ROYAL HOLLOWAY COLLEGE

(UNIVERSITY OF LONDON)

SOME DIOPHANTINE EQUATIONS

T
AOE
Vel
137,158
June 77

A THESIS SUBMITTED

BY

MANORANJITHAM VELUPPILLAI

IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

Department of Mathematics

Royal Holloway College

Egham, Surrey, England

March 1977

ProQuest Number: 10097852

All rights reserved

INFORMATION TO ALL USERS
The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript
and there are missing pages, these will be noted. Also, if material had to be removed,
a note will indicate the deletion.

ProQuest 10097852

Published by ProQuest LLC(2016). Copyright of the Dissertation is held by the Author.

All rights reserved.
This work is protected against unauthorized copying under Title 17, United States Code.
Microform Edition © ProQuest LLC.

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

CONTENTS

R.H.C.

ABSTRACT

For positive integers x, y, the equation $x^4 + (n^2 - 2)x^2y^2 + y^4 = z^2$ always has the trivial solution $x = y$. In Chapter 1, we discuss the conditions under which the above equation cannot have any non-trivial solutions in positive integers. We also prove that if the above equation has no non-trivial solutions, then the 1^{st}, 3^{rd}, $(n + 1)^{th}$, $(n + 3)^{th}$ terms of an arithmetical progression cannot each be square.

In Chapter 2, we prove that any set of positive integers, with the property that the product of any two integers increased by 2 is a perfect square, can have at most three elements. We also prove that there exist infinitely many sets of four positive integers with the property that the product of any two increased by 1 is a perfect square. Although in general we could not prove that a fifth integer cannot be added to these sets without altering the property, we prove it for a particular set $\{2, 4, 12, 420\}$. We also give an algebraic formula to find the fourth member of the set, if any three members are given.

In Chapter 3, we prove that the only positive integer solutions of the equation $(x(x - 1))^2 = 3y(y - 1)$ are $(x, y) = (1, 1)$ & $(3, 4)$.

In Chapter 4, we prove that the only positive integer solution of the equation $3y(y + 1) = x(x + 1)(x + 2)(x + 3)$ is $(x, y) = (12, 104)$.

The results of this thesis are, to the best of my knowledge original and my own, except for Theorem 1.1 (Chapter 1) & Theorem

2.4 (Chapter 2), which have been proved by my Supervisor.

Chapter 3 has been published in the Glasgow Mathematical Journal, Volume 17, Part 2, July 1976.

ACKNOWLEDGEMENTS

I wish to thank Dr J.H.E. Cohn, Reader in Mathematics, Royal Holloway College, for his supervision during this research, and for providing the initial opportunity to do it.

While preparing this thesis I was financed by a Tutorial Research Studentship provided by Royal Holloway College. I would like to thank Professor H.G. Eggleston, Head of the Mathematics Department, Royal Holloway College, whose support, together with that of my supervisor, helped me to obtain this Studentship.

I am grateful to all the members of the Mathematics Department, Royal Holloway College, who have made my stay in this country such a happy one.

Finally, I would like to thank the Vice-Chancellor, University of Ceylon, who granted me three years leave to complete this work.

NOTATIONS, DEFINITIONS, AND PREREQUISITES

An integer a is said to be divisible by an integer $b \neq 0$, if there exists an integer c, such that $a = bc$. We indicate this by writing $b \mid a$. We write $b \nmid a$ to indicate that b does not divide a. The greatest common divisor of a & b, denoted by (a, b), is defined to be the largest positive integer which divides both a & b.

We say that a is congruent to b modulo m, if $m \mid (a - b)$. We express this in symbols as $a \equiv b \pmod{m}$. We say that a is a quadratic residue of m if the congruence $x^2 \equiv a \pmod{m}$ is solvable. If this congruence has no solutions, then a is said to be a quadratic non-residue of m.

For an odd prime p, we define the Legendre symbol as follows:

$(a/p) = +1$, when a is a quadratic residue of p,

$(a/p) = -1$, when a is a quadratic non-residue of p.

The following relations are valid for this symbol:

$(a/p) = (a'/p)$, when $a \equiv a' \pmod{p}$,

$(aa'/p) = (a/p)(a'/p)$,

$(2/p) = (-1)^h$, where $h = \frac{1}{2}(p - 1).\frac{1}{2}(p + 1)$,

$(p/q)(q/p) = (-1)^h$, where p, q are odd primes and $h = \frac{1}{2}(p - 1).\frac{1}{2}(p + 1)$.

When $P = p_1 p_2 ---- p_m$, where p_1, p_2, ---- p_m are primes, distinct or not, and D is an integer prime to P, we define the Jacobi symbol (D/P) as

$$(D/P) = (D/p_1)(D/p_2)----(D/p_m).$$

We also assume the following results:

(i) If $ab = x^2$, with $(a, b) = 1$, then $a = x_1^2$, $b = x_2^2$, $x = x_1 x_2$,

(ii) If $d = x^2 + y^2$, with $(x, y) = 1$, then d cannot have a prime factor $\equiv 3 \pmod 4$.

Chapter 1

Introduction:

Equations of the form $ax^4 + bx^2y^2 + cy^4 = dz^2$ have a long history going back to Fermat and Euler [4]. One of Euler's results is that the equation $x^4 + 14x^2y^2 + y^4$ is not a square if x and y are relatively prime and x is even and y odd (excluding $x = 0$, $y = 1$) or if x and y are both odd (excluding $x = 1$, $y = 1$). An interesting corollary by Fermat is that there cannot be four squares in arithmetical progression. Pocklington [8] has also discussed the solutions of the equation $x^4 + nx^2y^2 + y^4 = z^2$ for certain values of n. Equations of the form,

$$x^4 + (n^2 - 2)x^2y^2 + y^4 = z^2 \tag{1}$$

always have the solution $x = y$.

In this chapter we shall prove some results concerning the integer solutions of (1).

Definition:

(1) is said to have a non-trivial solution if it has a solution (x, y, z) with $xy(x^2 - y^2) \neq 0$.

Theorem 1.1:

A necessary condition for (1) to have a non-trivial solution when $n = p$, a prime, is that there exist a factorisation of $p^2 - 4$ in the form rs with (r,s) not divisible by any prime $\equiv 3 \pmod 4$ satisfying,

either (i) $r \equiv 1 \pmod 8$, $r \neq \square$, r has no prime factor $\equiv 3 \pmod 4$

<u>or</u> (ii) $r \equiv 3 \pmod 8$, r has no prime factor $\equiv 5$ or $7 \pmod 8$ and s has no prime factor $\equiv 3$ or $5 \pmod 8$.

<u>Lemma 1.1</u>

The equation $x^2 + y^2 = z^2$, with $(x, y) = 1$, $z > 0$ has the solution $x = X^2 - Y^2$, $y = 2XY$, $z = X^2 + Y^2$, when y is even.

<u>Proof of Theorem 1.1</u>:

When $n = p$, (1) becomes,

$$x^4 + (p^2 - 2)x^2y^2 + y^4 = z^2 . \tag{2}$$

Suppose (x, y, z) is a non-trivial solution of (2), with $z > 0$ and minimal. Then $(x, y) = 1$ and in particular at least one of x and y must be odd. Without loss of generality, we can assume that y is odd. Then also z is odd.

<u>Case I</u>

Suppose $x^2 \equiv y^2 \pmod p$ and $x \equiv 1 \pmod 2$.

Then $p|z$ and we can write (2) as

$$\left(\frac{x^2 - y^2}{p}\right)^2 + (xy)^2 = \left(\frac{z}{p}\right)^2 \tag{3}$$

Since $(x, y) = 1$, we have, $(\frac{x^2 - y^2}{p}, xy) = 1$. Hence by lemma 1.1.1, we must have for integers X, Y

$$xy = X^2 - Y^2$$

$$x^2 - y^2 = 2pXY .$$

Then, $\left(\frac{x^2 + y^2}{2}\right)^2 = p^2X^2Y^2 + (X^2 - Y^2)^2 = X^4 + (p^2 - 2)X^2Y^2 + Y^4$.

Since $\frac{x^2 + y^2}{2} < z$ and $XY(X^2 - Y^2) \neq 0$, descent applies.

Hence this case is impossible.

Case II

Suppose $x^2 \equiv y^2 \pmod p$ and $x \equiv 0 \pmod 2$.

Then again we have (3) and now,

$$xy = 2XY,$$

$$x^2 - y^2 = p(X^2 - Y^2).$$

Now, $(x^2 + y^2)^2 = p^2(X^2 - Y^2)^2 + 16X^2Y^2$.

$$= l^4 + (p^2 - 2)l^2m^2 + m^4 \text{ , where } l = X + Y, \ m = |X - Y|.$$

Since $x^2 + y^2 < z$ and $lm(l^2 - m^2) = 4XY|X^2 - Y^2| \neq 0$, descent applies.

Hence this case is impossible.

Case III

Suppose $x^2 \not\equiv y^2 \pmod p$.

We can write (2) as,

$$(2x^2 + (p^2 - 2)y^2)^2 - y^4p^2(p^2 - 4) = 4z^2.$$

Hence, $p^2(p^2 - 4)y^4 = (2x^2 + (p^2 - 2)y^2 + 2z)(2x^2 + (p^2 - 2)y^2 - 2z)$,

$$= A.B, \text{ say.}$$

Now, let q be a prime dividing (A, B).

Then, $q|AB$ and $q|A + B$.

i.e $q|p^2(p^2 - 4)y^4$ and $q|2x^2 + (p^2 - 2)y^2$.

Now, $q \nmid y$, since $q|y \rightarrow q|x$, which is impossible as $(x, y) = 1$.

Also $q \neq p$, since $q = p$ would imply that $p|(x^2 - y^2)$.

Hence $(A, B)^2 \mid (p^2 - 4)$, and so $(A, B)^2 \mid (x^2 + y^2)$.

Since $(x, y) = 1$, A and B cannot have a prime factor $\equiv 3 \pmod 4$ in common. Thus we have,

$$2x^2 + (p^2 - 2)y^2 \pm 2z = p^2Rc^4, \qquad (4)$$

$$2x^2 + (p^2 - 2)y^2 \mp 2z = Sd^4, \qquad (5)$$

where $y = cd$, $RS = p^2 - 4$, R&S have no prime factor $\equiv 3 \pmod 4$ in common, and $(pc, d) = 1$.

$$(4) + (5) \rightarrow 4x^2 = p^2Rc^4 - 2(p^2 - 2)c^2d^2 + Sd^4,$$
$$= (Rc^2 - d^2)(p^2c^2 - Sd^2),$$
$$= C.D, \text{ say.}$$

Now, $D - SC = 4c^2$, $RD - p^2C = 4d^2$. Since $(c, d) = 1$, we have $(C, D)|4$. Hence we have to consider the following cases:

Case IIIa

Suppose $R \equiv 1 \pmod 8$.

Then $S \equiv 5 \pmod 8$, $C \equiv 0 \pmod 8$, $D \equiv 4 \pmod 8$.

Thus we must have

$$C = Rc^2 - d^2 = \pm 16x_1^2 ,$$
$$D = p^2c^2 - Sd^2 = \pm 4x_2^2,$$
$$x = 4x_1x_2.$$

Then $c^2 = \frac{1}{4}(D - SC) = \pm(x_2^2 - 4Cx_1^2)$ and so the minus sign is impossible. Thus,

$$Rc^2 = d^2 + 16x_1^2 .$$

Since $x_1 \mid x$, $d \mid y$, we must have $(d, x_1) = 1$ and hence R cannot have a prime factor $\equiv 3 \pmod 4$.

Suppose $R = \square$, say R_1^2. Then we should have

$d = X^2 - Y^2$, $2x_1 = XY$, $R_1c = X^2 + Y^2$.

But then
$$4R_1^2x_2^2 = p^2R_1^2c^2 - RSd^2,$$
$$= p^2(X^2 + Y^2)^2 - (p^2 - 4)(X^2 - Y^2)^2,$$
$$= 4X^4 + 4(p^2 - 2)X^2Y^2 + 4Y^4.$$

i.e $\quad (R_1x_2)^2 = X^4 + (p^2 - 2)X^2Y^2 + Y^4 .$

Since $(R_1x_2)^2 = Rx_2^2 < (p^2 - 4)x^2 < z^2$ and $XY(X^2 - Y^2) \neq 0$, descent applies. Thus $R \neq \square$.

Thus, taking $R = r$, $S = s$, we see that this case is impossible if condition (i) does not hold.

Case IIIb

Suppose $R \equiv 5 \pmod 8$.

Then $S \equiv 1 \pmod 8$, $C \equiv 4 \pmod 8$, $D \equiv 0 \pmod 8$.

Thus,

$$C = Rc^2 - d^2 = \pm 4x_1^2$$

$$D = p^2c^2 - Sd^2 = \pm 16x_2^2,$$

$$x = 4x_1x_2.$$

Then $c^2 = \pm(4x_2^2 - Sx_1^2)$ and hence the plus sign is impossible modulo 4. Thus $Sd^2 = p^2c^2 + 16x_2^2$. Since $(pc, x_2) = 1$, S cannot have a prime factor $\equiv 3 \pmod 4$.

Suppose $S = \square$, S_1^2, say. Then we should have

$S_1d = X^2 + Y^2$, $pc = X^2 - Y^2$, $2x_2 = XY$,

and then, $(S_1x_1)^2 = \frac{1}{4}S_1^2(d^2 - Rc^2)$,

$$= \tfrac{1}{4}(X^2 + Y^2)^2 - \tfrac{1}{4}(\frac{p^2 - 4}{p^2})(X^2 - Y^2)$$

$$= X^2Y^2 + (\frac{X^2 - Y^2}{p})^2$$

Thus, $XY = 2\lambda\mu$, $X^2 - Y^2 = (\lambda^2 - \mu^2)$, $(X^2 + Y^2)^2 = p^2(\lambda^2 - \mu^2)^2 + 16\lambda^2\mu^2$.

Putting $\lambda + \mu = l$, $\lambda - \mu = m$, we have,

$$(X^2 + Y^2) = p^2l^2m^2 + (l^2 - m^2)^2,$$

$$= l^4 + (p^2 - 2)l^2m^2 + m^4,$$

Since, $(X^2 + Y^2)^2 = Sd^2 < (p^2 - 4)y^2 < z^2$ and $lm(l^2 \quad m^2) \neq 0$, descent applies. Thus $S \neq \square$.

Hence, taking $R = s$, $S = r$, we see that this case is impossible if condition (i) does not hold.

Case IIIc

Suppose $R \equiv 3 \pmod 8$.

Then $S \equiv 7 \pmod 8$, $C \equiv 2 \pmod 8$, $D \equiv 2 \pmod 8$.

Hence we should have,

$$C = Rc^2 - d^2 = 2x_1^2 , \qquad (6)$$

$$D = p^2c^2 - Sd^2 = 2x_2^2 , \qquad (7)$$

$$x = x_1x_2 .$$

We see that (6) & (7) cannot hold simultaneously if R has a prime factor $\equiv 5$ or $7 \pmod 8$ or S has a prime factor $\equiv 3$ or $5 \pmod 8$.

Thus taking $R = r$, $S = s$ we see that this case is impossible if condition (ii) does not hold.

Case IIId

Suppose $R \equiv 7 \pmod 8$

Then $S \equiv 3 \pmod 8$, $C \equiv 6 \pmod 8$, $D \equiv 6 \pmod 8$.

Hence we should have,

$$-C = d^2 - Rc^2 = 2x_1^2 , \qquad (8)$$

$$-D = Sd^2 - p^2c^2 = 2x_2^2 , \qquad (9)$$

$$x = x_1x_2 .$$

Now, (8) & (9) cannot hold simultaneously if R has a prime factor $\equiv 3$ or $5 \pmod 8$ or S has a prime factor $\equiv 5$ or $7 \pmod 8$.

Thus taking $R = s$, $S = r$ we see that this case is impossible if condition (ii) does not hold.

Hence the theorem.

Theorem 1.2:

The equation (1) has no non-trivial solutions if $n = 2p$, where p is a prime such that $p \equiv \pm 3 \pmod 8$ and $p^2 - 1$ has no prime factor $\equiv 1 \pmod 4$.

To prove this theorem , we use principally lemma 1.1, and.

Lemma 1.2:

If $xy = uv$, then $x = \alpha\beta$, $y = \gamma\delta$, $u = \alpha\gamma$, $v = \beta\delta$.

(The proofs of both lemmas can be found in Pocklington [8]).

Proof of Theorem 1.2:

When $n = 2p$, (1) becomes,

$$x^4 + (4p^2 - 2)x^2y^2 + y^4 = z^2. \tag{10}$$

Suppose (x, y, z) is a non-trivial solution of (10) with $z > 0$ and minimal. Then $(x, y) = 1$ and without loss of generality we can assume that y is odd.

Case I

Suppose $x^2 \equiv y^2 \pmod p$ and $x \equiv 1 \pmod 2$.

Then we can write (10) as,

$$\left(\frac{z}{2p}\right) = \left(\frac{x^2 - y^2}{2p}\right)^2 + x^2y^2.$$

Since $\left(\frac{x^2 - y^2}{2p}, xy\right) = 1$, and xy is odd we should have,

$$xy = X^2 - Y^2$$
$$\frac{x^2 - y^2}{2p} = 2XY.$$

Then $\frac{1}{4}(x^2 + y^2)^2 = X^4 + (4p^2 - 2)X^2Y^2 + Y^4$.

Since $\frac{1}{2}(x^2 + y^2) < z$, and $XY(X^2 - Y^2) \neq 0$, descent applies. Hence this case is impossible.

Case II

Suppose $x^2 \equiv y^2 \pmod p$ and $x \equiv 0 \pmod 2$

Then z is odd and we can write (10) as,

$$\left(\frac{x^2 - y^2}{p}\right)^2 + 4x^2y^2 = \left(\frac{z}{p}\right)^2$$

Thus, we have,

$$\left(\frac{x^2 - y^2}{p}\right)^2 = X^2 - Y^2, \qquad (11)$$

$$xy = XY\ . \qquad (12)$$

By lemma 1.2, (12) $\rightarrow x = \alpha\beta$, $y = \gamma\delta$, $X = \alpha\gamma$, $Y = \beta\delta$, where α, β, γ, δ are integers.

Now, suppose $p \equiv 3 \pmod 8$. Then X is odd and Y is even. Hence β is even α, γ, δ are odd.

Then (11) $\rightarrow \alpha^2\beta^2 - \gamma^2\delta^2 = p(\alpha^2\gamma^2 - \beta^2\delta^2)$.

Hence, $\beta^2 - 1 \equiv 3(1 - \beta^2) \pmod 8$.

i.e $4(\beta^2 - 1) \equiv 0 \pmod 8$, which is impossible as β is even.

Next suppose that $p \equiv -3 \pmod 8$.

Then X is even, Y is odd. So, in this case α is even, β, γ, δ are odd. Thus we have, $\alpha^2 - 1 \equiv -3(\alpha^2 - 1) \pmod 8$.

i.e, $4(\alpha^2 - 1) \equiv 0 \pmod 8$, which is impossible as α is even.

Hence case II is impossible.

Case III

Suppose $x^2 \not\equiv y^2 \pmod p$ and $x \equiv 1 \pmod 2$

Now, (10) $\rightarrow (x^2 + (2p^2 - 1)y^2 + z)(x^2 + (2p^2 - 1)y^2 - z) = 4p^2(p^2 - 1)y^4$.

Let $A = x^2 + (2p^2 - 1)y^2 + z$, $B = x^2 + (2p^2 - 1)y^2 - z$.

Then $4|A$ and $4|B$. In fact $2^2||(A, B)$.

Suppose an odd prime $q \mid (A, B)$. Then $q|z$, $q|x^2 + (2p^2 - 1)y^2$ and $q^2|p^2(p^2 - 1)y^4$.

Now, $q|y \rightarrow q|x$, which is impossible since $(x, y) = 1$. So $q \nmid y$.

$q = p \rightarrow x^2 \equiv y^2 \pmod p$, which is impossible. Hence $q \neq p$.

Thus $q^2|(p^2 - 1) \rightarrow q|(x^2 + p^2y^2)$. But since $p^2 - 1$ has no prime factor $\equiv 1 \pmod 4$, this is impossible.

Thus $(A, B) = 4$.

Hence we should have,

<u>either</u>

$$x^2 + (2p^2 - 1)y^2 + z = 4p^2Rc^4,$$
$$x^2 + (2p^2 - 1)y^2 - z = Sd^4,$$

<u>or</u>

$$x^2 + (2p^2 - 1)y^2 + z = 4Rc^4,$$
$$x^2 + (2p^2 - 1)y^2 - z = p^2Sd^4,$$

where $y = cd$, $RS = p^2 - 1$, $(pRc, Sd) = 1$. Also, since $p^2 \equiv 9 \pmod{16}$ we have $RS \equiv 8 \pmod{16}$. Hence R is odd and $2^3 || S$.

So we have,

<u>either</u>

$$2x^2 = 4p^2Rc^4 - 2(2p^2 - 1)c^2d^2 + Sd^4,$$

<u>or</u>

$$2x^2 = 4Rc^4 - 2(2p^2 - 1)c^2d^2 + p^2Sd^4.$$

i.e , <u>either</u>

$$2x^2 = (2Rc^2 - d^2)(2p^2c^2 - Sd^2)$$

<u>or</u>

$$2x^2 = (2Rc^2 - p^2d^2)(2c^2 - Sd^2).$$

Hence we should have,

<u>either</u> $2Rc^2 - d^2 = \pm x_1^2$, $2p^2c^2 - Sd^2 = \pm 2x_2^2$, <u>or</u> $2Rc^2 - p^2d^2 = \pm x_1^2$, $2c^2 - Sd^2 = \pm 2x_2^2$,

where $x = x_1x_2$.

In both cases the minus sign is impossible modulo 4. Hence we have,

<u>either</u> $p^2c^2 - \frac{1}{2}Sd^2 = x_2^2$ <u>or</u> $c^2 - \frac{1}{2}Sd^2 = x_2^2$.

Since $2^3 || S$, both equations are impossible modulo 8.

Case IV

Suppose x is even and $x^2 \not\equiv y^2 \pmod{p}$.

Now, we can write (10) as,

$$(x^2 - y^2)^2 + 4p^2x^2y^2 = z^2.$$

Since $(x^2 - y^2, xy) = 1$ and pxy is even, we should have,

$$x^2 - y^2 = X^2 - Y^2, \tag{13}$$

$$pxy = XY. \tag{14}$$

Since x is even and y is odd, we have X is even and Y is odd.

(14) $\rightarrow$ either $x = \alpha\beta,\ y = \gamma\delta,\ X = p\alpha\gamma,\ Y = \beta\delta,$

or $x = \alpha\beta,\ y = \gamma\delta,\ X = \alpha\gamma,\ Y = p\beta\delta.$

Then (13) $\rightarrow$ either $\alpha^2\beta^2 - \gamma^2\delta^2 = p^2\alpha^2\gamma^2 - \beta^2\delta^2,$

or $\alpha^2\beta^2 - \gamma^2\delta^2 = \alpha^2\gamma^2 - p^2\beta^2\delta^2.$

Case IVa

Suppose $\alpha^2\beta^2 - \gamma^2\delta^2 = p^2\alpha^2\gamma^2 - \beta^2\delta^2.$

Then $\alpha^2(\beta^2 - p^2\gamma^2) = \delta^2(\gamma^2 - \beta^2).$

Now, $2^3 \| (\beta^2 - p^2\gamma^2, \gamma^2 - \beta^2)$. Hence we have $(\beta^2 - p^2\gamma^2, \gamma^2 - \beta^2) = 8R$, where R is odd and $R | (p^2 - 1)$.

Since $(\alpha, \delta) | (x, y) = 1$, we have $(\alpha, \delta) = 1$.

Thus we have,

$$\beta^2 - p^2\gamma^2 = \pm 8R\delta^2, \tag{15}$$

$$\gamma^2 - \beta^2 = \pm 8R\alpha^2, \tag{16}$$

(15) + (16) $\rightarrow \gamma^2(1 - p^2) = \pm 8R(\delta^2 + \alpha^2).$

The plus sign is impossible since $(1 - p^2) < 0$

Hence $\gamma^2(p^2 - 1) = 8R(\delta^2 + \alpha^2).$

i.e, $$\gamma^2\frac{(p^2 - 1)}{8R} = \delta^2 + \alpha^2. \tag{17}$$

If $R = 1$ and $p \neq 3$, then the above equation is impossible modulo 3. If $8R = p^2 - 1$, then

(17) $\to \gamma^2 = \delta^2 + \alpha^2$. Since $(\alpha, \delta) = 1$ and α is even, we should have,

$\delta = \xi^2 - \eta^2$, $\alpha = 2\xi\eta$, $\gamma^2 = \xi^2 + \eta^2$.

Then $\beta^2 = \gamma^2 + (p^2 - 1)\alpha^2$,

$= (\xi^2 + \eta^2)^2 + (p^2 - 1).\ 4\xi^2\eta^2$,

$= \xi^4 + (4p^2 - 2)\xi^2\eta^2 + \eta^4$.

Since $\beta < x < z$, $\xi\eta(\xi^2 - \eta^2) \neq 0$, descent applies.

Hence $8R \neq p^2 - 1$. Since $(\alpha, \delta) = 1$, and $\frac{p^2 - 1}{8R}$ has a prime factor $\equiv 3 \pmod 4$, this case is impossible.

Case IVb

Suppose $\alpha^2\beta^2 - \gamma^2\delta^2 = \alpha^2\gamma^2 - p^2\beta^2\delta^2$.
i.e, $\alpha^2(\beta^2 - \gamma^2) = \delta^2(\gamma^2 - p^2\beta^2)$.

Since, $2^3 || (\beta^2 - \gamma^2, \gamma^2 - p^2\beta^2)$, we have $(\beta^2 - \gamma^2, \gamma^2 - p^2\beta^2) = 8R$, where R is odd. Hence we should have,

$$\beta^2 - \gamma^2 = \pm 8R\delta^2, \qquad (18)$$

$$\gamma^2 - p^2\beta^2 = \pm 8R\alpha^2. \qquad (19)$$

$$(18) + (19) \to \beta^2(1 - p^2) = \pm 8R(\delta^2 + \alpha^2) \qquad (20)$$

The plus sign is impossible, since $(1 - p^2) < 0$.

Hence,

$$\beta^2(p^2 - 1) = 8R(\delta^2 + \alpha^2)$$

If $R = 1$, $p \neq 3$, then (20) is impossible modulo 3.

$R = 1$, $p = 3$ $\to$ $8R = p^2 - 1$ and hence,

$$\beta^2 = \delta^2 + \alpha^2.$$

Hence, we should have,

$$\delta = \xi^2 - \eta^2, \alpha = 2\xi\eta,\ \beta^2 = (\xi^2 + \eta^2).$$

But then, $\gamma^2 = p^2(\xi^2 - \eta^2)^2 + 4\xi^2\eta^2$.

$$4\gamma^2 = 4p^2(\xi^2 - \eta^2)^2 + 16\xi^2\eta^2.$$

So if we put $l = \xi + \eta$, $m = \xi - \eta$, then we have,

$$(2\gamma)^2 = l^4 + (4p^2 - 2)l^2m^2 + m^4.$$

Since $2\gamma < 2y < z$ and $lm(l^2 - m^2) \neq 0$, descent applies.

If $8R \neq p^2 - 1$, then again (20) is impossible as $(\alpha, \gamma) = 1$ and $\frac{p^2 - 1}{8}$ has a prime factor $\equiv 3 \pmod 4$.

Hence the theorem .

Theorem 1.3:

A necessary condition for the equation (1) to have a non-trivial solution when $n = 4p$, where p is a prime $\equiv 3 \pmod 4$ is that there exists a factorisation of $4p^2 - 1$ in the form rs with (r, s) not divisible by any prime $\equiv 3 \pmod 4$ satisfying,

either (i) $r \equiv 1 \pmod 8$, $r \neq 1$, r has no prime factor $\equiv 3 \pmod 8$,

or (ii) $r \equiv 7 \pmod 8$, $(r/p) = -1$.

Proof:

When $n = 4p$, (1) becomes,

$$x^4 + (16p^2 - 2)x^2y^2 + y^4 = z^2. \tag{21}$$

Suppose (21) has a solution (x, y, z) with $z > 0$ and minimal. Then $(x, y) = 1$ and without loss of generality we can assume that y is odd .

Case I

Suppose $x^2 \equiv y^2 \pmod p$ and $x \equiv 1 \pmod 2$.

Then we can write (21) as,

$$\left(\frac{x^2 - y^2}{4p}\right)^2 + x^2y^2 = \left(\frac{z}{4p}\right)^2.$$

Since $\left(\frac{x^2 - y^2}{p}, xy\right) = 1$, we should have,

$$\frac{x^2 - y^2}{4p} = 2XY,$$
$$xy = X^2 - Y^2.$$

Then $(\frac{1}{2}(x^2 + y^2))^2 = \frac{1}{4}(64p^2X^2Y^2 + 4(X^2 - Y^2)^2),$

$$= X^4 + (16p^2 - 2)X^2Y^2 + Y^4.$$

Since $\frac{1}{2}(x^2 + y^2) < z$, descent applies.

Hence this case is impossible.

Case II

Suppose $x^2 \not\equiv y^2 \pmod p$ and $x \equiv 1 \pmod 2$.

We can write (21) as,

$(x^2 + (8p^2 - 1)y^2 + z)(x^2 + (8p^2 - 1)y^2 - z) = 4^2.p^2.(4p^2 - 1)y^4.$

Let $A = x^2 + (8p^2 - 1)y^2 + z$ and $B = x^2 + (8p^2 - 1)y^2 - z$.

Then A and B are both even and $2^2 \| (A, B)$.

Suppose q is an odd prime dividing (A, B).

Then $q^2 | p^2(4p^2 - 1)y^4$, $q | 2x^2 + (16p^2 - 2)y^2$, $q | z$.

Now, $q|y \to q|x$, which is impossible as $(x, y) = 1$. So $q \nmid y$.

$q = p \to p | 2x^2 - 2y^2 \to x^2 \equiv y^2 \pmod p$, which is not true. Hence $q \neq p$.

Thus $q | (4p^2 - 1)$. So $q \,\Big|\, x^2 + 4p^2y^2$. Thus $q \not\equiv 3 \pmod 4$.

Hence we should have,

$$x^2 + (8p^2 - 1)y^2 \pm z = 4Rc^4,$$
$$x^2 + (8p^2 - 1)y^2 \mp z = 4Sp^2d^4,$$

where $y = cd$, $RS = 4p^2 - 1$, $(c, pd) = 1$, R&S have no prime factors $\equiv 3 \pmod 4$ in common.

Thus, $x^2 = 2Rc^4 - (8p^2 - 1)c^2d^2 + 2Sp^2d^4.$

$$= (2c^2 - Sd^2)\ (Rc^2 - 2p^2d^2)$$
$$= C \,.\, D, \text{ say.}$$

Since $RC - 2D = d^2$, $2p^2C - SD = c^2$ and $(c, d) = 1$, we have $(C, D) = 1$.

Hence we must have,

$$\begin{aligned} 2c^2 - Sd^2 &= \pm x_1^2, \\ Rc^2 - 2p^2d^2 &= \pm x_2^2, \\ x &= x_1x_2. \end{aligned} \tag{22}$$

From (22) we have, $R \not\equiv 5$ or $7 \pmod 8$. Hence we only have to consider the following two cases:

Case IIa

Suppose $R \equiv 1 \pmod 8$

Then $S \equiv 3 \pmod 8$, $C \equiv -1 \pmod 8$, $D \equiv -1 \pmod 8$.

Hence we have,

$$2c^2 - Sd^2 = -x_1^2, \tag{23}$$

$$Rc^2 - 2p^2d^2 = -x_2^2. \tag{24}$$

$R = 1 \rightarrow (R/p) = +1$ and in this case (24) is impossible modulo p. So $R \neq 1$. Now, (24) is impossible if R has a prime factor $\equiv 3 \pmod 8$. Taking $R = r$, $S = s$, we see that this case is impossible if condition (i) does not hold.

Case IIb

Suppose $R \equiv 3 \pmod 8$.

Then $S \equiv 1 \pmod 8$, $C \equiv 1 \pmod 8$, $D \equiv 1 \pmod 8$.

Hence we should have,

$$2c^2 - Sd^2 = x_1^2, \tag{25}$$

$$Rc^2 - 2p^2d^2 = x_2^2. \tag{26}$$

Suppose $S = 1$. Then $R = 4p^2 - 1$ and (26) is impossible modulo p. Hence $S \neq 1$. Now, (25) is impossible if S has a prime factor $\equiv 3 \pmod 8$. Thus taking $R = s$, $S = r$ we see that this case is impossible if (i) does not hold.

Case III

Suppose $x \equiv 0 \pmod{2}$.

Then z is odd and we have,

$$4^2 . p^2(4p^2 - 1)y^4 = A.B,$$

where $A = x^2 + (8p^2 - 1)y^2 + z$, $B = x^2 + (8p^2 - 1)y^2 - z$

$(A, B)|2z$. Since A& B are both even, we have $2||(A, B)$.

Suppose an odd prime $q|(A, B)$.

Then $q^2|p^2(4p^2 - 1)y^4$, $q|2x^2 + (16p^2 - 1)y^2$.

As in case II $q\nmid y$.

Suppose $q = p$. Then $q \nmid (4p^2 - 1)$. If $q \neq p$, then $q|(4p^2 - 1)$ and therefore $q \;|(x^2 + 4p^2y^2)$. Thus $q \not\equiv 3 \pmod{4}$.

Case IIIa

Suppose $2|(A, B)$, $p\nmid(A, B)$.

Then we have,

$$x^2 + (8p^2 - 1)y^2 \pm z = 8Rc^4,$$

$$x^2 + (8p^2 - 1)y^2 \mp z = 2p^2Sd^4, \text{ where } y = cd,$$

$(c, pd) = 1$, R,S have no factor $\equiv 3 \pmod{4}$ in common.

Thus we have,

$$\begin{aligned} x^2 &= 4Rc^4 - (8p^2 - 1)c^2d^2 + p^2Sd^4, \\ &= (4c^2 - Sd^2)(Rc^2 - p^2d^2), \\ &= C.D \text{ , say.} \end{aligned}$$

Now $(C, D) = 1$ and hence we should have,

$$4c^2 - Sd^2 = \pm x_1^2, \tag{27}$$

$$Rc^2 - p^2d^2 = \pm x_2^2, \tag{28}$$

$$x = x_1x_2,$$

where x_1 is odd, x_2 is even.

Since x_2 is even, $R \equiv 3 \pmod{4}$ is impossible. Hence $R \equiv 1 \pmod{4}$.

Suppose $R \equiv 5 \pmod 8$. Then $S \equiv 7 \pmod 8$ and in this case (27) is impossible modulo 8.

Hence $R \equiv 1 \pmod 8$ and we have,

$$4c^2 - Sd^2 = x_1^2,$$
$$Rc^2 - p^2d^2 = x_2^2. \tag{29}$$

Suppose $R = 1$. Then we have,

$$c^2 = p^2d^2 + x_2^2.$$

Hence, $pd = X^2 - Y^2$, $x_2 = 2XY$, $c^2 = (X^2 + Y^2)^2$.

Then $x_1^2 = 4(X^2 + Y^2)^2 - (4p^2 - 1)\left(\dfrac{X^2 - Y^2}{p}\right)^2$

$= 16X^2Y^2 + \left(\dfrac{X^2 - Y^2}{p}\right)^2$.

Thus $p^2x_1^2 = X^4 + (16p^2 - 2)X^2Y^2 + Y^4$.

Since $p^2x_1^2 < p^2x^2 < z^2$, descent applies. Hence $R \neq 1$.

(29) is impossible if R has a prime factor $\equiv 3 \pmod 4$.

Thus taking $R = r$, $S = s$, we see that this case is impossible if (i) does not hold.

Case IIIb

Suppose $2p \mid (A, B)$.

Then we have,

$$x^2 + (8p^2 - 1)y^2 \pm z = 8pRc^4,$$
$$x^2 + (8p^2 - 1)y^2 \mp z = 2pSd^4.$$

Hence, $x^2 = 4pRc^4 - (8p^2 - 1)c^2d^2 + pSd^4$,

$= (4pc^2 - Sd^2)(Rc^2 - pd^2)$,

$= C.D$, say.

Since $(A, B) = 1$, we should have,

$$4pc^2 - Sd^2 = \pm x_1^2, \tag{30}$$
$$Rc^2 - pd^2 = \pm x_2^2. \tag{31}$$

Since $p \equiv 3 \pmod 4$, $x_2 \equiv 0 \pmod 2$, we have, $R \not\equiv 1 \pmod 4$.

Suppose $R \equiv 3 \pmod 8$. Then $S \equiv 1 \pmod 8$ and we cannot have (30). Hence $R \equiv 7 \pmod 8$. Then,

$$4pc^2 - Sd^2 = -x_1^2,$$
$$Rc^2 - pd^2 = -x_2^2. \tag{32}$$

(32) cannot hold if $(R/p) = +1$.

Thus taking $S = s$, $R = r$, we see that this case is impossible if (ii) does not hold.

Hence the theorem.

Theorem 1.4

A necessary condition for the equation (1) to have a non-trivial solution when $n = 8p$, where p is a prime $\equiv 5, 11, 17$ or $23 \pmod{24}$, is that there exist a factorisation of $16p^2 - 1$ in the form rs with (r, s) not divisible by any prime $\equiv 3 \pmod 4$ satisfying,

either (i) $r \equiv 1 \pmod 8$, $r \neq 1$, $(r/p) = +1$,

or (ii) $r \equiv 3 \pmod 8$, $3 \mid r$, $(-r/p) = +1$, s has no prime factor $\equiv 3 \pmod 4$.

Proof:

When $n = 8p$, (1) becomes,

$$x^4 + (64p^2 - 2)x^2y^2 + y^4 = z^2 \tag{33}$$

Suppose (x, y, z) is a non-trivial solution of (33) with $z > 0$ and minimal. Then $(x, y) = 1$ and without loss of generality we can assume that y is odd.

Case I

Suppose $x^2 \equiv y^2 \pmod p$ and $x \equiv 1 \pmod 2$

Then we can write (33) as,

$$\left(\frac{x^2 - y^2}{8p}\right)^2 + x^2y^2 = \left(\frac{z}{8p}\right)^2.$$

Since $\left(\frac{x^2 - y^2}{8}, xy\right) = 1$, we should have

$$\frac{x^2 - y^2}{8p} = 2XY,$$
$$xy = X^2 - Y^2.$$

But then,

$$\left(\tfrac{1}{2}(x^2 + y^2)\right)^2 = \tfrac{1}{4}(256X^2Y^2 + 4(X^2 - Y^2)^2)$$
$$= X^4 + (64p^2 - 2)X^2Y^2 + Y^4.$$

Since $\frac{1}{2}(x^2 + y^2) < z$, descent applies.

Hence this case is impossible.

Case II

Suppose $x^2 \equiv y^2 \pmod{p}$ and $x \equiv 1 \pmod{2}$.

we can write (33) as,

$(x^2 + (32p^2 - 1)y^2 + z)(x^2 + (32p^2 - 1)y^2 - z) = p^2.64(16p^2 - 1)y^4.$

Let $A = x^2 + (32p^2 - 1)y^2 + z$ and $B = x^2 + (32p^2 - 1)y^2 - z$.

Now, $2^3 \| (A, B)$. Suppose a prime $q|(A, B)$. Then $q|x^2 + (32p^2 - 1)y^2$

$q^2|p^2(16p^2 - 1)y^4$.

$q|y \rightarrow q|x$, which is impossible. so $q\nmid y$.

$q = p \rightarrow x^2 \equiv y^2 \pmod{p}$, which is not true. So $q \neq p$

Hence $q|(16p^2 - 1)$. Thus $q \not\equiv 3 \pmod{4}$ and we have

$$x^2 + (32p^2 - 1)y^2 \pm z = 8Rc^4,$$
$$x^2 + (32p^2 - 1)y^2 \mp z = 8Sp^2d^4,$$

where $y = cd$, $(c, pd) = 1$, $RS = 16p^2 - 1$, R, S have no prime factor $\equiv 3 \pmod{4}$ in common.

By adding the two equations we have,

$$x^2 = 4Rc^4 + (32p^2 - 1)c^2d^2 + 4Sp^2d^4.$$

$$= (4c^2 - Sd^2)(Rc^2 - 4p^2d^2),$$

$$= C.D, \text{ say.}$$

Since $RC - 4D = d^2$, $4p^2C + SD = c^2$, $(c, d) = 1$, we have, $(C, D) = 1$.

Hence we have,

$$4c^2 - Sd^2 = \pm x_1^2, \tag{34}$$

$$Rc^2 - 4p^2d^2 = \pm x_2^2, \tag{35}$$

(35) $\rightarrow R \equiv \pm 1 \pmod 8$ is impossible. Hence we only have to consider the following two cases:

Case IIa

Suppose $R \equiv 3 \pmod 8$.

Then $S \equiv 5 \pmod 8$, $C \equiv -1 \pmod 8$, $D \equiv -1 \pmod 8$.

Thus we have,

$$4c^2 - Sd^2 = -x_1^2, \tag{36}$$

$$Rc^2 - 4p^2d^2 = -x_2^2. \tag{37}$$

Now, $3 \nmid R \rightarrow 3 \mid S$. Then (36) is impossible modulo 3. Hence $3|R$. (36) & (37) cannot hold simultaneously if S has a prime factor $\equiv 3 \pmod 4$ or $(-R/p) = -1$. Thus taking $R = r$, $S = s$, we see that this case is impossible if (ii) does not hold.

Case IIb

Suppose $R \equiv 5 \pmod 8$.

Then $S \equiv 3 \pmod 8$, $C \equiv 1 \pmod 8$, $D \equiv 1 \pmod 8$.

Thus we should have,

$$4c^2 - Sd^2 = x_1^2, \tag{38}$$

$$Rc^2 - 4p^2d^2 = x_2^2, \tag{39}$$

$3 \nmid S \rightarrow 3|R$. In this case (39) is impossible modulo 3. Hence $3|S$.

Now, (38) and (39) cannot hold simultaneously if either R has a prime factor $\equiv 3 \pmod 4$ or $(R/p) = -1$.

Since $RS = 16p^2 - 1$, $(R/p) = -1 \to (-S/p) = -1$.

Thus taking $R = s$, $S = r$, we see that this case is impossible if (ii) does not hold.

Case III

Suppose $x \equiv 0 \pmod 2$

Then again we have

$$64p^2(16p^2 - 1)y^4 = A.B \ ;$$

but in this case z is odd.

Since $(A, B)|2z$, we have $2||(A, B)$.

Now, suppose an odd prime $q \ |(A, B)$. Then $q|x^2 + (32p^2 - 1)y^2$, $q^2|p^2(16p^2 - 1)$. $q|y \to q|x$, which is impossible. Hence $q\nmid y$

So $q = p$ or $q|(16p^2 - 1)$. Thus we have the following cases:

Case IIIa

Suppose $p \nmid (A, B)$

Then we have

$$x^2 + (32p^2 - 1)y^2 \pm z = 32Rc^4,$$

$$x^2 + (32p^2 - 1)y^2 \mp z = 2Sp^2d^4.$$

Thus, $x^2 = 16Rc^4 + (32p^2 - 1)c^2d^2 + Sp^2d^4$

$$= (16c^2 - Sd^2)(Rc^2 - p^2d^2)$$

$$= C.D, \text{ say.}$$

Now, $(C, D) = 1$ and hence we have,

$$16c^2 - Sd^2 = \pm x_1^2, \qquad (40)$$

$$Rc^2 - p^2d^2 = \pm x_2^2, \qquad (41)$$

$$x = x_1x_2,$$

where x_1 is odd, x_2 is even.

(41) $\rightarrow R \equiv 1 \pmod 4$.

Suppose $R \equiv 5 \pmod 8$. Then $S \equiv 3 \pmod 8$ and we cannot have (40). Hence $R \equiv 1 \pmod 8$ and therefore we must have,

$$16c^2 - Sd^2 = x_1^2,$$
$$Rc^2 - p^2d^2 = x_2^2. \qquad (42)$$

Suppose $R = 1$. Then $c^2 = p^2d^2 + x_2^2$. Thus we should have $pd = X^2 - Y^2$, $x_2 = 2XY$. Then

$$x_1^2 = 16(X^2 + Y^2)^2 - (16p^2 - 1)\left(\frac{X^2 - Y^2}{p}\right)^2$$
$$= 64X^2Y^2 + \left(\frac{X^2 - Y^2}{p}\right)^2.$$

i.e, $p^2x_1^2 = X^4 + (64p^2 - 2)X^2Y^2 + Y^4$.

Since $p^2x_1^2 < p^2x^2 < z^2$, descent applies. Hence $R \neq 1$.

(42) is impossible if $(R/p) = -1$. Thus taking $R = r$, $S = s$ we see that this case is impossible if (i) does not hold.

Case IIIb

Suppose $p \mid (A, B)$.

Then we have,

$$x^2 + (32p^2 - 1)y^2 \pm z = 32Rpc^4,$$
$$x^2 + (32p^2 - 1)y^2 \mp z = 2Spd^4.$$

Thus $x^2 = 16Rpc^4 + (32p^2 - 1)c^2d^2 + Spd^4$

$= (16pc^2 - Sd^2)(Rc^2 - pd^2)$

$= C.D$, say.

Since $(C, D) = 1$, we should have

$$16pc^2 - Sd^2 = \pm x_1^2, \qquad (43)$$
$$Rc^2 - pd^2 = \pm x_2^2, \qquad (44)$$
$$x = x_1x_2,$$

where x_1 is odd, x_2 is even.

First consider $p \equiv 11$ or $23 \pmod{24}$. Then $R \equiv 3 \pmod 4$.

Suppose $R \equiv 3 \pmod 8$. Then $S \equiv 5 \pmod 8$ and we cannot have (43). Thus $R \equiv 7 \pmod 8$. Then we should have,

$$16pc^2 - Sd^2 = -x_1^2, \tag{45}$$

$$Rc^2 - pd^2 = -x_2^2 . \tag{46}$$

If $S = 1$ then $3|R$ and (46) is impossible modulo 3. Hence $S \neq 1$. Also (45) cannot hold if $(S/p) = -1$.

Thus taking $R = s$ $S = r$, we see that this case is impossible if condition (i) does not hold.

Next consider $p \equiv 5$ or $17 \pmod{24}$. Then $R \equiv 1$ or 5 (mod 8). Suppose $R \equiv 5 \pmod 8$. Then $S \equiv 3 \pmod 8$ and in this case we cannot have (45). Hence $R \equiv 1 \pmod 8$, and we have

$$16pc^2 - Sd^2 = x_1^2, \tag{47}$$

$$Rc^2 - pd^2 = x_2^2. \tag{48}$$

If $R = 1$ then $3|S$ and (47) is impossible modulo 3. Hence $R \neq 1$. Now, we cannot have (48) if $(R/p) = -1$.

Thus taking $R = r$, $S = s$, we see that this case is impossible if (i) does not hold.

Hence the theorem.

Theorem 1.5:

A necessary condition for (1) to have a non-trivial solution when $n = p_1p_2$, where p_1, p_2 are primes such that $p_1 \equiv p_2 \equiv 7, 11, 13, 17 \pmod{24}$, is that there exist a factorisation of $p_1^2p_2^2 - 4$ in the form rs, with (r, s) not divisible by any prime $\equiv 3 \pmod 4$ satisfying;

<u>either</u> (i) $r \equiv 1 \pmod 8$, $r \neq 1$, $(-s/p_1) = +1$, $(-s/p_2) = +1$,

<u>or</u> (ii) $r \equiv 3 \pmod 8$, $(-2s/p_1) = +1$, $(-2s/p_2) = +1$.

<u>Proof:</u>

When $n = p_1p_2$ (1) becomes,

$$x^4 + (p_1^2p_2^2 - 2)x^2y^2 + y^4 = z^2. \tag{49}$$

Suppose (x, y, z) is a non-trivial solution of (49) with $z > 0$ and minimal. Then $(x, y) = 1$ and without loss of generality we can assume that y is odd.

<u>Case I</u>

Suppose $x^2 \equiv y^2 \pmod{p_1p_2}$ and $x \equiv 1 \pmod 2$.

Then we can write (49) as,

$$\left(\frac{x^2 - y^2}{p_1p_2}\right)^2 + x^2y^2 = \left(\frac{z}{p_1p_2}\right)^2 \tag{50}$$

Hence we should have

$$\frac{x^2 - y^2}{p_1p_2} = 2XY,$$

$$xy = X^2 - Y^2.$$

Then $(\frac{1}{2}(x^2 + y^2))^2 = p_1^2p_2^2X^2Y^2 + (X^2 - Y^2)^2,$

$$= X^4 + (p_1^2p_2^2 - 2)X^2Y^2 + Y^4$$

Since $\frac{1}{2}(x^2 + y^2) < z$, descent applies.

Hence this case is impossible.

<u>Case II</u>

Suppose $x^2 \equiv y^2 \pmod{p_1p_2}$ and $x \equiv 0 \pmod 2$.

Then again we have (50), but now

$$xy = 2XY,$$

$$\frac{x^2 - y^2}{p_1p_2} = X^2 - Y^2.$$

Then $(x^2 + y^2)^2 = p_1^2p_2^2\,(X^2 - Y^2)^2 + 16X^2Y^2$
$= l^4 + (p_1^2p_2^2 - 2)l^2m^2 + m^4,$
with $l = X + Y$, $m = X - Y$. Since $x^2 + y^2 < z$, descent applies.
Hence this case is impossible.

Case III

Suppose $x^2 \not\equiv y^2 \pmod{p_1p_2}$.

We can write (49) as,

$$p_1^2p_2^2(p_1^2p_2^2 - 4)y^4 = (2x^2 + (p_1^2p_2^2 - 2)y^2 + 2z)(2x^2 + (p_1^2p_2^2 - 2)y^2 - 2z)$$
$$= A.B, \text{ say.}$$

Then A and B are both odd and if q is an odd prime dividing (A, B) we have $q|2x^2 + (p_1^2p_2^2 - 2)y^2$, $q^2|p_1^2p_2^2(p_1^2p_2^2 - 4)y^4$.
Now $q|y \rightarrow q|x$, which is impossible as $(x, y) = 1$. Hence $q \nmid y$.
$q = p_1$ or $p_2 \rightarrow q \nmid (p_1^2p_2^2 - 4)$. $q|(p_1^2p_2^2 - 4) \rightarrow q|(x^2 + y^2)$ and in this case $q \not\equiv 3 \pmod 4$.

Hence we have the following possibilities:

Case IIIa

Suppose $p_1 \nmid (A, B)$, $p_2 \nmid (A, B)$

Then we have,

either $2x^2 + (p_1^2p_2^2 - 2)y^2 \pm 2z = p_1^2p_2^2Rc^4,$
$2x^2 + (p_1^2p_2^2 - 2)y^2 \mp 2z = Sd^4,$

or $2x^2 + (p_1^2p_2^2 - 2)y^2 \pm 2z = p_1^2Rc^4,$
$2x^2 + (p_1^2p_2^2 - 2)y^2 \mp 2z = p_2^2Sd^4,$

where $y = cd$, $(c, d) = 1$, $RS = p_1^2p_2^2 - 4$, R & S have no factor $\equiv 3 \pmod 4$ in common.

Hence either $4x^2 = p_1^2p_2^2Rc^4 - (2p_1^2p_2^2 - 4)c^2d^2 + Sd^4,$
or $4x^2 = p_1^2Rc^4 - (2p_1^2p_2^2 - 4)c^2d^2 + p_2^2Sd^4.$

i.e <u>either</u> $4x^2 = (Rc^2 - d^2)(p_1^2p_2^2c^2 - Sd^2) = C.D$, say,

<u>or</u> $4x^2 = (Rc^2 - p_2^2d^2)(p_1^2c^2 - Sd^2) = E.F$, say.

Now $(C, D)|4$, $(E, F)|4$. Clearly C, D, E, F are all even and there are four cases.

<u>Case IIIa$_1$</u>

Suppose $R \equiv 1 \pmod 8$.

Then $S \equiv 5 \pmod 8$ and we should have,

<u>either</u> $Rc^2 - d^2 = \pm 16\ {}_1^2$, <u>or</u> $Rc^2 - p_2^2d^2 = \pm 16x_1^2$,

$p_1^2p_2^2c^2 - Sd^2 = \pm 4x_2^2$, $\qquad p_1^2c^2 - Sd^2 = \pm 4x_2^2$,

$x = 4x_1x_2$, $\qquad x = 4x_1x_2$.

We notice that in both cases the minus sign is impossible. Thus we have,

<u>either</u> $Rc^2 = d^2 + 16x_1^2$, (51)

$p_1^2p_2^2c^2 - Sd^2 = 4x_2^2$, (52)

<u>or</u> $Rc^2 = p_2^2d^2 + 16x_1^2$, (53)

$p_1^2c^2 - Sd^2 = 4x_2^2$. (54)

<u>Suppose $R = 1$</u>.

Then (51) $\to c^2 = d^2 + 16x_1^2$. Thus we should have,

$d = X^2 - Y^2$, $2x_1 = XY$. Then

$4x_2^2 = 4p_1^2p_2^2X^2Y^2 + 4(X^2 - Y^2)^2$.

i.e $x_2^2 = X^4 + (p_1^2p_2^2 - 2)X^2Y^2 + Y^4$. Since $x_2 < x < z$, descent applies. Thus we cannot have $R = 1$ in (51).

Now (53) $\to c^2 = p_2^2d^2 + 16x_1^2$. Thus $p_2d = X^2 - Y^2$,

$2x_1 = XY$. Then $4x_2^2 = p_1^2(X^2 + Y^2)^2 - \left(\frac{p_1^2p_2^2 - 4}{p_2^2}\right)(X^2 - Y^2)^2$

i.e $4p_2^2x_2^2 = p_1^2p_2^2(X^2 + Y^2)^2 - (p_1^2p_2^2 - 4)(X^2 - Y^2)^2$

i.e $p_2^2x_2^2 = X^4 + (p_1^2p_2^2 - 2)X^2Y^2 + Y^4$.

Since $p_2x_2 < p_2x < z$, descent applies.

Hence we cannot have $R = 1$ in (53).

Now (52) cannot hold if $(-S/p_1)$ or $(-S/p_2) = -1$. Also, we cannot have (53) & (54) if $(R/p_2) = -1$ or $(-S/p_1) = -1$. Since $(R/p_2) = -1 \to (-S/p_2) = -1$, (53) & (54) cannot hold simultaneously if $(-S/p_1)$ or $(-S/p_2) = -1$.

Thus taking $R = r$, $S = s$, we see that this case is impossible if (i) does not hold.

Case III a_2

Suppose $R \equiv 5 \pmod 8$.

Then $S \equiv 1 \pmod 8$ and we have

either $Rc^2 - d^2 = \pm 4x_1^2$, $p_1^2p_2^2c^2 - Sd^2 = \pm 16x_2^2$, $x = 4x_1x_2$,

or $Rc^2 - p_2^2d^2 = \pm 4x_1^2$, $p_1^2c^2 - Sd^2 = \pm 16x_2^2$, $x = 4x_1x_2$.

In both cases the plus sign is impossible. Thus

either

$$Sd^2 = p_1^2p_2^2c^2 + 16x_2^2, \qquad (55)$$

$$4x_1^2 = d^2 - Rc^2, \qquad (56)$$

or

$$Sd^2 = p_1^2c^2 + 16x_2^2, \qquad (57)$$

$$4x_1^2 = p_2^2d^2 - Rc^2. \qquad (58)$$

Suppose $S = 1$.

Then (55) $\to d^2 = p_1^2p_2^2c^2 + 16x_2^2$. Thus we should have $p_1p_2c = X^2 - Y^2$, $2x_2 = XY$. But then (56) would imply that $4x_1^2 = (X^2 + Y^2)^2 - (p_1^2p_2^2 - 4)\left(\dfrac{X^2 - Y^2}{p_1p_2}\right)^2$

Thus $p_1^2p_2^2x_1^2 = X^4 + (p_1^2p_2^2 - 2)X^2Y^2 + Y^4$. Since $p_1p_2x_1 < p_1p_2x < z$, descent applies.

(57) $\to d^2 = p_1^2c^2 + 16x_2^2$. Thus we should have,

$p_1c = X^2 - Y^2$, $2x_2 = XY$. Then (58) would imply that
$$4x_1^2 = p_2^2(X^2 + Y^2)^2 - (p_1^2p_2^2 - 4)\left(\frac{X^2 - Y^2}{p_1}\right)^2$$
Thus $p_1^2x_1^2 = X^4 + (p_1^2p_2^2 - 4)X^2Y^2 + Y^4$. Since $p_1x_1 < p_1x < z$, descent applies.

Thus $S \neq 1$. Now we cannot have (55) if (S/p_1) or $(S/p_2) = -1$. i.e if $(-R/p_1)$ or $(-R/p_2) = -1$. Also (57) & (58) cannot hold simultaneously if (S/p_1) or $(-R/p_2) = -1$. i.e if $(-R/p_1)$ or $(-R/p_2) = -1$. Thus taking $R = s$, $S = r$ we see that case IIIa$_2$ is impossible if (i) does not hold.

<u>Case IIIa$_3$</u>

Suppose $R \equiv 3 \pmod 8$.

Then $S \equiv 7 \pmod 8$ and we should have,

<u>either</u> $Rc^2 - d^2 = 2x_1^2$,
$$p_1^2p_2^2c^2 - Sd^2 = 2x_2^2, \tag{59}$$
<u>or</u>
$$Rc^2 - p_2^2d^2 = 2x_1^2, \tag{60}$$
$$p_1^2c^2 - Sd^2 = 2x_2^2. \tag{61}$$

(59) is impossible if $(-2S/p_1)$ or $(-2S/p_2) = -1$. (60) & (61) cannot hold simultaneously if $(-2S/p_1)$ or $(2R/p_2) = -1$; i.e if $(-2S/p_1)$ or $(-2S/p_2) = -1$. Thus taking $R = r$, $S = s$ we see that this case is impossible if (ii) does not hold.

<u>Case IIIa$_4$</u>

Suppose $R \equiv 7 \pmod 8$.

Then $S \equiv 3 \pmod 8$ and we have

<u>either</u> $Rc^2 - d^2 = -2x_1^2$,
$$p_1^2p_2^2c^2 - Sd^2 = -2x_2^2, \tag{62}$$

<u>or</u> $Rc^2 - p_2^2d^2 = -2x_1^2,$ (63)

$p^2c^2 - Sd^2 = -2x_2^2.$ (64)

(62) is impossible if $(2S/p_1)$ or $(2S/p_2) = -1$. i.e if $(-2R/p_1)$ or $(-2R/p_2) = -1$. Also (63) & (64) cannot hold simultaneously if $(-2R/p_2)$ or $(2S/p_1) = -1$. i.e if $(-2R/p_1)$ or $(-2R/p_2) = -1$. Thus taking $R = s$, $S = r$ we see that this case is impossible if (ii) does not hold.

<u>Case IIIb</u>

Suppose $p_1 | (A, B)$, $p_2 \nmid (A, B)$.

Then we have

$$2x^2 + (p_1^2p_2^2 - 2)y^2 \pm 2z = p_1p_2^2Rc^4,$$

$$2x^2 + (p_1^2p_2^2 - 2)y^2 \pm 2z = p_1Sd^4.$$

Hence $4x^2 = p_1p_2^2Rc^4 - (2p_1^2p_2^2 - 4)c^2d^2 + p_1Sd^4,$

$= (Rc^2 - p_1d^2)(p_1p_2^2c^2 - Sd^2)$

$= C.D$, say.

Now $(C, D) = 1$ and we have the following cases:

<u>Case IIIb$_1$</u>

Suppose $R \equiv 1 \pmod 8$.

Then we have

$$Rc^2 - p_1d^2 = \theta 16x_1^2, \qquad (65)$$

$$p_1p_2^2c^2 - Sd^2 = \theta 4x_2^2, \qquad (66)$$

when $p_1 \equiv 17 \pmod{24}$,

$$Rc^2 - p_1d^2 = \theta 4x_1^2, \qquad (67)$$

$$p_1p_2^2c^2 - Sd^2 = \theta 16x_2^2, \qquad (68)$$

when $p_1 \equiv 13 \pmod{24}$,

$$Rc^2 - p_1d^2 = 2x_1^2, \qquad (69)$$

$$p_1p_2^2c^2 - Sd^2 = 2x_2^2, \qquad (70)$$

when $p_1 \equiv 7 \pmod{24}$,

$$Rc^2 - p_1d^2 = -2x_1^2, \tag{71}$$

$$p_1p_2^2c^2 - Sd^2 = -2x_2^2, \tag{72}$$

when $p_1 \equiv 11 \pmod{24}$, where $\theta = \pm 1$.

(65) & (66) $\rightarrow c^2 = (p_1x_2^2 - 4Sx_1^2)$ and hence $\theta = +1$.

(67) & (68) $\rightarrow c^2 = (4p_1x_2^2 - Sx_1^2)$ and hence in this case $\theta = -1$.

Suppose $R = 1$. Then $3|S$ and (66), (68), (70), & (72) are impossible modulo 3. Hence $R \neq 1$. Also, we cannot have (66), (68), (70), (72) if $(-S/p_1)$ or $(-S/p_2) = -1$. Thus taking $R = r$, $S = s$, we see that case IIIb$_1$ is impossible if (i) does not hold.

Case IIIb$_2$

Suppose $R \equiv 5 \pmod 8$.

Then $S \equiv 1 \pmod 8$ and we have

$$Rc^2 - p_1d^2 = \theta 4x_1^2, \tag{73}$$

$$p_1p_2^2c^2 - Sd^2 = \theta 16x_2^2, \tag{74}$$

when $p_1 \equiv 17 \pmod{24}$;

$$Rc^2 - p_1d^2 = \theta 16x_1^2, \tag{75}$$

$$p_1p_2^2c^2 - Sd^2 = \theta 4x_2^2, \tag{76}$$

when $p_1 \equiv 13 \pmod{24}$;

$$Rc^2 - p_1d^2 = -2x_1^2, \tag{77}$$

$$p_1p_2^2c^2 - Sd^2 = -2x_2^2, \tag{78}$$

when $p_1 \equiv 7 \pmod{24}$;

$$Rc^2 - p_1d^2 = 2x_1^2, \tag{79}$$

$$p_1p_2^2c^2 - Sd^2 = 2x_2^2, \tag{80}$$

when $p_1 \equiv 11 \pmod{24}$, where $\theta = \pm 1$.

(73) & (74) $\rightarrow$ $c^2 = \theta(4p_1x_2^2 - Sx_1^2)$ and hence $\theta = -1$.

(75) & (76) $\rightarrow$ $c^2 = \theta(p_1x_2^2 - 4Sx_1^2)$ and hence in this case $\theta = +1$.

Suppose $S = 1$. Then $3|R$ and (73), (75), (77), (79) are impossible modulo 3. Hence $S \neq 1$. Now suppose $(-R/p_1) = -1$. Then

$p_1 \equiv 1 \pmod 4 \rightarrow (-S/p_1) = (S/p_1) = -1$ and hence (74), (76) are impossible,

$p_1 \equiv 7 \pmod 8 \rightarrow (2S/p_1) = -1$, and hence (78) is impossible,

$p_1 \equiv 3 \pmod 8 \rightarrow (-2S/p_1) = -1$, and hence (80) is impossible.

Similarly if $(-R/p_2) = -1$, we cannot have (74), (76), (78) & (80). Thus taking $R = s$, $S = r$, we see that this case is impossible if (i) does not hold.

Case IIIb_3

Suppose $R \equiv 3 \pmod 8$.

Then $S \equiv 7 \pmod 8$ and we have

$$Rc^2 - p_1d^2 = 2x_1^2,$$
$$p_1p_2^2c^2 - Sd^2 = 2x_2^2, \qquad (81)$$

when $p_1 \equiv 17 \pmod{24}$;

$$Rc^2 - p_1d^2 = -2x_1^2,$$
$$p_1p_2^2c^2 - Sd^2 = -2x_2^2, \qquad (82)$$

when $p_1 \equiv 13 \pmod{24}$;

$$Rc^2 - p_1d^2 = \theta 4x_1^2, \qquad (83)$$
$$p_1p_2^2c^2 - Sd^2 = \theta 16x_2^2 \qquad (84)$$

when $p_1 \equiv 7 \pmod{24}$;

$$Rc^2 - p_1d^2 = \theta 16x_1^2, \tag{85}$$
$$p_1p_2^2c^2 - Sd^2 = \theta 4x_2^2 \tag{86}$$

when $p_1 \equiv 11 \pmod{24}$, where $\theta = \pm 1$.

In (83) & (84) we have $\theta = +1$ and in (85) & (86) we have $\theta = -1$.

Now (81), (82), (84) & (86) are impossible if $(-2S/p_1)$ or $(-2S/p_2) = -1$. Thus taking $R = r$, $S = s$, we see that this case is impossible if (ii) does not hold.

Case IIIb_4

Suppose $R \equiv 7 \pmod 8$.

Then $S \equiv 3 \pmod 8$ and we have,

$$Rc^2 - p_1d^2 = -2x_1^2,$$
$$p_1p_2^2c^2 - Sd^2 = -2x_2^2, \tag{87}$$

when $p_1 \equiv 17 \pmod{24}$;

$$Rc^2 - p_1d^2 = 2x_1^2,$$
$$p_1p_2^2c^2 - Sd^2 = 2x_2^2; \tag{88}$$

when $p_1 \equiv 13 \pmod{24}$,

$$Rc^2 - p_1d^2 = \theta 16x_1^2, \tag{89}$$
$$p_1p_2^2c^2 - Sd^2 = \theta 4x_2^2, \tag{90}$$

when $p_1 \equiv 7 \pmod{24}$;

$$Rc^2 - p_1d^2 = \theta 4x_1^2, \tag{91}$$
$$p_1p_2^2c^2 - Sd^2 = \theta 16x_2^2, \tag{92}$$

when $p_1 \equiv 11 \pmod{24}$, where $\theta = \pm 1$.

In (89) & (90) we have $\theta = -1$ and in (91) & (92) we have $\theta = +1$.

Now suppose $(-2R/p_1) = -1$. Then

$p_1 \equiv 1 \pmod 4 \rightarrow (-2S/p_1) = (2S/p_1) = -1$, and hence we cannot have (87) & (88),

$p_1 \equiv 7 \pmod 8 \rightarrow (R/p_1) = -1$, and hence we cannot have (89),

$p_1 \equiv 3 \pmod 8 \rightarrow (R/p_1) = -1$, and hence we cannot have (91). Similarly if $(-R/p_2) = -1$, we cannot have (87) (88), (89) & (91).

Thus taking $R = s$; $S = r$, we see that this case is impossible if (ii) does not hold.

Case IIIc

Suppose $p_2 | (A, B)$, $p_1 \nmid (A, B)$.

This case is similar to case IIIb. We will get the same set of equations with p_1 & p_2 interchanged. We notice that the conditions for case IIIb to be impossible, are all involving modulo 24. Since $p_1 \equiv p_2 \pmod{24}$, this case is also impossible under the same conditions.

Hence the theorem.

Theorem 1.6:

The equation (1) has no non-trivial solutions when $n = 3p$, where p is a prime such that $p \equiv 5$ or $7 \pmod 8$, $3p + 2$ & $3p - 2$ are primes.

Proof:

When $n = 3p$ (1) becomes

$$x^4 + (9p^2 - 2)x^2y^2 + y^4 = z^2 \qquad (93)$$

Suppose (x, y, z) is a non-trivial solution of (91) with $z > 0$ and minimal. Then $(x, y) = 1$ and without loss of generality we can assume that y is odd.

From case I & case II of theorem 1.5, it follows that $x^2 \equiv y^2 \pmod{3p}$ is impossible. So we only have to consider the case when $x^2 \not\equiv y^2 \pmod{3p}$.

We can write (91) as

$$9p^2(9p^2 - 4)y^4 = (2x^2 + (9p^2 - 2)y^2 + 2z)(2x^2 + (9p^2 - 2)y^2 - 2z),$$
$$= A.B, \text{ say.}$$

Then $(A, B) = 1$, 3 or p .

Case I

Suppose $(A, B) = 1$.

Then we have

either $$2x^2 + (9p^2 - 2)y^2 \pm 2z = 9p^2Rc^4,$$
$$2x^2 + (9p^2 - 2)y^2 \mp 2z = Sd^4,$$

or $$2x^2 + (9p^2 - 2)y^2 \pm 2z = 9Rc^4,$$
$$2x^2 + (9p^2 - 2)y^2 \mp 2z = p^2Sd^4,$$

where $y = cd$, $(Rc, Sd) = 1$, $RS = 9p^2 - 4$.

Thus either $$4x^2 = (Rc^2 - d^2)(9p^2c^2 - Sd^2),$$

or $$4x^2 = (Rc^2 - p^2d^2)(9c^2 - Sd^2).$$

Case Ia

Suppose $R \equiv 1 \pmod 8$

Then we have

either $$Rc^2 - d^2 = 16x_1^2,$$
$$9p^2c^2 - Sd^2 = 4x_2^2, \tag{94}$$

or $$Rc^2 - p^2d^2 = 16x_1^2,$$
$$9c^2 - Sd^2 = 4x_2^2. \tag{95}$$

As in case IIIa_1 of Theorem 1.5, we cannot have $R = 1$.

We only have to consider $R = 3p + 2$, $p \equiv 5 \pmod 8$.

Now, $R = 3p + 2 \to S = 3p - 2$. But then (94) & (95) are impossible modulo 3.

Thus we cannot have this case.

Case Ib

Suppose $R \equiv 5 \pmod 8$.

Then we have

either
$$Rc^2 - d^2 = -4x_1^2, \quad 9p^2c^2 - Sd^2 = -16x_2^2, \tag{96}$$
or
$$Rc^2 - p^2d^2 = -4x_1^2, \quad 9c^2 - Sd^2 = -16x_2^2. \tag{97}$$

As in case IIIa_2 of Theorem 1.5, we cannot have $S = 1$.

So we only have to consider $S = 3p + 2$, $p \equiv 5 \pmod 8$.

But in this case (96) & (97) are impossible modulo 3.

Thus we cannot have this case.

Case Ic

Suppose $R \equiv 3 \pmod 8$.

Then we have

either
$$Rc^2 - d^2 = 2x_1^2, \quad 9p^2c^2 - Sd^2 = 2x_2^2, \tag{98}$$
or
$$Rc^2 - p^2d^2 = 2x_1^2, \quad 9c^2 - Sd^2 = 2x_2^2. \tag{99}$$

The only factor $\equiv 3 \pmod 8$ of $9p^2 - 4$ is $3p - 2$, $p \equiv 7 \pmod 8$. Now $R = 3p - 2 \to S = 3p + 2$ and both (98) & (99) are impossible modulo 3.

Thus this case is impossible.

Case Id

Suppose $R \equiv 7 \pmod 8$.

Then we have

either $\quad Rc^2 - d^2 = -2x_1^2,$

$$9p^2c^2 - Sd^2 = -2x_2^2, \tag{100}$$

or $\quad Rc^2 - p^2d^2 = -2x_1^2,$

$$9c^2 - Sd^2 = -2x_2^2. \tag{101}$$

The only factor $\equiv 7 \pmod 8$ of $9p^2 - 4$ is $3p + 2$, $p \equiv 7 \pmod 8$. Now, $R = 3p + 2 \rightarrow S = 3p - 2$, and both (100) & (101) are impossible modulo 3.

Hence we cannot have this case.

Case II

Suppose $(A, B) = 3$.

Then we have $4x^2 = (Rc^2 - 3d^2)(3p^2c^2 - Sd^2)$.

Case IIa

Suppose $R \equiv 1 \pmod 8$.

Then we have

$$Rc^2 - 3d^2 = -2x_1^2, \tag{102}$$

$$3p^2c^2 - Sd^2 = -2x_2^2. \tag{103}$$

Suppose $R = 1$. Then $S = 9p^2 - 4$ and (103) is impossible modulo p. Thus $R \neq 1$. So we only have to consider $R = 3p + 2$, $p \equiv 5 \pmod 8$. But then (102) is impossible modulo 3. Thus this case is impossible.

Case IIb

Suppose $R \equiv 5 \pmod 8$.

Then we have

$$Rc^2 - 3d^2 = 2x_1^2, \tag{104}$$

$$3p^2c^2 - Sd^2 = 2x_2^2. \tag{105}$$

Suppose $S = 1$. Then (105) is impossible modulo 3. Hence we cannot have $S = 1$. So we only have to consider the case when $R = 3p - 2$, $p \equiv 5 \pmod 8$. Since (104) is impossible modulo 3, we cannot have this case.

Case IIc

Suppose $R \equiv 3 \pmod 8$.

Then we have

$$Rc^2 - 3d^2 = -16x_1^2, \tag{106}$$
$$3p^2c^2 - Sd^2 = -4x_2^2.$$

If $p \equiv 5 \pmod 8$ then $9p^2 - 4$ has no factor $\equiv 3 \pmod 8$ and this case doesn't arise. So we only have to consider the case when $R = 3p - 2$, $p \equiv 7 \pmod 8$. But then (106) is impossible modulo 3.

Thus we cannot have this case.

Case IId

Suppose $R \equiv 7 \pmod 8$.

Then we have

$$Rc^2 - 3d^2 = 4x_1^2, \tag{107}$$
$$3p^2c^2 - Sd^2 = 16x_2^2.$$

If $p \equiv 5 \pmod 8$ then $9p^2 - 4$ has no factor $\equiv 7 \pmod 8$ and this case doesn't arise. When $p \equiv 7 \pmod 8$ we have $3p + 2 \equiv 7 \pmod 8$. Since then (107) is impossible modulo 3, we cannot have this case.

Case III

Suppose $(A, B) = p$.

Then we have $4x^2 = (Rc^2 - pd^2)(9pc^2 - Sd^2)$

Case IIIa

Suppose $R \equiv 1 \pmod 8$.

Then we have

$$Rc^2 - pd^2 = -4x_1^2,$$
$$9pc^2 - Sd^2 = -16x_2^2, \tag{108}$$

when $p \equiv 5 \pmod 8$;

$$Rc^2 - pd^2 = 2x_1^2,$$
$$9pc^2 - Sd^2 = 2x_2^2, \tag{109}$$

when $p \equiv 7 \pmod 8$.

The only factors $\equiv 1 \pmod 8$ of $9p^2 - 4$ are 1 & $3p - 2$, $p \equiv 5 \pmod 8$. In both cases $3p + 2 | S$ and since $(-9pc^2/3p + 2) = -1$, when $p \equiv 5 \pmod 8$ & $(18pc^2/3p + 2) = -1$, when $p \equiv 7 \pmod 8$, we cannot have (108) & (109). Hence this case is impossible.

Case IIIb

Suppose $R \equiv 5 \pmod 8$

Then we have

$$Rc^2 - pd^2 = 16x_1^2,$$
$$9pc^2 - Sd^2 = 4x_2^2,$$

when $p \equiv 5 \pmod 8$;

$$Rc^2 - pd^2 = -2x_1^2,$$
$$9pc^2 - Sd^2 = -2x_2^2,$$

when $p \equiv 7 \pmod 8$.

The possibilities are $R = 9p^2 - 4$ & $R = 3p - 2$, when $p \equiv 5 \pmod 8$; $R = 9p^2 - 4$ when $p \equiv 7 \pmod 8$. Thus we have

$$16x_1^2 \equiv -p \pmod{3p - 2},\ p \equiv 5 \pmod 8,$$
$$4x_1^2 \equiv 2pd^2 \pmod{3p - 2},\ p \equiv 7 \pmod 8.$$

Since $(-p/3p-2) = (3p-2/p) = -1$, when $p \equiv 5 \pmod 8$

and $(2pd^2/3p-2) = (3p-2/p) = -1$, when $p \equiv 7 \pmod 8$,

both congruences are impossible.

Thus we cannot have this case.

Case IIIc

Suppose $R \equiv 3 \pmod 8$.

The only possibility is $R = 3p - 2$, $p \equiv 7 \pmod 8$.

Then we have

$$\begin{aligned}(3p-2)c^2 - pd^2 &= 4x_1^2,\\ 9pc^2 - (3p+2)d^2 &= 16x_2^2.\end{aligned} \tag{110}$$

Since $(3p-2/p) = (-2/p) = -1$, we cannot have (110).

Thus this case is impossible.

Case IIId

Suppose $R \equiv 7 \pmod 8$.

Then the only possibility is $R = 3p + 2$, $p \equiv 7 \pmod 8$.

Then we have

$$\begin{aligned}(3p+2)c^2 - pd^2 &= -16x_1^2,\\ 9pc^2 - (3p-2)d^2 &= -4x_2^2.\end{aligned} \tag{111}$$

Since $(3p+2/p)(-1/p) = -1$, we cannot have (111).

Hence this case is impossible.

Hence the theorem.

Theorem 1.7

The equation (1) has no non-trivial solutions when $n = 4p_1p_2$, where p_1, p_2 are primes such that $p_1 \equiv 5$ or $17 \pmod{24}$, $p_2 \equiv 7$ or $19 \pmod{24}$, and if $4p_1^2p_2^2 - 1$ has prime factorisation of the form

$3^t \cdot \dfrac{p_1p_2 - 1}{3^t} \cdot 2p_1p_2 + 1$, $t \geqslant 1$ and odd.

Proof:

When $n = 4p_1p_2$, (1) becomes

$$x^4 + (16p_1^2p_2^2 - 2)x^2y^2 + y^4 = z^2 \tag{112}$$

Suppose $\{x, y, z\}$ is a non-trivial solution of (112) with $z > 0$ & minimal. Then $(x, y) = 1$ and without loss of generality we can assume that y is odd.

Case I

Suppose $x^2 \equiv y^2 \pmod{p_1p_2}$ and $x \equiv 1 \pmod 2$. Then we have

$$\left(\frac{x^2 - y^2}{4p_1p_2}\right)^2 + x^2y^2 = \left(\frac{z}{4p_1p_2}\right)^2$$

Thus we should have

$$\frac{x^2 - y^2}{4p_1p_2} = 2XY,$$
$$xy = X^2 - Y^2.$$

But then $(\frac{1}{2}(x^2 + y^2))^2 = (4XYp_1p_2)^2 + (X^2 - Y^2)^2$
$= X^4 + (16p_1^2p_2^2 - 2)X^2Y^2 + Y^4.$

Since $\frac{1}{2}(x^2 + y^2) < z$, descent applies.

Hence this case is impossible.

Case II

Suppose $x^2 \not\equiv y^2 \pmod{p_1p_2}$ and $x \equiv 1 \pmod 2$.

We can write (112) as

$$p_1^2p_2^2(4p_1^2p_2^2 - 1)y^4 = (x^2 + (8p_1^2p_2^2 - 1)y^2 + z)(x^2 + (8p_1^2p_2^2 - 1)y^2 - z)$$
$$= A.B \text{ , say.} \tag{113}$$

Then A & B are both even and $2^2 || (A, B)$

Suppose an odd prime $q|(A, B)$. Then $q = p_1$ or p_2.

Thus $(A, B) = 4$ or $4p_1$ or $4p_2$.

Case IIa

Suppose $(A, B) = 4$.

Then

either $x^2 + (8p_1^2p_2^2 - 1)y^2 \pm z = 4Rc^4$,

$x^2 + (8p_1^2p_2^2 - 1)y^2 \mp z = 4Sp_1^2p_2^2d^4$,

or $x^2 + (8p_1^2p_2^2 - 1)y^2 \pm z = 4Rp_1^2c^4$,

$x^2 + (8p_1^2p_2^2 - 1)y^2 \mp z = 4Sp_2^2d^4$,

where $RS = 4p_1^2p_2^2 - 1$, $(Rc, Sd) = 1$.

Thus we have

either $x^2 = 2Rc^4 - (8p_1^2p_2^2 - 1)c^2d^2 + 2Sp_1^2p_2^2d^4$,

$= (2c^2 - Sd^2)(Rc^2 - 2p_1^2p_2^2d^2)$,

or $x^2 = 2Rp_1^2c^4 - (8p_1^2p_2^2 - 1)c^2d^2 + 2Sp_2^2d^4$,

$= (2p_1^2c^2 - Sd^2)(Rc^2 - 2p_2^2d^2)$.

Hence either $2c^2 - Sd^2 = \pm x_1^2$,

$Rc^2 - 2p_1^2p_2^2d2 = \pm x_2^2$, (114)

or $2p_1^2c^2 - Sd^2 = \pm x_1^2$,

$Rc^2 - 2p_2^2d^2 = \pm x_2^2$. (115)

Both (114) & (115) implies that $R \not\equiv 5$ or $7 \pmod 8$

Thus $R \equiv 1$ or $3 \pmod 8$.

Case IIa_1

Suppose $R \equiv 3 \pmod 8$. Then we have to consider

$R = 3^t$ & $R = 4p_1^2p_2^2 - 1$.

Now we have

either $2c^2 - Sd^2 = x_1^2$,

$Rc^2 - 2p_1^2p_2^2d^2 = x_2^2$, (116)

<u>or</u> $$2p_1^2c^2 - Sd^2 = x_1^2,$$
$$Rc^2 - 2p_2^2d^2 = x_2^2 \qquad (117)$$

<u>First suppose that $R = 3^t$.</u>

Then both (116) & (117) implies that

$$x_2^2 \equiv 3^tc^2 \pmod{p_2}.$$

Since $(3^tc^2/p_2) = (3^t/p_2) = (3/p_2) = -1$, we cannot have (116) or (117). Thus $R \neq 3^t$.

<u>Next suppose that $R = 4p_1^2p_2^2 - 1$.</u>

Then both (116) & (117) would imply that

$$x_2^2 \equiv (4p_1^2p_2^2 - 1)c^2 \pmod{p_2}.$$

Since $(4p_1^2p_2^2 - 1/p_2) = (-1/p_2) = -1$, we cannot have (116) or (117).

Thus this case is impossible.

<u>Case IIa_2</u>

Suppose $R \equiv 1 \pmod 8$.

Then we have

<u>either</u> $$2c^2 - Sd^2 = -x_1^2,$$
$$Rc^2 - 2p_1^2p_2^2d^2 = -x_2^2, \qquad (118)$$

<u>or</u> $$2p_1^2c^2 - Sd^2 = -x_1^2,$$
$$Rc^2 - 2p_2^2d^2 = -x_2^2. \qquad (119)$$

The possibilities are $R = 1$ & $R = 3^{-t}(p_1^2p_2^2 - 1)$.

<u>Suppose $R = 1$.</u> Then (118) & (119) are impossible modulo p_2. Thus $R \neq 1$.

<u>Next suppose that $R = 3^{-t}(4p_1^2p_2^2 - 1)$.</u> Then both (118) & (119) would imply that

$$x_2^2 \equiv -3^{-t}(4p_1^2p_2^2 - 1)c^2 \pmod{p_2}.$$

Since $(-3^{-t}(4p_1^2p_2^2 - 1)c^2/p_2) = (-1/p_2)(3^t/p_2)(-1/p_2)$

$= -1$, we cannot have (118) or (119).

Thus this case is impossible.

Case IIb

Suppose $(A, B) = 4p_1$.

Then we have

$$x^2 + (8p_1^2p_2^2 - 1)y^2 \pm z = 4Rp_1c^4,$$
$$x^2 + (8p_1^2p_2^2 - 1)y^2 \mp z = 4Sp_1p_2^2d^4.$$

Thus $x^2 = (2p_1c^2 - Sd^2)(Rc^2 - 2p_1p_2^2d^2)$.

Hence we should have

$$2p_1c^2 - Sd^2 = \pm x_1^2,$$
$$Rc^2 - 2p_1p_2^2d^2 = \pm x_2^2.$$

Since $p_1 \equiv 1$ or $5 \pmod 8$, we cannot have $R \equiv 5$ or $7 \pmod 8$.

Thus $R \equiv 1$ or $3 \pmod 8$.

Case IIb$_1$

Suppose $R \equiv 1 \pmod 8$.

Then we have

$$2p_1c^2 - Sd^2 = -x_1^2, \qquad (120)$$
$$Rc^2 - 2p_1p_2^2d^2 = -x_2^2.$$

The only possibilities are $R = 1$ & $R = 3^{-t}(4p_1^2p_2^2 - 1)$.

But then $3|S$ and (120) is impossible modulo 3.

Thus we cannot have this case.

Case IIb$_2$

Suppose $R \equiv 3 \pmod 8$.

Then we have

$$2p_1c^2 - Sd^2 = x_1^2,$$
$$Rc^2 - 2p_1p_2^2d^2 = x_2^2. \qquad (121)$$

But in this case $3|R$ and (121) is impossible modulo 3.

Thus we cannot have this case.

Case IIc

Suppose $(A, B) = 4p_2$.

Then we have

$$2p_2c^2 - Sd^2 = \pm x_1^2,$$
$$Rc^2 - 2p_1^2p_2d^2 = \pm x_2^2.$$

Since $p_2 \equiv 3$ or $7 \pmod 8$, we cannot have $R \equiv 1$ or $3 \pmod 8$.

Thus $R \equiv 5$ or $7 \pmod 8$.

Case IIc$_1$

Suppose $R \equiv 5 \pmod 8$.

Then we have

$$2p_2c^2 - Sd^2 = -x_1^2,$$
$$Rc^2 - 2p_1^2p_2d^2 = -x_2^2. \tag{122}$$

The only value that R can take is $2p_1p_2 - 1$. Thus $3|R$ and (122) is impossible modulo 3.

Hence we cannot have this case.

Case IIc$_2$

Suppose $R \equiv 7 \pmod 8$

Then we have

$$2p_2c^2 - Sd^2 = x_1^2, \tag{123}$$
$$Rc^2 - 2p_1^2p_2d^2 = x_2^2.$$

The only possibilities are $R = 3^{-t}(2p_1p_2 - 1)$ & $R = 2p_1p_2 + 1$. In both cases $3|S$ and (123) is impossible modulo 3.

Thus we cannot have this case.

Case III

Suppose $x \equiv 0 \pmod 2$

Then again we have (113), but now z is odd. Thus $2||(A, B)$ and we have the following possibilities:

Case IIIa

Suppose $(A, B) = 2$.

Then we have

$$\text{either} \quad x^2 + (8p_1^2p_2^2 - 1)y^2 \pm z = 2Rc^4,$$
$$x^2 + (8p_1^2p_2^2 - 1)y^2 \mp z = 8Sp_1^2p_2^2d^4,$$
$$\text{or} \quad x^2 + (8p_1^2p_2^2 - 1)y^2 \pm z = 2Rp_1^2c^4,$$
$$x^2 + (8p_1^2p_2^2 - 1)y^2 \mp z = 8Sp_2^2d^4,$$

where $RS = 4p_1^2p_2^2 - 1$, $(Rc, Sd) = 1$.

Hence

$$\text{either} \quad x^2 = Rc^4 - (8p_1^2p_2^2 - 1)c^2d^2 + 4Sp_1^2p_2^2d^4,$$
$$= (Rc^2 - 4p_1^2p_2^2d^2)(c^2 - Sd^2)$$
$$\text{or} \quad x^2 = Rp_1^2c^4 - (8p_1^2p_2^2 - 1)c^2d^2 + 4Sp_2^2d^4,$$
$$= (Rc^2 - 4p_2^2d^2)(p_1^2c^2 - Sd^2).$$

Thus we must have

$$\text{either} \quad Rc^2 - 4p_1^2p_2^2d^2 = \pm x_1^2,$$
$$c^2 - Sd^2 = \pm x_2^2,$$
$$\text{or} \quad Rc^2 - 4p_2^2d^2 = \pm x_1^2,$$
$$p_1^2c^2 - Sd^2 = \pm x_2^2,$$

where x_1 is odd, x_2 is even, $x = x_1x_2$.

In both cases we cannot have $R \equiv \pm 1 \pmod 8$. Hence $R \equiv 3$ or $5 \pmod 8$.

Case IIIa_1

Suppose $R \equiv 3 \pmod 8$.

Then we have

$$\underline{\text{either}} \quad Rc^2 - 4p_1^2p_2^2d^2 = -x_1^2, \tag{124}$$

$$c^2 - Sd^2 = -x_2^2, \tag{125}$$

$$\underline{\text{or}} \quad Rc^2 - 4p_2^2d^2 = -x_1^2, \tag{126}$$

$$p_1^2c^2 - Sd^2 = -x_2^2. \tag{127}$$

<u>Suppose $R = 4p_1^2p_2^2 - 1$.</u>

Then $S = 1$ and

(125) $\rightarrow c^2 + x_2^2 = d^2$,

(127) $\rightarrow p_1^2c^2 + x_2^2 = d^2$.

Hence we should have <u>either</u>

$$c = \lambda^2 - \mu^2,\ x_2 = 2\lambda\mu,\ d^2 = (\lambda^2 + \mu^2)^2,$$

<u>or</u>

$$p_1c = \lambda^2 - \mu^2,\ x_2 = 2\lambda\mu,\ d^2 = (\lambda^2 + \mu^2)^2.$$

Now from (124) & (126) we have

<u>either</u> $x_1^2 = \lambda^4 + (16p_1^2p_2^2 - 2)\lambda^2\mu^2 + \mu^4$,

<u>or</u> $p_1^2x_1^2 = \lambda^4 + (16p_1^2p_2^2 - 2)\lambda^2\mu^2 + \mu^4$.

Since $x_1 < x < z$, $p_1x_1 < p_1x < z$, we cannot have $R = 4p_1^2p_2^2 - 1$ in (124) or (126).

So we only have to consider $R = 3^t$. In this case

(124) $\rightarrow x_1^2 \equiv -3^tc^2 \pmod{p_1}$, and

(127) $\rightarrow x_2^2 \equiv 3^{-t}(4p_1^2p_2^2 - 1)d^2 \pmod{p_1}$.

Since $(-3^tc^2/p_1) = (3/p_1) = -1$, and $(3^{-t}(4p_1^2p_2^2 - 1)d^2/p_1) = (3^t/p_1) = (3/p_1) = -1$, we cannot have (124) or (127).

Thus this case is impossible.

<u>Case IIIa_2</u>

Suppose $R \equiv 5 \pmod 8$.

Then we have

$$\underline{\text{either}} \quad Rc^2 - 4p_1^2p_2^2d^2 = x_1^2, \qquad (128)$$
$$c^2 - Sd^2 = x_2^2,$$
$$\underline{\text{or}} \quad Rc^2 - 4p_2^2d^2 = x_1^2, \qquad (129)$$
$$p_1^2c^2 - Sd^2 = x_2^2.$$

The only value that R can take in this case is $2p_1p_2 - 1$.

But then both (128) & (129) would imply that

$$x_1^2 \equiv (2p_1p_2 - 1)c^2 \pmod{p_2}.$$

Since $(2p_1p_2 - 1/p_2) = (-1/p_2) = -1$, (128) & (129) are impossible.

Thus we cannot have this case.

Case IIIb

Suppose $(A, B) = 2p_1$.

Then we have

$$x^2 + (8p_1^2p_2^2 - 1)y^2 \pm z = 2Rp_1c^4,$$
$$x^2 + (8p_1^2p_2^2 - 1)y^2 \mp z = 8Sp_2^2d^4.$$

Thus $x^2 = (Rc^2 - 4p_1p_2^2d^2)(p_1c^2 - Sd^2)$.

Hence we must have

$$Rc^2 - 4p_1p_2^2d^2 = \pm x_1^2,$$
$$p_1c^2 - Sd^2 = \pm x_2^2.$$

We notice that R cannot be congruent to $\pm 1 \pmod 8$.

Case IIIb_1

Suppose $R \equiv 3 \pmod 8$.

Then we have

$$Rc^2 - 4p_1p_2^2d^2 = -x_1^2, \qquad (130)$$
$$p_1c^2 - Sd^2 = -x_2^2.$$

Since $3|R$, (130) is impossible modulo 3.

Case IIIb$_2$

Suppose $R \equiv 5 \pmod 8$.

Then we have

$$Rc^2 - 4p_1p_2^2d^2 = x_1^2, \qquad (131)$$
$$p_1c^2 - Sd^2 = x_2^2.$$

Since the only value that R can take in this case is $2p_1p_2 - 1$, (131) is impossible modulo p_2.

Case IIIc

Suppose $(A, B) = 2p_2$.

Then we have

$$Rc^2 - 4p_2p_1^2d^2 = \pm x_1^2,$$
$$p_2c^2 - Sd^2 = \pm x_2^2.$$

From the fitst equation it follows that $R \equiv 3$ or $5 \pmod 8$

Case IIIc$_1$

Suppose $R \equiv 3 \pmod 8$

Then we have

$$Rc^2 - 4p_2p_1^2d^2 = -x_1^2, \qquad (132)$$
$$p_2c^2 - Sd^2 = -x_2^2.$$

Suppose $R = 4p_1^2p_2^2 - 1$.

Then (132) would imply that

$$x_1^2 \equiv 4p_1^2p_2d^2 \pmod{2p_1p_2 + 1}$$

Since $(4p_2p_1^2d^2/2p_1p_2 + 1) = (p_2/2p_1p_2 + 1) = -1$, (132) is impossible. Thus we cannot have $R = 4p_1^2p_2^2 - 1$.

Next suppose that $R = 3^t$.

Then (132) would imply that

$$x_1^2 \equiv -3^tc^2 \pmod{p_1}.$$

Since $(-3^tc^2/p_1) = (3/p_1) = -1$, (132) is impossible.

Hence we cannot have this case.

Case IIIc_2

Suppose $R \equiv 5 \pmod 8$

Then we have

$$Rc^2 - 4p_2p_1^2d^2 = x_1^2, \qquad (133)$$
$$p_2c^2 - Sd^2 = x_2^2.$$

Since $R = 2p_1p_2 - 1$, (133) is impossible modulo p_2.

Thus we cannot have this case.

Case IIId

Suppose $(A, B) = 2p_1p_2$.

Then we have

$$Rc^2 - 4p_1p_2d^2 = \pm x_1^2,$$
$$p_1p_2c^2 - Sd^2 = \pm x_2^2.$$

Since $p_1p_2 \equiv -1$ or $3 \pmod 8$, we cannot have $R \equiv \pm 1 \pmod 8$.

Case IIId_1

Suppose $R \equiv 3 \pmod 8$.

Then

$$Rc^2 - 4p_1p_2d^2 = -x_1^2, \qquad (134)$$
$$p_1p_2c^2 - Sd^2 = -x_2^2.$$

Since $3|R$, (134) is impossible modulo 3.

Thus we cannot have this case.

Case IIId_2

Suppose $R \equiv 5 \pmod 8$.

Then we have

$$Rc^2 - 4p_1p_2d^2 = x_1^2, \qquad (135)$$
$$p_1p_2c^2 - Sd^2 = x_2^2.$$

Since the only value that R can take in this case is $2p_1p_2 - 1$, (135) would imply that

$$x_1^2 \equiv 2p_1p_2 - 1 \pmod{p_2}, \text{ which is impossible}$$

modulo p_2.

Hence we cannot have this case.

Hence the theorem.

Corollary 1.1.1:

If the equation (1) has no non-trivial solutions, then the 1^{st}, 3^{rd}, $(n + 1)^{th}$, $(n + 3)^{th}$ terms of an arithmetical progression cannot each be square.

Proof:

Suppose the 1^{st}, 3^{rd}, $(n + 1)^{th}$, $(n + 3)^{th}$ terms of an arithmetical progression are all squares. Then there exist integers a, d p, q, r, s, satisfying the following equations:

$$a = p^2,$$
$$a + 2d = q^2,$$
$$a + nd = r^2,$$
$$a + (n + 2)d = s^2.$$

Let $x^2 = a(a + 2d)$ and $y^2 = (a + nd)(a + (n + 2)d)$.

Then $x^4 + (n^2 - 2)x^2y^2 + y^4 = \{na^2 + n(n + 2)ad + n(n + 2)d^2\}^2$

$$= z^2, \text{ say.}$$

Thus we see that if the equation (1) has no non-trivial solutions, then the 1^{st}, 3^{rd}, $(n + 1)$th, $(n + 3)$th terms of an A.P cannot each be squares.

Note:

From Corollary 1.1.1, it follows that the 0^{th}, 2^{nd}, n^{th}, $(n + 2)^{th}$

terms of an A.P cannot be each square if (1) has no non-trivial solutions. So when n is even we can write $n = 2N$, and we have the following result:

If the equation $x^4 + (4N^2 - 2)x^2y^2 + y^4 = z^2$ has no non-trivial solutions, then the 0^{th}, 1^{st}, N^{th}, $(N + 1)^{th}$ $\{\to 1^{st}$, 2^{nd}, $(N + 1)^{th}$, $(N + 2)^{th}\}$ terms of an A.P cannot each be square.

We notice that the corollary by Fermat [6] is the case when $N = 2$.

Note:

In Theorem 1.4, we notice that, when $p \equiv 11$ or $23 \pmod{24}$, condition (i) could be improved as follows:

(i) $r \equiv 1 \pmod 8$, $r \neq \square$, $(r/p) = +1$.

We shall now discuss the existence of a non-trivial solution in positive integers, of the equation (1), for integer values of $n < 100$.

From Theorems 1.1 - 1.6, it follows that (1) cannot have a non-trivial solution when n = 3, 6, 7, 10, 11, 12, 13, 15, 17, 21, 23, 26, 31, 39, 40, 41, 47, 49, 59, 69, 73, 74, 86, 88, 92, 97.

We find that non-trivial solutions exist when n = 2, 5, 9, 14, 19, 20, 22, 24, 25, 27, 28, 29, 33, 34, 35, 37, 38, 43 44, 46, 53, 54, 55, 56, 58, 60, 61, 63, 65, 66, 67, 71, 75, 76, 77, 78, 79, 80, 82, 83, 85, 89, 90, 91, 95, 96, 99.

The following table gives one solution for each of the above values of n.

n	x	y	z
2	2	1	5
5	3	1	17
9	3	133	18041
14	5	1	74
19	11	1	241
20	6	1	125
22	21	1	638
24	15	1	424
25	21	1	685
27	7	1	195
28	4	1	113
29	2967	517	45295769
33	19	1	723
34	88	3	11849
35	8	1	287
37	77	3	10397
38	34	1	1733
43	976	5365	226871801
44	9	1	404
46	35	17	27386
53	8	13	5513
54	10	1	549
55	4	95	22759
56	65	1	5576
58	2	13	1517

n	x	y	z
60	55	1	4476
61	23	3	4241
63	55	1	4599
65	11	1	725
66	51	5	17026
67	1306	22631	2124341489
71	41	1	3361
75	51	1	4625
76	8	195	124489
77	12	1	935
78	40	77	240279
79	267	133	2805881
80	20	1	1649
82	29	1	2522
83	42304	91039	319725098177
85	76	1	8665
89	18040	26381	42357898889
90	13	1	1182
91	21	1	1961
95	56	1	6175
96	35	1	3576
99	56	1	6369

Pocklington [8] has proved that (1) cannot have a non-trivial solution when $n = 1, 4$. So the cases still not considered are $n = 8, 16, 18, 30, 32, 36, 42, 45, 48, 50, 51, 52, 57, 62, 64, 68, 70, 72, 81, 84, 87, 93, 94, 98, 100$. For some of these values of n, we could prove that (1) cannot have a non-trivial solution; but, we could not generalize our method in these cases.

Chapter 2

Introduction:

The four numbers 1, 3, 8, 120 have the property that the product of any two increased by 1 is a perfect square. Baker and Davenport [1] proved that no other positive integer can replace 120 while preserving the property. In fact we can find infinite number of sets of four positive integers with the above mentioned property. A set of five positive integers with this property is not known.

However, if we consider the sets of positive integers with the property that the product of any two increased by 2 is a perfect square, then we can prove that those sets can have at most three elements. In this chapter we shall prove some results concerned with the two properties mentioned.

Notation:

A set S of positive integers is said to have property $(*M)$ if $a, b \in S \rightarrow ab + M$ is a perfect square.

Lemma 2.1:

If $\{a, b\}, a \neq b$ has property $(*M)$ with $ab + M = c^2$, then $\{a, b, a + b + 2c\}$ has property $(*M)$, where a, b, c, M are positive integers.

Proof:

We have,

$$\begin{aligned} a(a + b + 2c) + M &= a^2 + 2ac + ab + M = a^2 + 2ac + c^2 \\ &= (a + c)^2 \end{aligned}$$

and

$$b(a + b + 2c) + M = (b + c)^2.$$

Hence the lemma.

Note:

In the above lemma $a + b + 2c$ can be replaced by $a + b - 2c$. But it is not necessarily a positive integer distinct from a, b.

Lemma 2.2:

Let S be a set of positive integers having property (*2). Then S can have atmost three elements.

Proof:

$a \in S \to a \not\equiv 0 \pmod 4$, since then $ab + 2 \equiv 2 \pmod 4$, which is impossible.

$a, b \in S$ and $a \equiv b \equiv 1, 2,$ or $3 \pmod 4 \to ab + 2 \equiv 2$ or $3 \pmod 4$, which is also impossible.

Since any positive integer is congruent to 0, 1, 2, or 3 modulo 4, the set S can have atmost three elements. //

Note:

The above lemma is true for any $M \equiv 2 \pmod 4$.

Corollary 2.2.1:

If $S = \{a, b, c\}$ is a set having property (*2), then without loss of generality we can assume that,

$$a \equiv 1 \pmod 4,\ b \equiv 2 \pmod 4,\ c \equiv 3 \pmod 4.$$

Theorem 2.1:

Given a positive integer a, such that 2 is a quadratic residue of a there exist a set of three elements having property (*2).

Proof:

2 is a quadratic residue of a implies that there exist x such that $2|x^2 - 2$. For one such value of x define $b = \frac{x^2 - 2}{a}$. Then $ab + 2 = x^2$.

Now, by lemma 2.1, we can find a third distinct element d (say), such that

$$ad + 2 = \text{a perfect square},$$

and $$bd + 2 = \text{a perfect square}.$$

Hence there exist a set $\{a, b, d\}$, having property (*2). //

Note that by lemma 2.2, a fourth element cannot be added to the above set.

Theorem 2.2:

There exist infinite number of sets of four positive integers having property (*1).

Proof:

For any positive integer a, consider the numbers a, $a + 2$, $4(a + 1)$, $4(a + 1)(2a + 1)(2a + 3)$.

We have,

$$a(a + 2) + 1 = (a + 1)^2,$$

$$a.4(a + 1) + 1 = (2a + 1)^2,$$

$$a.4(a + 1).4(a + 1)(2a + 1)(2a + 3) + 1 = (4a^2 + 6a + 1)^2,$$

$$a + 2.4(a + 1) + 1 = (2a + 3)^2,$$

$$a + 2.4(a + 1)(2a + 1)(2a + 3) = (4a^2 + 10a + 5)^2,$$

$4(a + 1).4(a + 1)(2a + 1)(2a + 3) + 1 = (8a^2 + 16a + 7)^2.$

Hence the set $\{a, a + 2, 4(a + 1), 4(a + 1)(2a + 1)(2a + 3)\}$ has property (*1).

The theorem follows from the fact that a is an arbitary positive integer.

Note:

For $a = 1$, we get the set $\{1, 3, 8, 120\}$

$a = 2$, we get the set $\{2, 4, 12, 420\}$.

Theorem 2.3:

A fifth integer cannot be added to the set $\{2, 4, 12, 420\}$

Proof:

Suppose there exist such an integer N. Then we can replace 420 by that integer.

Now, N must satisfy the equations,

$$2N + 1 = x^2,$$

$$4N + 1 = y^2,$$

$$12N + 1 = z^2.$$

Eliminating N from the above equations we have,

$$z^2 - 3y^2 = -2 \text{ and } z^2 - 6x^2 = -5.$$

Now, the equation $z^2 - 3y^2$ can be written in the form

$$u^2 - 3v^2 = 1, \qquad (1)$$

Where $u = z^2 + 1$, $v = zy$.

Substituting for z^2 in $z^2 - 6x^2 = -5$, we have

$$X^2 = 6u + 24 \qquad (2)$$

where $X = 6x$.

Hence to solve the equations,

$$z^2 - 3y^2 = -2, \text{ and } z^2 - 6x^2 = -5,$$

it is sufficient to solve (1), and (2) simultaneously.

Now all the positive integral solutions of (1) are given by the formula,

$$u_n \pm \sqrt{3}v_n = (2 \pm \sqrt{3})^n \tag{3}$$

(See e.g. [7]).

Hence we have

$$u_n = \frac{\alpha^n + \beta^n}{2} \quad \text{and} \quad v_n = \frac{\alpha^n - \beta^n}{2\sqrt{3}}$$

Where $\alpha = 2 + \sqrt{3}$ and $\beta = 2 - \sqrt{3}$.

So, we have,

$$\alpha + \beta = 4 \text{ and } \alpha\beta = 1.$$

Now, $$u_{-n} = \frac{\alpha^{-n} + \beta^{-n}}{2} = \frac{\alpha^n + \beta^n}{2\alpha^n\beta^n} = \frac{\alpha^n + \beta^n}{2}.$$

Hence we have,

$$u_{-n} = u_n \tag{4}$$

Now, $$v_{-n} = \frac{\alpha^{-n} - \beta^{-n}}{2\sqrt{3}} = \frac{\beta^n - \alpha^n}{2\sqrt{3}\alpha^n\beta^n} = -\frac{\alpha^n - \beta^n}{2\sqrt{3}}.$$

Hence we have,

$$v_{-n} = -v_n \tag{5}$$

Now, $$u_{m+n} = \frac{\alpha^{m+n} + \beta^{m+n}}{2}$$

$$= \frac{\alpha^m + \beta^m}{2} \cdot \frac{\alpha^n + \beta^n}{2} + 3 \cdot \frac{\alpha^m - \beta^m}{2\sqrt{3}} \cdot \frac{\alpha^n - \beta^n}{2\sqrt{3}}$$

Hence we have,

$$u_{m+n} = u_m u_n + 3v_m v_n \tag{6}$$

Now, $$v_{m+n} = \frac{\alpha^{m+n} - \beta^{m+n}}{2\sqrt{3}}$$

$$= \frac{\alpha^m + \beta^m}{2} \cdot \frac{\alpha^n - \beta^n}{2\sqrt{3}} + \frac{\alpha^n + \beta^n}{2} \cdot \frac{\alpha^m - \beta^m}{2\sqrt{3}}$$

Hence,

$$v_{m+n} = u_m v_n + u_n v_m. \tag{7}$$

Now, using (6), wehave,

$$u_{2n} = u_n u_n + 3v_n v_n = u_n^2 + 3v_n^2 = 2u_n^2 - 1.$$

Hence,

$$u_{2n} = 2u_n^2 - 1 \tag{8}$$

Now, using (7), we have,

$$v_{2n} = u_n v_n + u_n v_n = 2u_n v_n.$$

Hence,

$$v_{2n} = 2u_n v_n \tag{9}$$

Now, $$\begin{aligned} u_{3n} &= u_n u_{2n} + 3v_n v_{2n}, \text{ (Using (6))} \\ &= u_n(2u_n^2 - 1) + 3v_n \cdot 2u_n v_n \\ &= u_n(2u_n^2 - 1) + 2u_n(u_n^2 - 1) = u_n(4u_n^2 - 3) \end{aligned}$$

Hence,

$$u_{3n} = u_n \cdot f_1(u_n) \tag{10}$$

where $f_1(u_n) = 4u_n^2 - 3$.

Now, using (7), we have,

$$\begin{aligned} v_{3n} &= u_n v_{2n} + v_n u_{2n} \\ &= u_n \cdot 2u_n v_n + v_n(2u_n^2 - 1), \text{ using (8) \& (9),} \\ &= v_n(4u_n^2 - 1) \end{aligned}$$

Hence,

$$v_{3n} = v_n \cdot f_2(u_n) \tag{11}$$

where $f_2(u_n) = 4u_n^2 - 1$.

Now, $\quad u_{5n} = u_{2n}u_{3n} + 3v_{2n}v_{3n}$

$$= 2u_n^2 - 1 \;.\; u_n \cdot f_1(u_n) + 3.2u_n v_n \;\cdot\; v_n \cdot f_2(u_n)$$

$$= u_n(16u_n^4 - 20u_n^2 + 5).$$

Hence,

$$u_{5n} = u_n \cdot f_3(u_n), \tag{12}$$

where $f_3(u_n) = 16u_n^4 - 20u_n^2 + 5$.

Now, $\quad v_{5n} = u_{2n}v_{3n} + v_{2n}u_{3n}$

$$= 2u_n^2 - 1 \;.\; v_n \cdot f_2(u_n) + 2u_n v_n \;\cdot\; u_n \cdot f_1(u_n)$$

$$= v_n(16u_n^4 - 12u_n^2 + 1).$$

Hence,

$$v_{5n} = v_n \cdot f_4(u_n) \tag{13}$$

where $f_4(u_n) = 16u_n^4 - 12u_n^2 + 1$.

Now, $\quad u_{7n} = u_{2n}u_{5n} + 3v_{2n}v_{3n}$

$$= 2u_n^2 - 1 \;.\; u_n \cdot f_3(u_n) + 3.2u_n v_n \;\cdot\; v_n \cdot f_4(u_n)$$

$$= u_n(64u_n^6 - 112u_n^4 + 56u_n^2 - 7).$$

Hence,

$$u_{7n} = u_n \cdot f_5(u_n) \tag{14}$$

where $f_5(u_n) = 64u_n^6 - 112u_n^4 + 56u_n^2 - 7$.

Now, $\quad v_{7n} = u_{2n}v_{5n} + u_{5n}v_{2n}$

$$= 2u_n^2 - 1 \cdot v_n \cdot f_4(u_n) + 2u_n v_n \cdot u_n \cdot f_3(u_n)$$
$$= v_n(64u_n^6 - 80u_n^4 + 24u_n^2 - 1).$$

Hence,

$$v_{7n} = v_n \cdot f_6(u_n) \tag{15}$$

where $f_6(u_n) = 64u_n^6 - 80u_n^4 + 24u_n^2 - 1.$

Now, $u_{9n} = u_{3.3n} = u_{3n} \cdot f_1(u_{3n})$
$= u_n \cdot f_1(u_n). (64u_n^6 - 96u_n^4 + 36u_n^2 -3).$

Hence,

$$u_{9n} = u_n \cdot f_1(u_n) \cdot f_7(u_n) \tag{16}$$

where $f_7(u_n) = 64u_n^6 - 96u_n^4 + 36u_n^2 - 3.$

Now, $v_{9n} = v_{3.3n} = v_{3n} \cdot f_2(u_{3n})$
$= v_n \cdot f_2(u_n).(64u_n^6 - 96u_n^4 + 36u_n^2 - 1).$

Hence,

$$v_{9n} = v_n \cdot f_2(u_n) \cdot f_8(u_n) \tag{17}$$

where $f_8(u_n) = 64u_n^6 - 96u_n^4 + 36u_n^2 - 1.$

Now, $u_{15n} = u_{3.5n} = u_{5n} \cdot f_1(u_{5n})$

Also, $u_{15n} = u_{5.3n} = u_{3n} \cdot f_3(u_n).$

Hence we have, $u_{15n} = u_n \cdot f_1(u_n) \cdot f_3(u_n).(256u_n^8 -448u_n^6 + 224u_n^4 - 32u_n^2 + 1).$ Let $f_9(u_n) = 256u_n^8 -448u_n^6 + 224u_n^4 - 32u_n^2 + 1.$

Then we have,

$$u_{15n} = u_n \cdot f_1(u_n) \cdot f_3(u_n) \cdot f_9(u_n) \tag{18}$$

Now, $v_{15n} = v_{3.5n} = v_{3n} \cdot f_2(u\ n)$

We also have, $v_{15n} = v_{5.3n} = v_{3n} \cdot f_4(u_{3n})$.

Hence, $v_{15n} = v_n \cdot f_2(u_n) \cdot f_4(u_n) \cdot (256u_n^{\ 8} - 576u_n^{\ 6} + 416u_n^{\ 4} - 96u_n^{\ 2} + 1)$. So if we denote the last expression by $f_{10}(u_n)$, then

$$v_{15n} = v_n \cdot f_2(u_n) \cdot f_4(u_n) \cdot f_{10}(u_n) \tag{19}$$

Using (6)—(9), we have,

$$u_{n + 2r} \equiv u_n \pmod{v_r} \tag{20}$$

and

$$u_{n + 2r} \equiv -u_n \pmod{u_r} . \tag{21}$$

We have also the following table of values;

n	u_n	v_n
0	1	0
1	2	1
2	7	4
3	26	15
4	97	56
5	362	209
6	1351	780
7	5042	2911
8	18817	10864
9	70226	40545
10	262087	151316
11	978122	564719
12	3650401	2107560
13	13623482	7865521

We note that both z and y are odd and hence u is even and v is odd. Hence we have to consider only the odd values of n.

The proof is now accomplished in eleven stages:

(i) (2) is impossible if $n \equiv 3 \pmod 6$

For, $u_n \equiv 0 \pmod{13}$ and then $X^2 \equiv -2 \pmod{13}$ and since the Jacobi-Legendre symbol $(-2/13) = -1$, (2) is impossible

(ii) (2) is impossible if $n \equiv 5 \pmod{10}$.

For, using (20),
$$\begin{aligned} u_n &\equiv u_5 && \pmod{v_5} \\ &\equiv 362 && \pmod{209} \\ &\equiv -1 && \pmod{11} \end{aligned}$$

But then $X^2 \equiv 7 \pmod{11}$ and $(7/11) = -1$, and hence (2) is impossible.

(iii) (2) is impossible if $n \equiv \pm 5 \pmod{14}$.

For, using (20), we have,
$$\begin{aligned} u_n &\equiv u_{\pm 5} \pmod{v_7} \\ &\equiv u_5 \pmod{v_7}, \text{ using (4).} \end{aligned}$$

Now $71 | v_7$, $u_5 \equiv 7 \pmod{71}$ and then $X^2 \equiv -5 \pmod{71}$. Since $(-5/71) = -1$, (2) is impossible.

(iv) (2) is impossible if $n \equiv \pm 3 \pmod{20}$.

For, using (21), $u_n \equiv \pm u_{\pm 3} \equiv \pm u_3 \pmod{u_{10}}$ and then $X^2 \equiv 180$ or $-132 \pmod{7.37441}$. Now since $(180/7) = -1$ and $(-132/37441) = -1$, (2) is impossible.

(v) (2) is impossible if $n \equiv \pm 3, \pm 11, \pm 13 \pmod{28}$.

For, when $n \equiv \pm 11 \pmod{28}$, using (4) and (20) we have, $u_n \equiv u_{11} \pmod{v_{14}}$. Now, $2521 | v_{14}$ and $u_{11} \equiv -26 \pmod{2521}$. But then $X^2 \equiv -132 \pmod{2521}$ and since $(-132/2521) = -1$, this is impossible.

When $n \equiv \pm 3, \pm 13 \pmod{28}$, using (4) and (21) we have $u_n \equiv \pm u_3, \pm u_{13} \pmod{u_{14}}$. Now, $7, 337, 3079 | u_{14}$ and $u_3, u_{13} \equiv 5 \pmod 7$, $u_3 \equiv 26 \pmod{337}$ and $u_{13} \equiv 1986 \pmod{3079}$. Hence $X^2 \equiv 24 + 6u_3$, $X^2 \equiv 24 + 6u_{13}$ are impossible modulo 7, $X^2 - 6u_3$ is impossible modulo 337 and $X^2 \equiv 24 - 6u_{13}$ is impossible modulo 3079.

(vi) (2) is impossible if $n \equiv \pm 11, \pm 13 \pmod{30}$.

For, $u_n \equiv u_{11}, u_{13} \pmod{v_{15}}$. Now, $29 | v_{15}$ and $u_{11} \equiv 10 \pmod{29}$ and $u_{13} \equiv 7 \pmod{29}$. Hence $X^2 \equiv -3 \pmod{29}$ and $X^2 \equiv 8 \pmod{29}$ and since $(-3/29) = -1$, $(8/29) = -1$, both are impossible.

(vii) (2) is impossible if $n \equiv \pm 13 \pmod{42}$.

For, $u_n \equiv u_{13} \pmod{v_{21}}$ and then $X^2 \equiv 24 + 6u_{13} \pmod{v_{21}}$. Now $2017 | v_{21}$ and $X^2 \equiv 1991 \pmod{2017}$, and since $(1991/2017) = -1$, (2) is impossible.

(viii) (2) is impossible if $n \equiv \pm 21 \pmod{70}$.

For, $u_n \equiv u_{21} \pmod{v_{35}}$, and

$$v_{35} = v_{7.5} = v_5 \cdot f_6(u_5)$$
$$= 209 \cdot 2911 \cdot 9243361 \cdot 5352481$$

Now, $u_{21} = u_7(4u_7^2 - 3)$.

Hence $X^2 \equiv 24 + 6 \, . \, u_7(4u_7^2 - 3) \pmod{5352481}$

$\equiv 24 - 6 \, . \, 5042 \, . \, 10086 \pmod{5352481}$

$\equiv - 305121648 \pmod{5352481}$

Since $(-305121648/5352481) = -1$, (2) is impossible.

(ix) (2) is impossible if $n \equiv \pm 29, \pm 31 \pmod{90}$

For, $u_n \equiv u_{29}, u_{31} \pmod{v_{45}}$. Now, $83609 | v_{45}$ and

$u_{29} = 2u_{30} - 3v_{30} = 2u_{10}(4u_{10}^2 - 3) - 3v_{10}(4u_{10}^2 - 1)$

$\equiv 9253 \pmod{83609}$.

Hence $X^2 \equiv 55542 \pmod{83609}$ and since $(55542/83609)$ $= -1$, (2) is impossible.

Also $17 | v_{45}$ and $u_{31} = 2u_{30} + 3v_{30} \equiv 5 \pmod{17}$. and hence $X^2 \equiv 3 \pmod{17}$. Since $(3/17) = -1$, (2) is impossible.

(x) (2) is impossible if $n \equiv \pm 1 \pmod{252}$, $n \neq \pm 1$.

For, we can write $n = \pm 1 + 63k(2l + 1)$ where l is an integer, and $k = 2^t$, $t \geq 2$. Then,

$$u_n \equiv \pm u_{\pm 1 + 63k} \equiv \pm 3v_{63k} \pmod{u_{63k}}.$$

Now, $v_{63k} = v_{9 \, . \, 7k} \equiv v_{7k} \pmod{u_{7k}}$

$\equiv v_k \, (32 u_k^4 - 32 u_k^2 + 6) \pmod{f_5(u_k)}$.

Also, $v_{63k} = v_{7.9k} \equiv - v_{9k} \pmod{u_{9k}}$

$\equiv - 2v_k(4u_k^2 - 1) \pmod{f_7(u_k)}$

Hence $X^2 \equiv 24 \pm 18v_k(32u_k^4 - 32u_k^2 + 6) \pmod{f_5(u_k)}$

$\equiv 24 \mp 36v_k(4u_k^2 - 1) \pmod{f_7(u_k)}$.

First consider $X^2 \equiv 24 \pm 18v_k \, (32 u_k^4 - 32u_k^2 + 6) \pmod{f_5(u_k)}$.

Now, $\left(\dfrac{24 + 18v_k(32u_k^4 - 32u_k^2 + 6)}{f_5(u_k)}\right)$

$$= \left(\frac{24 + 18v_k(288v_k^4 + 96v_k^2 + 6)}{1728v_k^6 + 720v_k^4 + 72v_k^2 + 1}\right)$$

$$= \left(\frac{144v_k^4 + 36v_k^2 - 8v_k^2 + 1}{\frac{1}{2}(432v_k^5 + 144v_k^3 + 9v_k + 2)}\right)$$

$$= \left(\frac{36v_k^3 + 24v_k^2 + 6v_k + 2}{144v_k^4 + 36v_k^2 - 8v_k + 1}\right)$$

$$= \left(\frac{3}{\frac{1}{2}(36v_k^3 + 24v_k^2 + 6v_k + 2)}\right)\left(\frac{228v_k^2 + 19}{\frac{1}{2}(36v_k^3 + 24v_k^2 + 6v_k + 2}\right)$$

$$= (-)\left(\frac{36v_k^3 + 24v_k^2 + 6v_k + 2}{19}\right)$$

Similarly, we have,

$$\left(\frac{24 - 18v_k(32u_k^4 - 32u_k^2 + 6)}{f_5(u_k)}\right) = \left(\frac{36v_k^3 - 24v_k^2 + 6v_k - 2}{19}\right)$$

Next consider $X^2 \equiv 24 \mp 36v_k(4u_k^2 - 1) \pmod{f_7(u_k)}$

Now, $\left(\dfrac{24 - 36v_k(4u_k^2 - 1)}{f_7(u_k)}\right) = \left(\dfrac{24 - 36v_k(12v_k^2 + 3)}{1728v_k^6 + 864v_k^4 + 108v_k^2 + 1}\right)$

$$= \left(\frac{1728v_k^6 + 864v_k^4 + 108v_k^2 + 1}{\frac{1}{2}(36v_k^3 + 9v_k - 2)}\right)$$

$$= \left(\frac{96v_k^3 + 24v_k + 1}{\frac{1}{2}(36v_k^3 + 9v_k - 2)}\right)$$

$$= \left(\frac{36v_k^3 + 9v_k - 2}{19}\right)$$

Similarly, we have,

$$\left(\frac{24 + 36v_k(4u_k^2 - 1)}{f_7(u_k)}\right) = (-)\left(\frac{36v_k^3 + 9v_k + 2}{19}\right)$$

The residues of v_k, $36v_k^3 \pm 24v_k^2 \pm 6v_k + 2$ and $36v_k^3 + 9v_k \pm 2$ modulo 19 are periodic and the length of the period is 4. The following table gives these residues and the signs of

$(24 \pm 18v_k(32u_k^4 - 32u_k^2 + 6)/f_5(u_k))$ and

$(24 \mp 36v_k(4u_k^2 - 1)/f_7(u_k))$.

$k = t$	$t = 2$	3	4	5	6
v_k (mod 19)	-1	-4	1	4	-1
$36v_k^3 + 24v_k^2 + 6v_k + 2$ (mod 19)	3	-4	-8	-3	
$36v_k^3 - 24v_k^2 + 6v_k - 2$ (mod 19)	8	3	-3	4	
$36v_k^3 + 9v_k + 2$ (mod 19)	-5	-1	9	5	
$36v_k^3 + 9v_k - 2$ (mod 19)	-9	-5	5	1	
$24 + 18v_k(32u_k^4 - 32u_k^2 + 6)\|f_5(u_k))$	+1	+1	-1	-1	
$(24 - 36v_k(4u_k^2 - 1)\|f_7(u_k))$	-1	-1	+1	+1	
$(24 - 18v_k(32u_k^4 - 32u_k^2 + 6)\|f_5(u_k))$	-1	-1	+1	+1	
$(24 + 36v_k(4u_k^2 - 1)\|f_7(u_k))$	+1	+1	-1	-1	

From the above table, we see that the congruences

$$X^2 \equiv 24 + 18v_k(32u_k^4 - 32u_k^2 + 6) \pmod{f_5(u_k)}$$

and $X^2 \equiv 24 - 36v_k(4u_k^2 - 1) \pmod{f_7(u_k)}$

cannot hold simultaneously and the congruences

$$X^2 \equiv 24 \div 18v_k(32u_k^{\ 4} - 32u_k^{\ 2} + 6) \pmod{f_5(u_k)},$$

and $X^2 \equiv 24 + 36v_k(4u_k^{\ 2} - 1) \pmod{f_7(u_k)}$

cannot hold simultaneously.

Hence (2) is impossible.

(xi) (2) is impossible if $n \equiv \pm 7 \pmod{60}$; $n \neq \pm 7$.

For, we can write $n = \pm 7 + 2.15kl$ where $k = 2^t$, $t \geqq 1$ and l is an odd integer.

Then by applying (21), l times we have,

$$u_n \equiv -u_7 \pmod{u_{15k}}$$
$$\equiv -5042 \pmod{u_k \cdot f_1(u_k).f_3(u_k).f_9(u_k)}$$

Hence $X^2 \equiv 24 - 6.5042 \equiv -30228 \pmod{u_k \cdot f_1(u_k).f_3(u_k).f_9(u_k)}$.

Note that when $t = 1$, $u_n \equiv -2 \pmod 7$ and then $X^2 \equiv 5 \pmod 7$ and $(5/7) = -1$.

When $t \geqq 2$, we have,

$$(-30228/u_k) = (u_k/11)\,(u_k/229) = (-)\,(u_k/229) \text{ when } u_k \equiv -4 \pmod{11},$$
$$= (u_k/229) \text{ when } u_k \equiv -2 \pmod{11},$$

$$(-30228/f_1(u_k)) = (-)\,(f_1(u_k)/229),$$
$$(-30228/f_3(u_k)) = (-)\,(f_3(u_k)/229), \text{ when } u_k \equiv -4 \pmod{11},$$
$$= (f_3(u_k)/229), \quad \text{when } u_k \equiv -2 \pmod{11},$$
$$(-30228/f_9(u_k)) = (-)\,(f_9(u_k)/229).$$

The residues of u_k, $f_1(u_k)$, $f_3(u_k)$, and $f_9(u_k)$ modulo 229 are periodic and the lenth of the period is 9. The following table gives the values of these residues and the signs of $(-30228/u_k)$, $(-30228/f_1(u_k))$, $(-30228/f_3(u_k))$, & $(-30228/f_5(u_k))$.

$k = 2^t$	$t = 2$	3	4	5	6	7	8	9	10
$u_k \pmod{229}$	97	39	64	-53	121	-31	89	40	-7
$f_1(u_k) \pmod{229}$	77	127	122	12	-63	177	79	-15	193
$f_3(u_k) \pmod{229}$	51	-4	-109		12	132	-93		
$f_9(u_k) \pmod{229}$	103				159		58		
	when $u_k \equiv -4 \pmod{11}$								
$(-30228/u_k)$	-1	+1	-1	-1	-1	+1	+1	+1	+1
$(-30228/f_1(u_k))$		+1				+1	+1	-1	-1
$(-30228/f_3(u_k))$		-1				-1	+1		
$(-30228/f_9(u_k))$							-1		
	when $u_k \equiv -2 \pmod{11}$								
$(-30228/u_k)$	+1	-1	+1	+1	+1	-1	-1	-1	-1
$(-30228/f_1(u_k))$	+1		+1	-1	+1				
$(-30228/f_3(u_k))$	+1		-1		+1				
$(-30228/f_9(u_k))$	-1				-1				

Hence (2) is impossible.

Since, from (i), (ii) and (vi) we have (2) is impossible when $n \equiv 3 \pmod 6$, $5 \pmod{10}$, ± 11, $\pm 13 \pmod{30}$, it follows that (2) is impossible for all values of n except when $n \not\equiv \pm 1, \pm 7 \pmod{30}$ From (iv), we have (2) is impossible when $n \equiv \pm 3 \pmod{20}$. Hence we have (2) is impossible for all values of n except when $n \not\equiv \pm 1, \pm 7$,

$\pm 29 \pmod{60}$.

Now, from (xi) we have (2) is impossible when $n \equiv \pm 7 \pmod{60}, n \neq \pm 7$.

Hence (2) is impossible for all values of n except when $n = 7$ and $n \equiv \pm 1, \pm 29 \pmod{60}$.

Now, from (iii) and (v) it follows that (2) is impossible for all values of n except when $n \equiv \pm 1, \pm 7 \pmod{28}$

Combining the last two statements, we have (2) is impossible for all values of n except when $n = 7$ and $n \equiv \pm 1, \pm 29, \pm 91, \pm 119 \pmod{420}$.

From (vii) and (viii) we have, (2) is impossible when $n \equiv \pm 13 \pmod{42}$, $n \equiv \pm 21 \pmod{70}$.

So we cannot have $n \equiv \pm 29, \pm 91, \pm 119 \pmod{420}$.

Hence (2) is impossible for all values of n except when $n = 7$ and $n \equiv \pm 1 \pmod{420}$; That is when $n = 7$, $n \equiv \pm 1, \pm 421, \pm 419 \pmod{1260}$.

Now, since from (ix) and (x) we have, (2) is impossible when $n \equiv \pm 29$, $\pm 31 \pmod{90}$, $\pm 1 \pmod{252}$, $n \neq \pm 1$, we can conclude that (2) is impossible for all values of n except when $n = \pm 1, \pm 7$.

Summarising the results, we see that (1) and (2) can hold for n odd, only for $n = \pm 1$ and $n = \pm 7$ and these values do indeed satisfy with $u = 2$, $v = 1$, $x = 1$ and $u = 5042$, $v = 2911$, $x = 29$.

$x = 1$ give the trivial solution $N = 0$ and $x = 29$ give the solution $N = 420$.

Hence no other positive integer can replace 420 in the set $\{2, 4, 12, 420\}$. In other words a fifth integer cannot be added to the set $\{2, 4, 12, 420\}$. //

Theorem 2.4:

Given a set S of three positive integers, having property (*1), there exist an algebraic formula which gives a fourth element of the set.

Proof:

Soppose $x_1, x_2, x_3 \varepsilon S$.

If another positive integer x distinct from $x_1, x_2, x_3 \varepsilon S$, then x must satisfy the following equations:

$$xx_1 + 1 = a^2$$
$$xx_2 + 1 = b^2$$
$$xx_3 + 1 = c^2.$$

Eliminating x from the first two equations, we have,

$$x_2a^2 - x_1b^2 = x_2 - x_1.$$

i.e $$(x_2a)^2 - x_1x_2b^2 = x_2^{\ 2} - x_1x_2 \ .$$

Now, one solution of this equation is $x = x_3$,

$$a = (x_1x_3 + 1)^{\frac{1}{2}},\ b = (x_2x_3 + 1)^{\frac{1}{2}}.$$

Hence a class of solution is given by,

$$x_2a + (x_1x_2)^{\frac{1}{2}}b = (x_2(x_1x_3 + 1)^{\frac{1}{2}} + (x_1x_2)^{\frac{1}{2}}(x_2x_3 + 1)^{\frac{1}{2}}\varepsilon$$

where ε is any unit in $Q(x_1x_2)^{\frac{1}{2}}$.

The fundermental unit is $(x_1x_2 + 1)^{\frac{1}{2}} + (x_1x_2)^{\frac{1}{2}}$.

Try the solution

$$x_2a + (x_1x_2)^{\frac{1}{2}}b = (x_2(x_1x_3+ 1)^{\frac{1}{2}} + (x_1x_2)^{\frac{1}{2}}(x_2x_3 + 1)^{\frac{1}{2}})$$
$$((x_1x_2 + 1)^{\frac{1}{2}} +(x_1x_2)^{\frac{1}{2}})$$

i.e $$x_2a = x_2(x_1x_3 + 1)^{\frac{1}{2}}(x_1x_2+ 1)^{\frac{1}{2}} + x_1x_2(x_2x_3 + 1)^{\frac{1}{2}}$$

Hence, $$a = (x_1x_3 + 1)^{\frac{1}{2}}\ (x_1x_2 + 1)^{\frac{1}{2}} + x_1(x_2x_3 + 1)^{\frac{1}{2}}$$

So, $$x = \frac{a^2 - 1}{x_1} = 2x_1x_2x_3 + x_1 + x_2 + x_3 + 2(x_1x_2 + 1)^{\frac{1}{2}}$$
$$(x_1x_3 + 1)^{\frac{1}{2}}(x_2x_3 + 1)^{\frac{1}{2}}.$$

This x satisfies the first two equations and by symmetry it will also satisfy the third equation. //

Chapter 3

Introduction:

The only positive integer solutions of the equation

$$(X(X-1))^2 = 2Y(Y-1)$$

are $(X,Y) = (1,1),(2,2),(4,9)$. A complicated proof was given by Ljunggren [5] depending upon the p-adic methods applied to a quartic field and a simple method was given by Cassels [2] depending upon the properties of the quartic field $Q(\sqrt[4]{2})$. In this chapter we shall discuss the positive integer solutions of the equation

$$(X(X-1))^2 = 3Y(Y-1).$$

Our method is based on the ideas used by Cohn [3].

Theorem:

The only positive integer solutions of the equation

$$(X(X-1))^2 = 3Y(Y-1)$$

are $(X,Y) = (1,1),\ (3,4)$.

Proof:

Substituting $x = 2X - 1$, $y = 2Y - 1$ in the above equation we have,

$$\left(\frac{x+1}{2}\cdot\frac{x-1}{2}\right)^2 = 3.\left(\frac{y+1}{2}\right).\left(\frac{y-1}{2}\right)$$

i.e $$\left(\frac{x^2-1}{4}\right)^2 = 3\left(\frac{y^2-1}{4}\right)$$

i.e $$y^2 - \left(\frac{x^2-1}{6}\right)^2 = 1$$

This is of the form $u^2 - 3v^2 = 1$, where $u = y$ and $v = \dfrac{x^2-1}{6}$.

Hence we must have,

$$x^2 = 1 + 6v \tag{22}$$

We have already discussed the integral solutions of the equation $u^2 - 3v^2 = 1$ in chapter 2. In this chapter we shall assume the results that we have derived in chapter 2.

Using the equations (6) - (9), we have,

$$v_{n+2r} \equiv v_n \pmod{v_r} \tag{23}$$

$$v_{n+2r} \equiv -v_n \pmod{u_r} \tag{24}$$

We note that y is odd and hence u is odd. Thus we have to consider only the even values of n.

The proof is now accomplised in six stages:

(i) (22) is impossible if $n \equiv \pm 4 \pmod{10}$

For,

$$\begin{aligned} v_n &\equiv v_{\pm 4} \pmod{v_5}, \text{ using (23)}, \\ &\equiv \pm v_4 \pmod{v_5}, \text{ using (5)}, \\ &\equiv \pm 56 \pmod{209}; \end{aligned}$$

whence $v_n \equiv \pm 1 \pmod{11}$. Then $x^2 = 1 + 6v_n \equiv 7$ or $-5 \pmod{11}$, and since the Jacobi-Legendre symbol $(7/11) = -1$, $(-5/11) = -1$, (22) is impossible.

(ii) (22) is impossible if $n \equiv 8 \pmod{10}$

For,

$$\begin{aligned} v_n \equiv v_8 &\equiv v_{-2} \pmod{v_5}, \\ &\equiv -4 \pmod{209}. \end{aligned}$$

However, then $1 + 6v_n \equiv -1 \pmod{11}$ and since $(-1/11) = -1$, (22) is impossible.

(iii) (22) is impossible if $n \equiv 12 \pmod{20}$.

For,

$$v_n \equiv v_{12} \equiv v_{-8} \pmod{v_{10}}$$

i.e $\qquad v_n \equiv -10864 \pmod{151316}$.

Now, $181 | 151316$ and $1 + 6v_n \equiv -23 \pmod{181}$. Since $(-23/181)$ $= -1$, (22) is impossible.

(iv) (22) is impossible if $n \equiv 10 \pmod{20}$.

For,

$$v_n \equiv \pm v_{10} \pmod{u_{10}}, \text{ using (24)},$$
$$\equiv \pm 151316 \pmod{262087}.$$

Hence, $x^2 \equiv 1 \pm 6.151316 \pmod{7.37441}$. That is either $x^2 \equiv 90$ 907897 or $x^2 \equiv -907895 \pmod{7.37441}$. Since $(907897/37441)$ and $(-907895/7) = -1$, (22) is impossible.

(v) (22) is impossible if $n \equiv 0 \pmod{20}$, $n \neq 0$.

For, if $n \neq 0$, we may write,

$$n = 5.2^t\,(2l + 1)$$

where l is an integer, odd or even, and $t \geq 2$.

i.e $\qquad n = 5k + 2.5k.l$, where $k = 2^t$.

Then by using (24) l times, we obtain,

$$v_n \equiv \pm v_{5k} \pmod{u_{5k}}$$
$$\text{i.e, } v_n \equiv \pm v_k(16u_k^4 - 12u_k^2 + 1) \pmod{u_k(16u_k^4 - 20u_k^2 + 5)}$$
$$\equiv \pm v_k(8u_k^2 - 4) \pmod{16u_k^4 - 20u_k^2 + 5}$$
$$\equiv \pm v_k(24v_k^2 + 4) \pmod{144v_k^4 + 36v_k^2 + 1}$$

Hence $x^2 \equiv 1 \pm 6v_k\,(24v_k^2 + 4) \pmod{144v_k^4 + 36v_k^2 + 1}$

First consider

$$x^2 \equiv 1 + 6v_k(24v_k^2 + 4) \pmod{144v_k^4 + 36v_k^2 + 1}$$

Now,
$$\left(\frac{1 + 6v_k(24v_k^2 + 4)}{144v_k^4 + 36v_k^2 + 1}\right) = \left(\frac{12v_k^2 - v_k + 1}{144v_k^3 + 24v_k + 1}\right)$$

$$= \left(\frac{12v_k^2 + 12v_k + 1}{12v_k^2 - v_k + 1}\right)$$

$$= \left(\frac{13v_k}{12v_k^2 - v_k + 1}\right)$$

$$= \left(\frac{12v_k^2 - v_k + 1}{13}\right)$$

Similarly, we have,

$$\left(\frac{1 - 6v_k(24v_k^2 + 4)}{144v_k^4 + 36v_k^2 + 1}\right) = \left(\frac{12v_k^2 + v_k + 1}{13}\right)$$

Hence, $\left(\dfrac{1 \pm 6v_k(24v_k^2 + 4)}{144v_k^4 + 36v_k^2 + 1}\right) = \left(\dfrac{12v_k^2 \mp v_k + 1}{13}\right)$

Now, $v_k \equiv \pm 4 \pmod{13}$ and hence,

$$\left(\frac{12v_k^2 \mp v_k + 1}{13}\right) = -1.$$

Hence (22)is impossible.

(vi) (22) is impossible if $n \equiv 2 \pmod{20}$, $n \neq 2$.

For, we can write,

$$n = 2 + 2k.5l$$

where $k = 2^t$, $t \geqslant 1$, and l is an integer.

Using (24) l times, we obtain,

$$v_n \equiv - v_2 \pmod{u_{5k}}$$

$$\equiv - 4 \text{ (mod } u_k(16u_k^4 - 20u_k^2 + 5)$$

Hence, $x^2 \equiv - 23 \pmod{u_k(16u_k^4 - 20u_k^2 + 5)}$.

Now, $(- 23/u_k) = (u_k/23)$ and

$$(-23/16u_k^4 - 20u_k^2 + 5) = (16u_k^4 - 20u_k^2 + 5/23).$$

The residues of u_k, $16u_k^4 - 20u_k^2 + 5$ modulo 23 are peridoic and the length of the period is 5. The following table gives these residues and the signs of $(u_k/23)$ and $(16u_k^4 - 20u_k^2 + 5/23)$.

$k = 2^t$	u_k (mod 23)	$(u_k/23)$	$f_3(u_k)$ (mod 23)	$(f_3(u_k)/23)$
$t = 1$	7	-1		
$= 2$	5	-1		
$= 3$	3	+1	-6	-1
$= 4$	-6	-1		
$= 5$	2	+1	-3	-1
$= 6$	7			

From the above table we see that the congruences $x^2 \equiv -23 \pmod{u_k}$ and $x^2 \equiv -23 \pmod{f_3(u_k)}$ cannot hold simultaneously and hence (22) is impossible.

Summarising the results, we see that (22) can hold for n even, only for $n = 0$ & $n = 2$ and these values do indeed satisfy with $u = 1$, $v = 0$, $x = 1$, $y = 1$ and $u = 7$, $v = 4$, $x = 5$, $y = 7$. $x = 1$, $y = 1$ give the solution $(X,Y) = (1,1)$ and $x = 5$, $y = 7$ give the solution $(X,Y) = (3,4)$. //

Chapter 4

Introduction:

Cohn [3] has proved that the only solution in positive integers of the equation,

$$Y(Y + 1)(Y + 2)(Y + 3) = 2X(X + 1)(X + 2)(X + 3)$$

is $(X,Y) = (4,5)$.

Our aim in this chapter is to prove that the only solution in positive integers of the equation,

$$3Y(Y + 1) = X(X + 1)(X + 2)(X + 3)$$

is $(X,Y) = (12,104)$.

Proof:

To prove the result, we put $y = 2Y + 1$, and $x = 2X + 3$ which gives the equation,

$$3(y^2 - 1) = \left(\frac{x^2 - 5}{2}\right)^2 - 4.$$

This is of the form

$$u^2 - 3v^2 = 1$$

where $u = \dfrac{x^2 - 5}{2}$, $v = y$.

Hence we must have,

$$x^2 = 5 + 2u. \tag{25}$$

We have already discussed the positive integral solutions of the equation $u^2 - 3v^2 = 1$ in chapter 2. In addition to the equations derived in chapter 2, we also need the following equations:

$$u_{11n} = u_{n + 10n} = u_n u_{10n} + 3v_n v_{10n}$$

$$= u_n(2u_{5n}^2 - 1) + 3v_n \cdot u_{5n}v_{5n}$$

$$= u_n(2u_{5n}^2 - 1) + 3v_n . 2u_{5n}v_{5n}$$
$$= u_n(2u_{5n}^2 - 1) + 3v_n^2 . 2u_{5n}f_4(u_n)$$
$$= u_n(2u_{5n}^2 - 1) + u_n(u_n^2 - 1) . 2f_3(u_n) . f_4(u_n)$$
$$= u_n . f_{11}(u_n) \qquad (26)$$

where $f_{11}(u_n) = 1024u_n^{10} - 2816u_n^8 + 2816u_n^6 - 1232u_n^4 + 220u_n^2 - 11.$

$$u_{33n} = u_{3.11n} = u_{11n}(4u_{11n}^2 - 3)$$
$$= u_{11n} . f_{12}(u_n) \qquad (27)$$

where $f_{12}(u_n) = 4u_{11n}^2 - 3$

We note that both x and y are odd and hence v is odd. Hence we have to consider only the odd values of n. The proof is now accomplished in ten stages:

(i) (25) is impossible if $n \equiv 3 \pmod 6$.

For, using (20), we find that for such n,

$$u_n \equiv u_3 (\mathrm{mod}\ v_3)$$
$$\equiv 26 \pmod{15}$$

But then $x^2 \equiv 2 \pmod 5$, and since the Jacobi-Legendre $(2/5) = -1$, (25) is impossible.

(ii) (25) is impossible if $n \equiv \pm 3 \pmod{10}$.

For,

$$u_n \equiv u_{\pm 3} (\mathrm{mod}\ v_5)$$
$$\equiv u_3 (\mathrm{mod}\ v_5), \text{ using } (4),$$
$$\equiv 26 \pmod{209},$$

whence $u_n \equiv 4 \pmod{11}$, and then $x^2 \equiv 2 \pmod{11}$, and since $(2/11) = -1$, (25) is impossible.

(iii) (25) is impossible if $n \equiv \pm 3, \pm 7, \pm 9, 11 \pmod{22}$.

For,

$$u_n \equiv u_{\pm 3}, u_{\pm 7}, u_{\pm 9}, u_{11} \pmod{v_{11}}$$
$$\equiv u_3, u_7, u_9, u_{11} \pmod{564719}$$
$$\equiv 3, 5, 7, 1 \pmod{23}$$

But then $x^2 \equiv 11, 15, 19, 7 \pmod{23}$, and since $(11/23) = -1$, $(15/23) = -1$, $(19/23) = -1$, $(7/23) = -1$, (25) is impossible.

(iv) (25) is impossible if $n \equiv \pm 11 \pmod{30}$.

For,

$$u_n \equiv u_{\pm 11} \pmod{v_{15}}$$
$$\equiv 978122 \pmod{v_{15}}.$$

Now, using (10), we have, $v_{15} = v_5(2u_5 - 1)(2u_5 + 1)$ and since $2u_5 - 1 = 723$, $241 | v_{15}$. Then $x^2 \equiv 52 \pmod{241}$ and since, $(52/241) = -1$, (25) is impossible.

(v) (25) is impossible if $n \equiv \pm 17 \pmod{44}$.

For, using (21), we have,

$$u_n \equiv -u_{\pm 5} \pmod{u_{11}}$$
$$\equiv -362 \pmod{489061}.$$

Then, $x^2 \equiv -719 \pmod{489061}$, and since $(-719 | 489061) = -1$, (25) is impossible.

(vi) (25) is impossible if $n \equiv \pm 29 \pmod{60}$.

For,

$$u_{\pm 29} = u_{29} = 2u_{30} - 3v_{30} \equiv -3v_{30} \pmod{u_{30}},$$

$$u_n \equiv \pm\, u_{29} \pmod{u_{30}},$$
$$\equiv \mp\, 3v_{30} \pmod{u_{30}}\ ,$$

and hence $x^2 \equiv 5 \mp 6v_{30} \pmod{u_{30}}$.

Now, $u_{30} = u_{10}(4u_{10}^2 - 3)$ and $4u_{10}^2 - 3 = 274758382273$

$= 193.1201.1185361$, and

$v_{30} = v_{10}(4u_{10}^2 - 1) \equiv -20 \pmod{1201}$, $302632 \pmod{1185361}$.

Hence ,

either $x^2 \equiv -\, 115 \pmod{1201}$

or $\quad x^2 \equiv -\, 630426 \pmod{1185361}$.

Since $(-\, 115/1201) = -1$, and $(-\, 630426/1185361) = -1$,

(25) is impossible.

(vii) (25) is impossible if $n \equiv \pm\, 23 \pmod{66}$.

For,

$$u_n \equiv u_{\pm 23} \equiv u_{23} \pmod{v_{33}}$$

Now, since $v_{33} = v_{11}(2u_{11} - 1)(2u_{11} + 1)$ and $2u_{11} + 1 =$

1956245, we have $391249 | v_{33}$.

Also, $u_{23} = 2u_{24} - 3v_{24}$

$$= 2(2u_{12}^2 - 1) - 3.2u_{12}v_{12}$$
$$\equiv -\, 129162 \pmod{391249}.$$

Hence $x^2 \equiv -\, 258319 \pmod{391249}$ and since $(-258319/$

$391249) = -1$, (25) is impossible.

(viii) (25) is impossible if $n \equiv \pm\, 65 \pmod{132}$.

For,

$$u_n \equiv \pm\, u_{\pm 65} \equiv \pm u_{65} \pmod{u_{66}}$$

Now, $u_{65} = u_{66}u_{-1} + 3v_{66}v_{-1}$

$$\equiv -3v_{66} \pmod{u_{66}}$$

Hence $u_n \equiv \mp 3v_{66} \pmod{u_{66}}$ and

$$x^2 \equiv 5 \mp 6v_{66} \pmod{u_{66}}$$

$$\equiv 5 \mp 6v_{22}(4u_{22}^2 - 1) \pmod{4u_{22}^2 - 3}$$

$$\equiv 5 \mp 12v_{22} \pmod{4u_{22}^2 - 3}$$

Now,

$$\left(\frac{5 \mp 12v_{22}}{4u_{22}^2 - 3}\right) = \left(\frac{5 \mp 12v_{22}}{12v_{22}^2 + 1}\right)$$

$$= \left(\frac{12v_{22}^2 + 1}{12v_{22} \mp 5}\right)$$

$$= \left(\frac{1 \pm 5v_{22}}{12v_{22} \mp 5}\right)$$

$$= \left(\frac{12v_{22} \mp 5}{5v_{22} \pm 1}\right)$$

$$= \left(\frac{5}{5v_{22} \pm 1}\right)\left(\frac{60v_{22} \mp 25}{5v_{22} \pm 1}\right)$$

$$= \left(\frac{\mp 37}{5v_{22} \pm 1}\right)$$

$$= \left(\frac{5v_{22} \pm 1}{37}\right)$$

Now, $v_{22} = 2u_{11}v_{11} \equiv 2.27.25 \equiv 18 \pmod{37}$ and hence

$$\left(\frac{5v_{22} \pm 1}{37}\right) = (91/37) \text{ or } (89/37).$$

Since $(91/37)$ and $(89/37) = -1$, (25) is impossible.

(ix) (25) is impossible if $n \equiv \pm$ (mod 12), $n \neq \pm 1$.

For, if $n \neq \pm 1$, we may write,

$$n = \pm 1 + 3k + 6kl,$$

where $k = 2^t$, $t \geqslant 2$ and l is an integer. Then using (21) we have

$$u_n \equiv \pm u_{3k+1} \pmod{u_{3k}}$$

$$\text{i.e } u_n \equiv \pm 3v_{3k} \pmod{u_k(1 + 12v_k^2)}$$

$$\equiv \pm 3v_k(4u_k^2 - 1) \pmod{u_k(1 + 12v_k^2)}$$

Hence $x^2 = 5 + 2u_n \equiv 5 \pm 6v_k(4u_k^2 - 1) \pmod{u_k(1 + 12v_k^2)}$

which implies that

$$x^2 = 5 + 2u_n \equiv 5 \mp 6v_k \pmod{u_k}$$

and

$$x^2 \equiv 5 \pm 12v_k \pmod{(1 + 12v_k^2)}$$

First consider $x^2 = 5 - 6v_k \pmod{u_k}$. Let $k = 2s$.

$$\left(\frac{5 - 6v_k}{u_k}\right) = \left(\frac{5 - 6v_{2s}}{u_{2s}}\right) = \left(\frac{5(u_s^2 - 3v_s^2) - 12u_sv_s}{u_s^2 + 3v_s^2}\right)$$

$$= \left(\frac{10u_s^2 - 12u_sv_s}{u_s^2 + 3v_s^2}\right)$$

$$= \left(\frac{2}{u_{2s}}\right)\left(\frac{u_s}{u_s^2 + 3v_s^2}\right)\left(\frac{5u_s - 6v_s}{u_s^2 + 3v_s^2}\right)$$

Now $\left(\frac{2}{u_{2s}}\right) = \left(\frac{2}{2u_s^2 - 1}\right) = +1$,

$$\left(\frac{u_s}{u_s^2 + 3v_s^2}\right) = \left(\frac{u_s^2 + 3v_s^2}{u_s}\right) = \left(\frac{3}{u_s}\right) = \left(\frac{1}{3}\right) = +1,$$

$$\left(\frac{5u_s - 6v_s}{u_s^2 + 3v_s^2}\right) = \left(\frac{u_s^2 + 3v_s^2}{5u_s - 6v_s}\right) = \left(\frac{111v_s^2}{5u_s - 6v_s}\right)$$

$$= \left(\frac{3}{5u_s - 6v_s}\right)\left(\frac{37}{5u_s - 6v_s}\right)$$

$$= \left(\frac{5u_s - 6v_s}{3}\right)\left(\frac{5u_s - 6v_s}{37}\right)$$

$$= \left(\frac{2}{3}\right)\left(\frac{5u_s - 6v_s}{37}\right) = (-)\left(\frac{5u_s - 6v_s}{37}\right)$$

Hence $\left(\frac{5 - 6v_k}{u_k}\right) = (-)\left(\frac{5u_{k/2} - 6v_{k/2}}{37}\right)$

$$\left(\frac{5 - 6v_k}{u_k}\right)\left(\frac{5 + 6v_k}{u_k}\right) = \left(\frac{25 - 36v_k^2}{u_k}\right)$$

$$= \left(\frac{25 - 12(u_k^2 - 1)}{u_k}\right)$$

$$= \left(\frac{37}{u_k}\right) = \left(\frac{u_k}{37}\right).$$

Next consider $x^2 \equiv 5 \pm 12v_k \pmod{(1 + 12v_k^2)}$

$$\left(\frac{5 \pm 12v_k}{1 + 12v_k^2}\right) = \left(\frac{\pm 5 + 12v_k}{1 + 12v_k^2}\right) = \left(\frac{12v_k^2 + 1}{12v_k \pm 5}\right)$$

$$= \left(\frac{12}{12v_k \pm 5}\right)\left(\frac{(12^2v_k^2 - 5^2) + 37}{12v_k \pm 5}\right)$$

$$= \left(\frac{3}{12v_k \pm 5}\right)\left(\frac{37}{12v_k \pm 5}\right)$$

$$= -\left(\frac{12v_k \pm 5}{37}\right).$$

The residues of u_k, v_k, $5u_k - 6v_k$, $5 \pm 12v_k$, modulo 37 are periodic and the length of the period is 6. The following table gives these residues and the signs of the Legendre symbols $(5 + 6v_k/u_k)$, $(5 - 12v_k/1 + 12v_k^2)$ $(5 - 6v_k/u_k)$ and $(5 + 12v_k/1 + 12v_k^2)$.

$k = 2^t$	$t = 2$	3	4	5	6	7	8
u_k (mod 37)	-14	21	-7	-14	21	-7	-14
v_k (mod 37)	-18	-14	4	18	14	-4	-18
$5u_k - 6v_k$(mod 37)	1	4	-22	7	21	-11	1
$12v_k - 5$ (mod 37)	1	12	6	-11	15	-16	1
$5 + 12v_k$ (mod 37)	11	-15	16	-1	-12	-6	11
$(5 + 6v_k/u_k)$	+1	-1	-1	+1	-1	-1	+1
$(5 - 12v_k/1 + 12v_k^2)$	-1	-1	+1	-1	+1	-1	-1
$(5 - 6v_k/u_k)$	-1	-1	-1	+1	-1	-1	-1
$(5 + 12v_k/1 + 12v_k^2)$	-1	+1	-1	-1	-1	+1	-1

From the above table we see that the congruences $x^2 \equiv 5 - 6v_k \pmod{u_k}$ and $x^2 \equiv 5 + 12v_k \pmod{(1 + 12v_k^2)}$ cannot hold simultanaously and the congruences $x^2 \equiv 5 + 6v_k \pmod{u_k}$ and $x^2 \equiv 5 - 12v_k \pmod{(1 + 12v_k^2)}$ cannot hold simultaneously.

Hence (25) is impossible.

(x) (25) is impossible if $n \equiv \pm 5 \pmod{60}$, $n \neq \pm 5$.

For, we can write $n = \pm 5 + 2l.165k$, where $k = 2^t$, $t \geq 1$

Then $u_n \equiv -u_5 \pmod{u_{165k}}$

$\equiv -362 \pmod{u_{165k}}$,

and hence we should have $x^2 \equiv -719 \pmod{u_{165k}}$.

Since $u_{165k} = u_{11.15k} = u_{5.33k}$, we have, $u_{15k} | u_{165k}$ and $u_{33k} | u_{165k}$.

Thus we have,

$$x^2 \equiv -719 \pmod{u_k}, \tag{28}$$

$$x^2 \equiv -719 \pmod{f_1(u_k)}, \tag{29}$$

$$x^2 \equiv -719 \pmod{f_3(u_k)}, \tag{30}$$

$$x^2 \equiv -719 \pmod{f_9(u_k)}, \tag{31}$$

$$x^2 \equiv -719 \pmod{f_{11}(u_k)}, \tag{32}$$

$$x^2 \equiv -719 \pmod{f_{12}(u_k)} \tag{33}$$

Now, the quadractic non-residues of 719 are

11	17	19	22	23	33	34	38	41	43
44	46	47	51	53	55	57	66	67	68
69	71	73	76	77	79	82	85	86	88
89	92	94	95	97	99	101	102	106	109
110	114	115	119	123	127	129	131	132	133
134	136	138	139	141	142	143	146	152	153
154	157	158	159	161	164	165	170	171	172
173	176	178	179	184	188	190	193	194	197
198	199	201	202	204	205	207	212	213	215
218	219	220	221	223	228	229	230	231	233
235	237	238	239	246	247	251	254	255	258
262	264	265	266	267	268	269	271	272	275
276	278	282	284	285	286	287	291	292	297
299	301	303	304	306	307	308	313	314	316
318	319	322	327	328	329	330	335	337	340
341	342	344	345	346	347	349	352	353	355
356	357	358	359	365	368	369	371	376	380
381	383	385	386	387	388	393	394	395	396
398	399	402	404	407	408	409	410	414	417

419	421	423	424	425	426	429	430	431	436
438	439	440	442	445	446	449	456	458	459
460	462	463	466	467	469	470	471	474	475
476	477	478	479	483	485	487	492	493	494
495	497	502	503	505	508	509	510	511	513
516	519	523	524	527	528	530	532	533	534
536	537	538	539	542	544	545	550	551	552
553	556	557	559	563	564	568	569	570	571
572	574	575	579	582	584	589	591	593	594
595	597	598	599	601	602	603	606	607	608
611	612	614	615	616	619	621	623	626	628
629	632	635	636	638	639	641	644	645	647
649	654	655	656	657	658	659	660	661	663
665	667	669	670	671	674	677	679	680	682
683	684	687	688	689	690	691	692	693	694
695	698	699	701	703	704	705	706	707	709
710	711	712	713	714	715	716	717	718.	

The residues of u_k, $f_1(u_k)$, $f_3(u_k)$, $f_9(u_k)$, $f_{11}(u_k)$ $f_{12}(u_k)$ are periodic and the length of the period is 179. Consequently we obtain the following results:

(a) The residues of u_k, modulo 719, for = 1, 2,---179 are

7	97	123	59	490	626	41	485	223	235
442	310	226	53	584	499	453	587	335	121
521	36	434	674	454	244	436	559	150	421
14	391	186	167	414	547	209	362	371	623
456	289	233	8	127	621	513	29	243	181

92	390	62	497	64	282	148	667	374	60
9	161	73	591	412	119	280	57	26	632
38	11	241	402	376	184	125	332	433	378
324	3	17	577	63	28	129	207	136	322
295	51	168	365	419	249	333	325	582	149
542	104	61	251	176	117	55	297	262	677
651	619	586	146	210	481	404	5	49	487
516	451	566	82	505	278	701	647	301	13
337	652	349	579	373	4	31	483	665	79
258	112	641	663	519	190	299	489	106	182
99	188	225	589	6	71	15	449	561	316
548	242	649	452	215	417	500	294	311	30
361	363	25	530	260	27	19	2		

and therefore (28) is impossible for t = 2, 3, 6, 7, 8, 9, 10, 11, 14, 15, 19, 24, 27, 28, 30, 35, 39, 40, 41, 43, 45, 46, 47, 51, 54, 56, 58, 62, 63, 64, 66, 68, 70, 71, 72, 74, 75, 76, 83, 87, 88, 89, 90, 92, 94, 95, 99, 101, 104, 105, 107, 108, 109, 110, 112, 114, 117, 120, 121, 124, 125, 126, 127, 128, 129, 131, 133, 134, 138, 139, 140, 141, 143, 144, 145, 146, 147, 149, 151, 152, 154, 156, 158, 160, 163, 165, 166, 173, 175, 178.

(b) The residues of $f_1(u_k)$ modulo 719, for t = 1, 5, 18, 20, 21, 23, 25, 26, 32, 36, 38, 48, 52, 55, 57, 59, 60, 65, 69, 77, 78, 80, 82, 85, 91, 96, 97, 106, 113, 116, 118, 119, 137, 150, 153, 155, 157, 161, 164, 168, 172, 174, 176, are

193, 532,669, 322, 71, 628, 487, 152, 371, 417, 22, 485, 123

563, 614, 119, 17, 237, 544, 663, 146, 647, 33, 55, 101, 665, 649, 109, 291, 88, 97, 254, 246, 197, 458, 141, 178, 483, 429, 621, 46, 340, 53, respectively and therefore (29) is impossible for the above values of t.

(c) The residues of $f_3(u_k)$ modulo 719 for t = 13, 16, 33, 34, 37, 49, 50, 61, 67, 79, 86, 93, 100, 102, 103, 111, 112, 122, 135, 148, 169, 171, 179, are
344, 269, 495, 267, 19, 542, 597, 544, 658, 612, 157, 109, 563, 381, 570, 654, 471, 55, 153, 663, 41, 57, respectively and therefore (30) is impossible for the above values of t.

(d) The residues of $f_9(u_k)$ modulo 719, for t = 17, 22, 31, 42, 44, 53, 81, 115, 123, 130, 136, 142, 159, 162, 167, 177, are
44, 141, 635, 306, 344, 701, 626, 299, 497, 346, 701, 127, 213, 693, 86, 89, respectively and therefore (31) is impossible for the above values of t.

(e) The residues of $f_{11}(u_k)$ modulo 719, for t = 12, 73, 84, 98, 132, 170, are
86, 46, 683, 89, and therefore (32) is impossible for the above values of t.

(f)) The residues of $f_{12}(u_k)$ modulo 719, for t = 4, 29, are 17, 55 respectively and therefore (33) is impossible for these values of t.

Thus we see that at least one of (28), (29), (30), (31), (32), (33) is impossible for t = 1, 2, --- 719. Thus (25) is impossible.

Summarizing the results we see that (25) can hold for n odd, only when $n = 1$ and $n = 5$ and these values do indeed satisfy with $u = 2$, $v = 1$, $x = 3$, $y = 1$, and $u = 362$, $v = 209$, $x = 19$, $y = 209$. $x = 3$, $y = 1$ give the solution $X = 0$, $Y = 0$, and $X = 19$, $Y = 209$ give the solution $X = 12$, $Y = 104$.

Hence the theorem.

BIBLIOGRAPHY

1. Baker, A. & Davenport, H., The equation $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$, Quart. J. Math. Oxford (2), 20 (1969), 129-137.

2. Cassels, J.W.S., Integral points on certain elliptic curves, Proc. Lond. Math. Soc. (3), 14A (1965), 55-57.

3. Cohn, J.H.E., The diophantine equation $Y(Y + 1)(Y + 2)(Y + 3) = 2X(X + 1)(X + 2)(X + 3)$, Pac. Journ. Maths. 37 (1971), 331-335.

4 Dickson, L.E., History of Theory of Numbers, Volume II, New York (1952), 634-639.

5. Ljunggren, W., Solution complete de quelques equations du sixieme degre a deux indeterminees, Arch. Math. Naturv., 48 (1946), Nr. 7, 26-29.

6. Mordell, L.J., Diophantine Equations, London & New York, (1969), 21.

7. Nagell, T., Introduction to Number Theory, New York, (1951), 158.

8. Pocklington, H.C., Some diophantine impossibilities, Proc. Camb. Phil. Soc. 17 (1913) 108-121.