Journal of Analysis & Number Theory
An International Journal

Quadratic and Cubic Equations in the Form of Fermat's Last Theorem

Meena Joshi and A. S. Uniyal

Kumoan University, Nainital, India

Email: lohumim@gmail.com, asuniyal0111@gmail.com

Received*: 8 Feb. 2012; Revised 15 May. 2012; Accepted 23 Jul. 2012*

Abstract: In this paper we have converted the various quadratic and cubic forms of equations in the form of Fermat's Last Theorem under different restrictions so that the fascinating results can be obtained by the use of the said method of infinite descent. As the general quadratic and cubic equations of different forms can be converted into the form of Fermat's last theorem under different conditions and restrictions so that the results of Fermat last theorem can be applied on the same. The general equations with multiple variables can be modified under different modulo system and by using respective restrictions the equations can be converted to the form of Fermat's last theorem. For example the equation of the form $x^4 + y^4 = z^2 \pmod m$ can be expressed in the form of Fermat's last theorem under modulo m by applying the restrictions $x^2 = A \pmod m$ and $y^2 = B \pmod m$ and hence the equation in the form of Fermat's last theorem for n = 2 can be obtained.

Introduction

Fermat's Last Theorem states that no three positive integers *a*, *b*, and *c* can satisfy the equation $a^n+b^n = c^n$ for any integer value of *n* greater than two.

The general quadratic and cubic equations of different forms can be converted into the form of Fermat's last theorem under different conditions and restrictions so that the results of Fermat last theorem can be applied on the same. The general equations with multiple variables can be modified under different modulo system and by using respective restrictions the equations can be converted to the form of Fermat's last theorem.

We have converted the various quadratic and cubic forms of equations in the form of Fermat's Last Theorem under different restrictions so that the fascinating results can be obtained by the use of the said method of infinite descent In this paper different equations for example quadratic, cubic, etc are expressed to the form of Fermat last theorem under modulo system under different restrictions.

THEOREM (2.1) The equation of the form $x^4 + y^4 = z^2 \pmod m$ can be expressed in the form of Fermat's last theorem.

PROOF: Consider the equation

$$x^4 + y^4 = z^2 \pmod m$$

Let $x^2 = A \pmod m$ and $y^2 = B \pmod m$. Then the above equation transforms to the form

$$A^2 + B^2 = z^2 \pmod m$$

where $x^2 = A \pmod m$ and $y^2 = B \pmod m$. The equation $x^4 + y^4 = z^2 \pmod m$ has solution if (A/m) = 1 and (B/m) = 1

THEOREM (2.2) The equation of the form $x^4 - 8y^4 = z^2 \pmod m$ can be expressed in the form of Fermat's last theorem.

PROOF: Consider the equation

$$x^4 - 8y^4 = z^2 \pmod m$$

i.e. $x^4 - 9y^4 + y^4 = z^2 \pmod m$

$$A^2 + B^2 = z^2 \pmod m$$

where $x^4 - 9y^4 = A^2 \pmod m$

$$3y^2 = C^2 \pmod m$$

$$x^4 = A^2 + C^2 \pmod m$$

$$y^2 = B \pmod m$$

THEOREM (2.3) The equation of the form $x^4 - 2y^4 = z^2 \pmod m$ can be expressed in the form of Fermat's last theorem under the restrictions

$$A^2 - B^2 = z^2 \pmod m$$

$$x^4 - y^4 = A^2 \pmod m$$

$$\& \; y^2 = B \pmod m$$

THEOREM (2.4) The equation of the form $ax^2 + by^2 = cz^2 \pmod m$ can be expressed in the form of Fermat's last theorem as $A^2 + B^2 = C^2 \pmod m$

PROOF: Consider the equation

$$ax^2 + by^2 = cz^2 \pmod m$$

$$\text{If } \lambda^2 = a \pmod m$$

$$\mu^2 = b \pmod m$$

$$\nu^2 = c \pmod m$$

Then it would transforms to the form

$$A^2 + B^2 = C^2 \pmod m$$

$$\text{where } \lambda x = A \pmod m$$

$$\mu y = B \pmod m$$

$$\& \; \nu z = C \pmod m$$

THEOREM (2.5) The equation of the form $ax^n + by^n = cz^n \pmod m$ can be expressed in the form of Fermat's last theorem as $A^n + B^n = C^n \pmod m$ provided

$$\lambda x = A \pmod m$$

$$\mu y = B \pmod m$$

$$\& \; \nu z = C \pmod m$$

THEOREM (2.6) The cubic equation of the form $x^3 + 3Hx^2 + G = 0 \pmod m$ and $x^3 + 3Hx + G = 0 \pmod m$ can be expressed in the form of Fermat's last theorem.

PROOF: Consider the cubic equation

$$x^3 + 3Hx^2 + G = 0 \pmod m$$

Taking under modulo H, it transforms to the form

$$x^3 + G \equiv 0 \pmod{H}$$

which implies

$$x^3 \equiv -G \pmod{H}$$

$$\text{Let } -G = \pm \lambda^3 \pmod{H}$$

$$x^3 \equiv \pm \lambda^3 \pmod{H}$$

$$x \equiv \pm \lambda \pmod{H}$$

where H can be written as $H = p_1.p_2.p_3.\ldots\ldots\ldots\ldots\ldots p_\alpha$. Hence $x^3 + G \equiv 0 \pmod{H}$ can be written as

$$x^3 + G \equiv 0 \pmod{p_1}$$

$$x^3 + G \equiv 0 \pmod{p_2}$$

$$x^3 + G \equiv 0 \pmod{p_\alpha}$$

Using the above results, we have the equations in the form of Fermat's last Theorem as

$$x^3 + \lambda^3 \equiv p_1^3 \pmod{p_1}$$

$$x^3 + \lambda^3 \equiv p_2^3 \pmod{p_2}$$

$$x^3 + \lambda^3 \equiv p_\alpha^3 \pmod{p_\alpha}$$

Taking under modulo G, we have

$$x^3 + 3Hx^2 \equiv 0 \pmod{G}$$

$$x^2 (x + 3H) \equiv 0 \pmod{G}$$

$$x^2 \equiv 0 \pmod{G} \text{ or } x \equiv -3H \pmod{G}$$

Let $3H \equiv \lambda^2 \pmod{G}$

Therefore we have

$$x^3 + \lambda^2 x^2 \equiv 0 \pmod{G}$$

$$x^3 + y^2 \equiv 0 \pmod{G}$$

$$\text{where } y = \lambda x$$

Taking suitable transformations

$$y^2 = \mu^3 \pmod{G}$$

It gives

$$x^3 + \mu^3 \equiv 0 \pmod{G}$$

which can be written in the form of Fermat's last theorem as

$$x^3 + \mu^3 \equiv G^3 \pmod{G}$$

Taking $G = q_1.q_2.q_3.\ldots\ldots\ldots\ldots q_r$; the equation can be written in the form of Fermat's last theorem as

$$x^3 + \mu^3 \equiv q_1^3 \pmod{q_1}$$

$$x^3 + \mu^3 \equiv q_2^3 \pmod{q_2}$$

$$x^3 + \mu^3 \equiv q_\alpha^3 \pmod{q_\alpha}$$

Similarly, the cubic equation of the form $x^3 + 3Hx + G = 0 \pmod m$ can be expressed in the form of Fermat's last theorem.

COROLLARY

The general cubic equation $ax^3+bx^3 + cx + d = 0$, $a \neq 0$ can be expressed in the form of Fermat's last theorem by taking it under different modulo systems i.e. b, c & d.

PROOF: The above cubic equation will transforms to the equations mentioned in Theorem 2.6 when taken under modulo c and b respectively.

When taken under modulo $d = p_1.p_2.p_3\ldots\ldots\ldots\ldots\ldots\ldots p_r$; it transforms to

$$ax^3 + bx^2 + cx \equiv 0 \pmod{p_i}$$

$$x(ax^2 + bx + c) \equiv 0 \pmod{p_i}$$

$$x \equiv 0 \pmod{p_i}$$

Or $(ax^2 + bx + c) \equiv 0 \pmod{p_i}$, which can be written as

$$(x + \alpha)^2 + \nu \equiv 0 \pmod{p_i}$$

and further can be written in the form of Fermat's last theorem as

$$(x + \alpha)^2 + \mu^2 \equiv p_i \pmod{p_i}$$

where $\nu = \mu^2 \pmod{p_i}$

CONCLUSION

Much work has been done on the conversion of different form of equations in the form of Fermat's last theorem. In this paper, we have described some results of specific type of quadratic and cubic equations.

References

[1] Edward, H.M.; Fermat's last theorem, a genetic introduction to algebraic number theory, Springer

[2] Manin, YU.I.; Cubic forms, Algebra, Geometry, arithmetic, North Holland

[3] Baily, A. M.; On the density of discriminants of quartic fields. *J. Reine Angew. Math*. 315 (1980).

[4] Cohen, H.; A course in computational algebraic number theory, *Springer, Berlin*, (1993).

[5] Kaplansky, I.; Composition of binary quadratic forms, Studia Math. 31 (1968).

[6] Kneser, M.; Composition of binary quadratic forms, *J. Number Theory* 15 (1982).