-1}qk.p + p^2\ (mod\ p^n q)$

$\equiv p^n qk(p^{n-2}qk \pm 2) + p^2\ (mod\ p^n q)$

$\equiv p^2 (mod\ p^n q)$

Therefore, $x \equiv p^{n-1}qk \pm p\ (mod\ p^n q)$ gives the solutions of the congruence.

But for $k = p$, the solutions becomes $x \equiv p^{n-1}q.p \pm p\ (mod\ p^n q)$

$\equiv p^n q \pm p\ (mod\ p^n q)$

$\equiv 0 \pm p\ (mod\ p^n q)$

This is the same solutions as for $k = 0$.

Similarly, $for\ k = 8, 9 \dots \dots$, the solutions repeats as for $k = 1, 2, \dots \dots$

Therefore, all the solutions are given by

$x \equiv p^{n-1}q.k \pm p\ (mod\ p^n q); k = 0, 1, 2, \dots \dots, (p-1)$.

These are the $2p$ incongruent solutions of the said congruence.

Case-III: $Let\ b = q$.

Then the congruence reduces to the form $x^2 \equiv q^2\ (mod\ p^n q)$

For the solutions, consider $x \equiv p^n qk \pm q\ (mod\ p^n q)$

Then, $x^2 \equiv (p^n qk \pm q)^2\ (mod\ p^n q)$

$\equiv (p^n qk)^2 \pm 2.p^n qk.q + q^2\ (mod\ p^n q)$

$\equiv p^n qk(p^n qk \pm 2q) + q^2\ (mod\ p^n q)$

$\equiv q^2 (mod\ p^n q)$

But for $k = 1$, the solutions becomes $x \equiv p^n q \pm p\ (mod\ p^n q)$

$\equiv 0 \pm p\ (mod\ p^n q)$

This is the same solutions as for $k = 0$.

Similarly, $for\ k = 2, 3 \dots \dots$, the solutions repeats as for $k = 1, 2, \dots \dots$

Therefore, all the solutions are given by

$x \equiv p^n q.k \pm p\ (mod\ p^n q); k = 0$.

These are the two − incongruent solutions of the said congruence.

ILLUSTRATIONS

Example-1: Consider the example $x^2 \equiv 4\ (mod\ 175)$.

It can be written as $x^2 \equiv 4 \equiv 2^2\ (mod\ 5^2.7)$.

It is of the type: $x^2 \equiv b^2\ mod\ p^n q)\ with\ b = 2, p = 5, q = 7$.

It has exactly four solutions; the two obvious solutions are given by

$x \equiv \pm b \ (mod\ p^n q)$.

$\equiv \pm 2 \ (mod\ 5^2.7)$

$\equiv 2, 173 \ (mod\ 175)$.

The remaining two solutions are given by

$x \equiv \pm(p^n k \pm a)\ mod\ p^n q),\ if\ k(p^n k \pm 2a) = qt.$

$\equiv \pm(5^2 k \pm 2)\ (mod\ 5^2.7),\ if\ k(25k \pm 2.2) = 7t.$

$\equiv \pm 25k \pm 2)\ (mod\ 175)$, if $k(25k \pm 4) = 7t$.

$\equiv \pm(25.1 - 2)\ (mod\ 5^2.7)\ as\ for\ k = 1, 1(25.1 - 4) = 7t$

$\equiv \pm 23\ (mod\ 175)$

$\equiv 23, 175 - 23\ (mod\ 175)$

$\equiv 23, 152\ (mod\ 175)$.

Therefore all the four solutions are given by

$x \equiv 2, 173; 23, 152\ (mod\ 175)$.

Example-2: Consider the example $x^2 \equiv 25\ (mod\ 539)$.

It can be written as $x^2 \equiv 25 \equiv 5^2\ (mod\ 7^2.11)\ with\ b = 5, p = 7, q = 11.$

It is of the type: $x^2 \equiv b^2\ mod\ p^n q)$.

It has exactly four solutions; the two obvious solutions are given by

$x \equiv \pm b\ (mod\ p^n q)$.

$\equiv \pm 5\ (mod\ 7^2.11)$

$\equiv 5, 534\ (mod\ 539)$.

The remaining two solutions are given by

$x \equiv \pm(p^n k \pm a)\ mod\ p^n q),\ if\ k(p^n k \pm 2a) = qt.$

$\equiv \pm(7^2 k \pm 5)\ (mod\ 7^2.11),\ if\ k(49k \pm 2.5) = 11t.$

$\equiv \pm(49k \pm 5)\ (mod\ 539)$, if $k(49k \pm 10) = 11t$.

$\equiv \pm(49.2 - 5)\ (mod\ 7^2.11)\ as\ for\ k = 2, 2(49.2 - 10) = 11t$

$\equiv \pm 93(mod\ 539)$

$\equiv 93, 539 - 93\ (mod\ 175)$

$\equiv 93,\ 446\ (mod\ 539)$.

Therefore all the four solutions are given by

$x \equiv 5, 534; 93, 446\ (mod\ 539)$.

Example-3: Consider the example $x^2 \equiv 49\ (mod\ 539)$.

It can be written as $x^2 \equiv 49 \equiv 7^2\ (mod\ 7^2.11)\ with\ b = 7, p = 7, q = 11.$

It is of the type: $x^2 \equiv p^2\ mod\ p^n q)$ and has exactly $2p = 2.7 = 14$ solutions,

given by: $x \equiv p^{n-1} qk \pm p\ (mod\ p^n q); k = 0, 1, 2, \dots \dots,\ (p-1).$

$\equiv 7^{2-1}.11k \pm 7\ \ (mod\ 7^2.11); k = 0, 1, 2, 3, 4, 5, 6.$

$\equiv 77k \pm 7\ (mod\ 539)$

$\equiv 0 \pm 7; 77 \pm 7; 154 \pm 7; 231 \pm 7; 308 \pm 7; 385 \pm 7; 462 \pm 7\ (mod\ 539)$

$\equiv 7, 532; 70, 84; 147, 161; 224, 238; 301, 315; 378, 392; 455, 469 \ (mod\ 539).$

These are the fourteen incongruent solutions of the said congruence.

Example-4: Consider the example $x^2 \equiv 121(mod\ 3773)$.

It can be written as $x^2 \equiv 121 \equiv 11^2\ (mod\ 7^3.11)\ with\ b = 11, p = 7, q = 11.$

It is of the type: $x^2 \equiv q^2\ mod\ p^n q)$ and has exactly two solutions, given by

$x \equiv p^n qk \pm q\ (mod\ p^n q)$

$\equiv o \pm q\ (mod\ p^n q)$

$\equiv \pm q\ (mod\ p^n q)$

$\equiv \pm 11\ (mod\ 3773)$

$\equiv 11, 3762\ (mod\ 3773).$

CONCLUSION

Therefore, it is concluded that the congruence $x^2 \equiv b^2\ mod\ p^n q)$ has exactly four incongruent solutions; two of them are given by $x \equiv \pm b\ (mod\ p^n q)$; the other two solutions are given by $x \equiv \pm(p^n k \pm a)\ mod\ p^n q),\ if\ k(p^n k \pm 2a) = qt.$

REFERENCES

[1] Roy B M, *Formulation of solutions of a standard quadratic congruence of composite modulus- an odd prime multiple of power of an odd prime*, International Journal of Scientific research and Engineering development (IJSRED), ISSN: 2581-7175, Vol-03, Issue-02, March-2020.

[2] 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 and Engineering development (IJSRED), ISSN: 2581-7175, Vol-03, Issue-04, Jul-Aug-20.

[3]Roy B M, (2016) *Discrete Mathematics & Number Theory*, Das Ganu prakashan, Nagour (India), 1/e, ISBN:

[4]Thomas Koshy, *(2009) Elementary Number Theory with Applications*, Academic Press (An Imprint of Elsevier), ISBN: 978-81-312-1859-4.

[5] Zuckerman H. S., Niven I., Montgomery H. L., (2008) "*An Introduction to The Theory of Numbers*", 5/e, Wiley India (Pvt) Ltd, ISBN: 978-81-265-1811-1.