ACTA ARITHMETICA
139.3 (2009)

Squares in Lehmer sequences and the Diophantine equation $Ax^4 - By^2 = 2$

by

Pingzhi Yuan (Guangzhou) and Yuan Li (Winston-Salem, NC)

1. Introduction. Let $L > 0$ and M be rational integers such that $L - 4M > 0$ and $(L, M) = 1$. Let α and β be the two roots of the trinomial $x^2 - \sqrt{L}\,x + M$. For a non-negative integer n, the nth term in the Lehmer sequence $\{P_n\}$ (see [5]) is defined by

$$P_n := P_n(\alpha,\beta) = \begin{cases} \dfrac{\alpha^n - \beta^n}{\alpha - \beta} & \text{for } n \text{ odd},\\[2mm] \dfrac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} & \text{for } n \text{ even}.\end{cases} \tag{1.1}$$

Lehmer sequences have many interesting properties and often arise in the study of Diophantine equations. The arithmetic properties of the numbers P_n can be found in [5, 15].

The main purpose of the present paper is to investigate the occurrence of squares in Lehmer sequences and their applications to Diophantine equations of the form

$$aX^4 - bY^2 = 2, \tag{1.2}$$

where a and b are given positive odd integers. This type of problem has received considerable interest (see [3, 4, 11, 10, 14]). In certain ways it actually goes back to the classical work of Ljunggren [6–9], who was able to prove many theorems on equations of the form $aX^4 - bY^2 = c$ with $c \in \{\pm 1, -2, \pm 4\}$, but he did not prove any result on the case $c = 2$ (curiously). Therefore, the result of this paper can be viewed as a case that Ljunggren missed, for reasons that will never be known. Here as well as throughout the paper, we use $\left(\frac{A}{B}\right)$ to denote the Jacobi symbol of A with respect to B, where A and B are coprime integers.

Rotkiewicz proved the following two results concerning the equations $P_p = px^2$, $P_p = x^2$, where p is an odd prime.

2010 *Mathematics Subject Classification*: 11D25, 11B39.
Key words and phrases: Diophantine equations, Lehmer sequences.

DOI: 10.4064/aa139-3-6

Theorem R1 (Theorem 5 in [11]). *For an odd prime p the equation $P_p = px^2$, with x an integer, has no solutions provided that one of the following two sets of assumptions is satisfied*:

- $(L, M) \equiv (1, 0) \pmod 4$ *and* $\left(\frac{L}{M}\right) = 1$, *or*
- $(L, M) \equiv (0, 3) \pmod 4$ *and* $\left(\frac{M}{L}\right) = 1$.

Theorem R2 (Theorem 3 in [11]). *For an odd prime p the equation $P_p = x^2$, with x an integer, has no solutions provided that one of the following two sets of assumptions is satisfied*:

- $(L, M) \equiv (3, 0) \pmod 4$ *and* $\left(\frac{L}{M}\right) = 1$, *or*
- $(L, M) \equiv (0, 1) \pmod 4$ *and* $\left(\frac{M}{L}\right) = 1$.

Motivated by Diophantine equations of the form

$$aX^2 - bY^4 = 2, \tag{1.3}$$

where a and b are odd positive integers, Luca and Walsh [10] proved the following results similar to those in Theorems R1 and R2 for different sets of Lehmer sequences.

Theorem LW1 (Theorem 1 in [10]). *Let p be an odd prime.*

- *If* $(L, M) \equiv (2, 1) \pmod 4$ *and* $\left(\frac{L}{M}\right) = 1$, *then the equation $P_p = px^2$, with x an integer, has no solutions.*
- *If* $(L, M) \equiv (2, 1) \pmod 4$ *and* $\left(\frac{L}{M}\right) = 1$, *then the equation $P_p = x^2$, with x an integer, has no solutions provided that $p > 3$.*

In the first part of this paper, by the method similar to that of Luca and Walsh [10], we will prove similar results for more sets of Lehmer sequences.

Theorem 1.1. *Let p be an odd prime. If* $(L, M) \equiv (2, 3) \pmod 4$ *and* $\left(\frac{L}{M}\right) = 1$, *then the equation $P_p = x^2$, with x an integer, has no solutions.*

Theorem 1.2. *Let p be an odd prime. If* $(L, M) \equiv (2, 3) \pmod 4$ *and* $\left(\frac{L}{M}\right) = 1$, *then the equation $P_p = px^2$, with x an integer, has no solutions provided that $p > 3$.*

1.1. *Diophantine applications.* Suppose that a and b are odd positive integers for which the equation

$$aX^2 - bY^2 = 2 \tag{1.4}$$

is solvable in positive integers (X, Y). Let (a_1, b_1) be the minimal positive solution of equation (1.4), and define

$$\alpha = \frac{a_1\sqrt{a} + b_1\sqrt{b}}{\sqrt{2}}. \tag{1.5}$$

Furthermore, for k odd, define

$$\alpha^k = \frac{a_k\sqrt{a} + b_k\sqrt{b}}{\sqrt{2}},$$

where $(a_k,\ b_k)$ are positive integers. It is well known that all positive integer solutions (X,Y) of equation (1.4) are of the form $(a_k,\ b_k)$. Thus we see that a solution to (1.2) is equivalent to the existence of an index k for which $a_k = x^2$.

As an application of Theorem LW1, Luca and Walsh [10] proved the following theorem.

Theorem LW2 (Theorem 2 in [10]).

- *If* b_1 *is not a square, then equation* (1.3) *has no solutions.*
- *If* b_1 *is a square and* b_3 *is not a square, then* $(X,Y) = (a_1, \sqrt{b_1})$ *is the only solution of equation* (1.3).
- *If* b_1 *and* b_3 *are both squares, then* $(X,Y) = (a_1, \sqrt{b_1})$ *and* $(a_3, \sqrt{b_3})$ *are the only solutions of equation* (1.3).

In recent papers [1, 2, 13], using the Thue–Siegel method, it is proved that the equation (1.2) has at most two solutions in positive integers. Moreover, Akhtari, Togbé and Walsh [2] posed the following conjecture.

Conjecture 1.3. *For any positive odd integers* a, b, *the equation* $aX^4 - bY^2 = 2$ *has at most one solution in positive integers, and such a solution must arise from the fundamental solution to the quadratic equation* $aX^2 - bY^2 = 2$.

As an application of Theorem 1.1, we prove the following result which confirms this conjecture.

Theorem 1.4. *For any positive odd integers* a, b, *the equation* $aX^4 - bY^2 = 2$ *has at most one solution in positive integers, and such a solution arises from the fundamental solution to the quadratic equation* $aX^2 - bY^2 = 2$.

2. Properties of Jacobi's symbol $\left(\frac{P_n}{P_m}\right)$**.** Let m and n be coprime positive odd integers. As in the Eisenstein rule (see [9, p. 330]) we write the following sequence of equalities:

$$\tag{2.1} \begin{cases} n = 2k_1 m + \varepsilon_1 r_1, & 0 < r_1 < p, \\ m = 2k_2 r_1 + \varepsilon_2 r_2, & 0 < r_2 < r_1, \\ r_1 = 2k_3 r_2 + \varepsilon_3 r_3, & 0 < r_3 < r_2, \\ \qquad \dots & \\ r_{l-3} = 2k_{l-1} r_{l-2} + \varepsilon_{l-1} r_{l-1}, & 0 < r_{l-1} < r_{l-2}, \\ r_{l-2} = 2k_l r_{l-1} + \varepsilon_l r_l, & r_l = 1, \\ \varepsilon_i = \pm 1, \quad 2 \nmid r_i, & i = 1, 2, \dots, l. \end{cases}$$

Then (see [12, p. 332])

$$\left(\frac{n}{m}\right) = (-1)^{\sum_{i=1}^{l} \frac{r_{i-1}-1}{2} \cdot \frac{\varepsilon_i r_i - 1}{2}}, \quad r_0 = m. \tag{2.2}$$

To compute the Jacobi symbol $\left(\frac{P_n}{P_m}\right)$ in the case $(L, M) \equiv (2, 3) \pmod 4$ and $\left(\frac{L}{M}\right) = 1$, we need a result of Rotkiewicz (Lemmas 1 and 3 in [11]).

Lemma 2.1. *If* $(L, M) \equiv (2, 3) \pmod 4$ *and* $\left(\frac{L}{M}\right) = 1$, *then* $P_n \equiv \left(\frac{2}{n}\right) \pmod 4$ *and* $\left(\frac{M}{P_n}\right) = \left(\frac{2}{n}\right)$.

With the above notations, by Theorem 1 in [11] we have the following result.

Theorem 2.2. *If* $(L, M) \equiv (2, 3) \pmod 4$ *and* $\left(\frac{L}{M}\right) = 1$, *then*

$$\left(\frac{P_n}{P_m}\right) = (-1)^{\sum_{i=1}^{l} \frac{\left(\frac{2}{r_{i-1}}\right)-1}{2} \cdot \frac{\varepsilon_i \left(\frac{2}{r_i}\right)-1}{2}} \cdot \left(\frac{2}{m}\right)^{k_1 + \frac{\varepsilon_1 - 1}{2}} \cdots \left(\frac{2}{r_{l-1}}\right)^{k_l + \frac{\varepsilon_l - 1}{2}},$$

where $r_0 = m$.

A closer look at the above formula shows that we only need to consider those r_i $(i = 0, \ldots, l-1)$ such that $r_i \equiv 3, 5 \pmod 8$. If $r_i \equiv 3, 5 \pmod 8$ and $r_{i+1} \equiv 1, 7 \pmod 8$, then the contribution of r_i to the above formula is

$$(-1)^{k_{i+1} + \frac{\varepsilon_{i+1} - 1}{2} + \frac{\varepsilon_{i+1} - 1}{2}} = (-1)^{k_{i+1}}.$$

If $r_i \equiv 3, 5 \pmod 8$ and $r_{i+1} \equiv 3, 5 \pmod 8$, then the contribution of r_i to the above formula is

$$(-1)^{k_{i+1} + \frac{\varepsilon_{i+1} - 1}{2} + \frac{-\varepsilon_{i+1} - 1}{2}} = (-1)^{k_{i+1}+1}.$$

For the sake of brevity, we introduce the following notations:

$$\lambda_1 = \lambda_1(m, n) = \sharp\{i : r_{i-1} \equiv 3, 5 \pmod 8,\ r_i \equiv 1, 7 \pmod 8 \text{ and } 2 \nmid k_i\},$$
$$\lambda_2 = \lambda_2(m, n) = \sharp\{i : r_{i-1} \equiv 3, 5 \pmod 8,\ r_i \equiv 3, 5 \pmod 8 \text{ and } 2 \mid k_i\}.$$

With the above notations, we can rewrite Theorem 2.2 as follows.

Corollary 2.3. *If* $(L, M) \equiv (2, 3) \pmod 4$ *and* $\left(\frac{L}{M}\right) = 1$, *then*

$$\left(\frac{P_n}{P_m}\right) = (-1)^{\lambda_1 + \lambda_2}.$$

Note that the above formula for the Jacobi's symbol is independent of the signs of ε_i, $i = 1, \ldots, l$. For the sake of brevity, we use

$$a_1 - a_2 - \cdots - a_s$$

to denote the division $a_1 = 2a_2 \pm a_3, a_2 = 2a_3 \pm a_4, \ldots, a_{s-2} = 2a_{s-1} \pm a_s$;

$$\lambda_1 = u; r_{i_1}, \ldots, r_{i_u}$$

to denote $r_{i_j} \equiv 3, 5 \pmod 8), r_{i_j+1} \equiv 1, 7 \pmod 8)$ and $2 \nmid k_{i_j+1}$ $(j = 1, \ldots, u)$, and

$$\lambda_2 = v; r_{i_1}, \ldots, r_{i_v}$$

to denote $r_{i_j} \equiv 3, 5 \pmod 8), r_{i_j+1} \equiv 3, 5 \pmod 8)$ and $2 \mid k_{i_j+1}$ $(j = 1, \ldots, v)$.

3. Proof of Theorem 1.1. By Lemma 2.1 and $P_p = x^2$, we have $p \equiv \pm 1 \pmod 8$ and $\left(\frac{P_p}{P_q}\right) = 1$ for any positive integer q coprime with p. Hence it suffices to choose a positive integer $q = r_0$ such that $\gcd(p, q) = 1$ and $\lambda_1(q, p) + \lambda_2(q, p)$ is odd.

3.1. *The case* $p \equiv 1 \pmod 8$. To begin, we prove the following four claims.

Claim 3.1. $p \equiv 1 \pmod 9$.

For $p \equiv -1 \pmod 3$, choosing $q = r_0 = 3$, we have

$$p = 6k_1 - 1, \qquad 2 \nmid k_1.$$

It follows that $\lambda_1 = 1; 3$ and $\lambda_2 = 0$, a contradiction.

For $p \equiv -5 \pmod 9$, choosing $q = r_0 = 9$, we have

$$p = 18k_1 - 5, \qquad 9 = 2 \times 5 - 1,$$

and so $\lambda_1 = 1; 5$ and $\lambda_2 = 0$, a contradiction again.

For $p \equiv 7 \pmod 9$, choosing $q = r_0 = 9$, we have

$$p = 18k_1 + 7, \qquad 9 - 7 - 5 - 3 - 1,$$

and so $\lambda_1 = 1; 3$ and $\lambda_2 = 0$, again a contradiction. Claim 3.1 is proved.

Claim 3.2. $p \equiv 1, 2 \pmod 5$.

Now we choose $q = r_0 = 5$. For $p \equiv -1 \pmod 5$, we have

$$p = 10k_1 - 1, \qquad 2 \nmid k_1,$$

and so $\lambda_1 = 1; 5$ and $\lambda_2 = 0$, a contradiction.

For $p \equiv 3 \pmod{10}$, we have

$$p = 10k_1 + 3, \qquad 2 \nmid k_1, \qquad 5 = 2 \times 3 - 1,$$

and so $\lambda_1 = 1; 3$ and $\lambda_2 = 0$, a contradiction again, which proves Claim 3.2.

Claim 3.3. $p \equiv \pm 1 \pmod 7$.

In this case, we choose $q = r_0 = 7$. If $p \equiv \pm 3 \pmod 7$, then

$$p = 14k_1 \pm 3, \qquad 7 = 2 \times 3 + 1.$$

It follows that $\lambda_1 = 1; 3$ and $\lambda_2 = 0$, a contradiction. If $p \equiv \pm 5 \pmod 7$, then

$$p = 14k_2 \pm 5, \qquad 7 = 2 \times 5 - 3, \qquad 5 = 2 \times 3 - 1.$$

It follows that $\lambda_1 = 1; 3$ and $\lambda_2 = 0$, a contradiction again, which proves Claim 3.3.

Claim 3.4. If $p \equiv 1 \pmod 3$ and $p \equiv 2 \pmod 5$, then $p \equiv -1 \pmod 7$.

Choose $q = r_0 = 105$. If $p \equiv 1 \pmod 7$, then

$$p = 210k_1 - 83, \quad 105 - 83 - 61 - 39 - 17 - 5,$$
$$17 = 4 \times 5 - 3, \quad 5 = 2 \times 3 - 1.$$

Therefore $\lambda_1 = 2; 61, 3$ and $\lambda_2 = 1; 5$, a contradiction.

By the above four claims, if an odd positive integer p with $p \equiv 1 \pmod 8$ satisfies $P_p = x^2$ for some positive integer x, then $p \equiv 1 \pmod 3$, $1, 2 \pmod 5$ and when $p \equiv 2 \pmod 5$ then $p \equiv -1 \pmod 7$. We divide the remaining proof into four cases.

For positive integers k and l, we use $P(k)$ and $Q(l)$ to denote the properties that

$$3^k \mid (p-1) \quad \text{and} \quad 5^l \mid (p+8).$$

Case 3.1: $[p \equiv 1 \pmod 5,\ p \equiv 1 \pmod 3,\ P(2k)] \Rightarrow P(2k+1)$. Otherwise, we have $p \equiv 1 \pmod 5$, $p \equiv 1 \pmod{3^{2k}}$, $p \not\equiv 1 \pmod{3^{2k+1}}$. First we consider the case where $p \equiv 1 + 2 \cdot 3^{2k} \pmod{3^{2k+1}}$, and choose $q = r_0 = 15 \cdot 3^{2k}$. Then we have $p \equiv 1 - 10 \cdot 3^{2k} \pmod{30 \cdot 3^{2k}}$ and

$$p = 10 \cdot 3^{2k+1} k_1 - (10 \cdot 3^{2k} - 1),$$
$$15 \cdot 3^{2k} = 2(10 \cdot 3^{2k} - 1) - (5 \cdot 3^{2k} - 2), \quad 10 \cdot 3^{2k} - 1 = 2(5 \cdot 3^{2k} - 2) + 3,$$
$$5 \cdot 3^{2k} - 2 = 6k_4 + 1, \quad 2 \nmid k_4.$$

It follows that $\lambda_1 = 1; 3$ and $\lambda_2 = 0$, a contradiction.

Next we consider the case where $p \equiv 1 - 2 \cdot 3^{2k} \pmod{3^{2k+1}}$, and choose $q = r_0 = 15 \cdot 3^{2k}$. Then $p \equiv 1 + 10 \cdot 3^{2k} \pmod{30 \cdot 3^{2k}}$ and

$$p = 30 \cdot 3^{2k} k_1 + (10 \cdot 3^{2k} + 1),$$
$$15 \cdot 3^{2k} = 2(10 \cdot 3^{2k} + 1) - (5 \cdot 3^{2k} + 2), \quad 10 \cdot 3^{2k} + 1 = 2(5 \cdot 3^{2k} + 2) - 3,$$
$$5 \cdot 3^{2k} + 2 = 6k_4 - 1, \quad 2 \mid k_4.$$

Hence $\lambda_1 = 1; 10 \cdot 3^{2k} + 1$ and $\lambda_2 = 0$, again a contradiction.

Case 3.2: $[p \equiv 1 \pmod 3,\ P(2k-1)] \Rightarrow P(2k)$. In this case we choose $q = r_0 = 3^{2k}$. First we consider the case where $p \equiv 1 + 2 \cdot 3^{2k-1} \pmod{3^{2k}}$. Note that

$$p = 2 \cdot 3^{2k} k_1 + (2 \cdot 3^{2k-1} + 1),$$
$$3^{2k} = 2(2 \cdot 3^{2k-1} + 1) - (3^{2k-1} + 2), \quad 2 \cdot 3^{2k-1} + 1 = 2(3^{2k-1} + 2) - 3,$$
$$3^{2k-1} + 2 = 6k_4 - 1, \quad 2 \nmid k_4.$$

Therefore $\lambda_1 = 1; 3$ and $\lambda_2 = 0$, a contradiction.

Next we consider the case where $p \equiv 1 - 2 \cdot 3^{2k-1} \pmod{3^{2k}}$, and choose $q = r_0 = 3^{2k}$. We have

$$p = 2 \cdot 3^{2k} k_1 - (2 \cdot 3^{2k-1} - 1),$$
$$3^{2k} = 2(2 \cdot 3^{2k-1} - 1) - (3^{2k-1} - 2), \qquad 2 \cdot 3^{2k-1} - 1 = 2(3^{2k-1} - 2) + 3,$$
$$3^{2k-1} - 2 = 6k_4 + 1, \qquad 2 \mid k_4.$$

Hence $\lambda_1 = 1; 2 \cdot 3^{2k-1} - 1$ and $\lambda_2 = 0$, a contradiction again.

Case 3.3: $[p \equiv 2 \pmod 5, Q(2k)] \Rightarrow Q(2k+1)$. Otherwise, we have $p \equiv -8 + 5^{2k}$, $-8 - 5^{2k}$, $-8 - 3 \cdot 5^{2k}$, $-8 + 3 \cdot 5^{2k} \pmod{5^{2k+1}}$, so we divide the proof into four subcases.

Subcase 3.3.1: $p \equiv -8 + 3 \cdot 5^{2k} \pmod{5^{2k+1}}$. Since $p \equiv 1 \pmod 3$ and $p \equiv -1 \pmod 7$, choosing $q = r_0 = 105 \cdot 5^{2k}$, we have $p \equiv 63 \cdot 5^{2k} - 8 \pmod{210 \cdot 5^{2k}}$ and

$$p = 210 \cdot 5^{2k} k_1 + (63 \cdot 5^{2k} - 8),$$
$$105 \cdot 5^{2k} = 2(63 \cdot 5^{2k} - 8) - (21 \cdot 5^{2k} - 16),$$
$$63 \cdot 5^{2k} - 8 = 4(21 \cdot 5^{2k} - 16) - (21 \cdot 5^{2k} - 56),$$
$$(21 \cdot 5^{2k} - 16) - (21 \cdot 5^{2k} - 56) - (21 \cdot 5^{2k} - 96) - \cdots$$
$$\cdots - 109 - 69 - 29 - 11 - 7 - 3 - 1.$$

Hence $\lambda_1 = 2; 11, 3$ and $\lambda_2 = 1; 21 \cdot 5^{2k} - 16$, a contradiction.

Subcase 3.3.2: $p \equiv -8 - 3 \cdot 5^{2k} \pmod{5^{2k+1}}$. Since $p \equiv 1 \pmod 3$ and $p \equiv -1 \pmod 7$, choosing $q = r_0 = 105 \cdot 5^{2k}$, we have $p \equiv -63 \cdot 5^{2k} - 8 \pmod{210 \cdot 5^{2k}}$ and

$$p = 210 \cdot 5^{2k} k_1 - (63 \cdot 5^{2k} + 8),$$
$$105 \cdot 5^{2k} = 2(63 \cdot 5^{2k} + 8) - (21 \cdot 5^{2k} + 16),$$
$$63 \cdot 5^{2k} + 8 = 2(21 \cdot 5^{2k} + 16) + (21 \cdot 5^{2k} - 24),$$
$$(21 \cdot 5^{2k} + 16) - (21 \cdot 5^{2k} - 24) - (21 \cdot 5^{2k} - 64) - \cdots$$
$$\cdots - 101 - 61 - 21 - 19 - 17 - 15 - 13 - 11 - 9 - 7 - 5 - 3 - 1.$$

Hence $\lambda_1 = 3; 19, 11, 3$ and $\lambda_2 = 0$, again a contradiction.

Subcase 3.3.3: $p \equiv -8 + 5^{2k} \pmod{5^{2k+1}}$. Since $p \equiv 1 \pmod 3$, choosing $q = r_0 = 15 \cdot 5^{2k}$, we have $p \equiv -9 \cdot 5^{2k} - 8 \pmod{30 \cdot 5^{2k}}$ and

$$p = 30 \cdot 5^{2k} k_1 - (9 \cdot 5^{2k} + 8),$$
$$15 \cdot 5^{2k} = 2(9 \cdot 5^{2k} + 8) - (3 \cdot 5^{2k} + 16),$$

$$9\cdot 5^{2k}+8=2(3\cdot 5^{2k}+16)+(3\cdot 5^{2k}-24),$$
$$(3\cdot 5^{2k}+16)-(3\cdot 5^{2k}-24)-(3\cdot 5^{2k}-64)-\cdots-91-51-11,$$
$$51=4\times 11+7,\quad 11-7-3-1.$$

Hence $\lambda_1=1;3$ and $\lambda_2=0$, again a contradiction.

SUBCASE 3.3.4: $p\equiv -8-5^{2k} \pmod{5^{2k+1}}$. Since $p\equiv 1 \pmod 3$, choosing $q=r_0=15\cdot 5^{2k}$, we have $p\equiv 9\cdot 5^{2k}-8 \pmod{30\cdot 5^{2k}}$ and

$$p=30\cdot 5^{2k}k_1+(9\cdot 5^{2k}-8),$$
$$15\cdot 5^{2k}=2(9\cdot 5^{2k}-8)-(3\cdot 5^{2k}-16),$$
$$9\cdot 5^{2k}-8=4(3\cdot 5^{2k}-16)-(3\cdot 5^{2k}-56),$$
$$(3\cdot 5^{2k}-16)-(3\cdot 5^{2k}-56)-(3\cdot 5^{2k}-96)-\cdots-99-59-19,$$
$$59=4\times 19-17,\quad 19-17-15-13-11-9-7-5-3-1.$$

Hence $\lambda_1=2;\ 11,\ 3$ and $\lambda_2=1;\ 3\cdot 5^{2k}-16$, a contradiction again.

CASE 3.4: $[p\equiv 2 \pmod 5, Q(2k-1)] \Rightarrow Q(2k)$. Otherwise, $p\equiv -8+5^{2k-1}, -8-5^{2k-1}, -8-3\cdot 5^{2k-1}, -8+3\cdot 5^{2k-1} \pmod{5^{2k}}$, so we also divide the proof into four subcases.

SUBCASE 3.4.1: $p\equiv -8+3\cdot 5^{2k-1} \pmod{5^{2k}}$. Choosing $q=r_0=5^{2k}$, we have

$$p=2\cdot 5^{2k}k_1+(3\cdot 5^{2k-1}-8),$$
$$5^{2k}=2(3\cdot 5^{2k-1}-8)-(5^{2k-1}-16),$$
$$3\cdot 5^{2k-1}-8=4(5^{2k-1}-16)-(5^{2k-1}-56),$$
$$(5^{2k-1}-16)-(5^{2k-1}-56)-(5^{2k-1}-96)-\cdots$$
$$\cdots-109-69-29-11-7-3-1.$$

Hence $\lambda_1=2;11,3$ and $\lambda_2=1$ or $5^{2k-1}-16$, a contradiction.

SUBCASE 3.4.2: $p\equiv -8-3\cdot 5^{2k-1} \pmod{5^{2k}}$. Choosing $q=r_0=5^{2k}$, we have

$$p=2\cdot 5^{2k}k_1-(3\cdot 5^{2k-1}+8),$$
$$5^{2k}=2(3\cdot 5^{2k-1}+8)-(5^{2k-1}+16),$$
$$3\cdot 5^{2k-1}+8=2(5^{2k-1}+16)+(5^{2k-1}-24),$$
$$(5^{2k-1}+16)-(5^{2k-1}-24)-(5^{2k-1}-64)-\cdots$$
$$\cdots-101-61-21-19-17-15-13-11-9-7-5-3-1.$$

Hence $\lambda_1=3;19,11$ or 3 and $\lambda_2=0$, a contradiction again.

Subcase 3.4.3: $p \equiv -8 + 5^{2k-1} \pmod{5^{2k}}$. Choose $q = r_0 = 18 \cdot 5^{2k}$. Since $p \equiv 1 \pmod 9$, we have $p \equiv -9 \cdot 5^{2k-1} - 8 \pmod{90 \cdot 5^{2k-1}}$ and

$$p = 90 \cdot 5^{2k-1} k_1 - (9 \cdot 5^{2k-1} + 8),$$
$$45 \cdot 5^{2k-1} = 4(9 \cdot 5^{2k-1} + 8) + (9 \cdot 5^{2k-1} - 32),$$
$$9 \cdot 5^{2k-1} + 8 = 2(9 \cdot 5^{2k-1} - 32) - (9 \cdot 5^{2k-1} - 72),$$
$$(9 \cdot 5^{2k-1} + 8) - (9 \cdot 5^{2k-1} - 32) - (9 \cdot 5^{2k-1} - 72) - \cdots - 93 - 53 - 13,$$
$$53 = 4 \times 13 + 1.$$

Hence $\lambda_1 = 0$ and $\lambda_2 = 1; 9 \cdot 5^{2k-1} + 8$, a contradiction again.

Subcase 3.4.4: $p \equiv -8 - 5^{2k-1} \pmod{5^{2k}}$. Choosing $q = r_0 = 5^{2k}$, we have

$$p = 2 \cdot 5^{2k} k_1 - (5^{2k-1} + 8),$$
$$5^{2k} = 4(5^{2k-1} + 8) + (5^{2k-1} - 32),$$
$$5^{2k-1} + 8 = 2(5^{2k-1} - 32) - (5^{2k-1} - 72),$$
$$(5^{2k-1} + 8) - (5^{2k-1} - 32) - (5^{2k-1} - 72) - \cdots - 93 - 53 - 13,$$
$$53 = 4 \times 13 + 1.$$

Hence $\lambda_1 = 0$ and $\lambda_2 = 1; 5^{2k-1} + 8$, again a contradiction.

3.2. *The case $p \equiv -1 \pmod 8$.* Now let us say something about the case $p \equiv -1 \pmod 8$. It is not difficult to see that the argument is quite the same as in the case $p \equiv 1 \pmod 8$. We can use the same modules to derive contradictions. For the sake of completeness, we present the details.

We have the following four claims.

Claim 4.1. $p \equiv -1 \pmod 9$.

For $p \equiv 1 \pmod 3$, choosing $q = r_0 = 3$, we have

$$p = 6k_1 + 1, \quad 2 \nmid k_1.$$

It follows that $\lambda_1 = 1; 3$ and $\lambda_2 = 0$, a contradiction.

For $p \equiv 5 \pmod 9$, choosing $q = r_0 = 9$, we have

$$p = 18k_1 + 5, \quad 9 = 2 \times 5 - 1,$$

and so $\lambda_1 = 1; 5$ and $\lambda_2 = 0$, a contradiction again.

For $p \equiv -7 \pmod 9$, choosing $q = r_0 = 9$, we have

$$p = 18k_1 - 7, \quad 9 - 7 - 5 - 3 - 1,$$

and so $\lambda_1 = 1; 3$ and $\lambda_2 = 0$, again a contradiction. Claim 4.1 is proved.

Claim 4.2. $p \equiv -1, -2 \pmod 5$.

Now we choose $q = r_0 = 5$. For $p \equiv 1 \pmod 5$, we have

$$p = 10k_1 + 1, \quad 2 \nmid k_1.$$

Then $\lambda_1 = 1; 5$ and $\lambda_2 = 0$, a contradiction.

For $p \equiv 7 \pmod{10}$, we have

$$p = 10k_1 - 3, \quad 2 \nmid k_1, \quad 5 = 2 \times 3 - 1,$$

so $\lambda_1 = 1; 3$ and $\lambda_2 = 0$, a contradiction again, which proves Claim 4.2.

Claim 4.3. $p \equiv \pm 1 \pmod 7$.

In this case, we choose $q = r_0 = 7$. If $p \equiv \pm 3 \pmod 7$, then

$$p = 14k_1 \pm 3, \quad 7 = 2 \times 3 + 1.$$

It follows that $\lambda_1 = 1; 3$ and $\lambda_2 = 0$, a contradiction. If $p \equiv \pm 5 \pmod 7$, then

$$p = 14k_2 \pm 5, \quad 7 = 2 \times 5 - 3, \quad 5 = 2 \times 3 - 1.$$

It follows that $\lambda_1 = 1; 3$ and $\lambda_2 = 0$, a contradiction again, which proves Claim 4.3.

Claim 4.4. If $p \equiv -1 \pmod 3$, $p \equiv -2 \pmod 5$, then $p \equiv 1 \pmod 7$.

Choose $q = r_0 = 105$. If $p \equiv -1 \pmod 7$, then

$$p = 210k_1 + 83, \quad 105 - 83 - 61 - 39 - 17 - 5,$$
$$17 = 4 \times 5 - 3, \quad 5 = 2 \times 3 - 1.$$

Therefore $\lambda_1 = 2; 61, 3$ and $\lambda_2 = 1; 5$, a contradiction.

By the above four claims, if an odd positive integer p with $p \equiv -1 \pmod 8$ satisfies $P_p = x^2$ for some positive integer x, then $p \equiv -1 \pmod 9$, $p \equiv -1, -2 \pmod 5$ and if $p \equiv -2 \pmod 5$ then $p \equiv 1 \pmod 7$. We divide the remaining proof into four cases.

For positive integers k and l, we use $P(k)$ and $Q(l)$ to denote the properties that

$$3^k \mid (p+1) \quad \text{and} \quad 5^l \mid (p-8).$$

Case 4.1: $[p \equiv -1 \pmod 5,\ p \equiv -1 \pmod 3,\ P(2k)] \Rightarrow P(2k+1)$. Otherwise, we have $p \equiv -1 \pmod 5$, $p \equiv -1 \pmod{3^{2k}}$, $p \not\equiv -1 \pmod{3^{2k+1}}$. First we consider the case where $p \equiv -1 - 2 \cdot 3^{2k} \pmod{3^{2k+1}}$, and choose $q = r_0 = 15 \cdot 3^{2k}$. Then $p \equiv -1 + 10 \cdot 3^{2k} \pmod{30 \cdot 3^{2k}}$ and

$$p = 10 \cdot 3^{2k+1} k_1 + (10 \cdot 3^{2k} - 1),$$
$$15 \cdot 3^{2k} = 2(10 \cdot 3^{2k} - 1) - (5 \cdot 3^{2k} - 2), \quad 10 \cdot 3^{2k} - 1 = 2(5 \cdot 3^{2k} - 2) + 3,$$
$$5 \cdot 3^{2k} - 2 = 6k_4 + 1, \quad 2 \nmid k_4.$$

It follows that $\lambda_1 = 1; 3$ and $\lambda_2 = 0$, a contradiction.

Next we consider the case where $p \equiv -1+2\cdot 3^{2k} \pmod{3^{2k+1}}$, and choose $q = r_0 = 15\cdot 3^{2k}$. Then $p \equiv -1-10\cdot 3^{2k} \pmod{30\cdot 3^{2k}}$ and

$$p = 30\cdot 3^{2k}k_1 - (10\cdot 3^{2k}+1),$$
$$15\cdot 3^{2k} = 2(10\cdot 3^{2k}+1)-(5\cdot 3^{2k}+2), \qquad 10\cdot 3^{2k}+1 = 2(5\cdot 3^{2k}+2)-3,$$
$$5\cdot 3^{2k}+2 = 6k_4-1, \qquad 2\mid k_4.$$

Hence $\lambda_1 = 1; 10\cdot 3^{2k}+1$ and $\lambda_2 = 0$, again a contradiction.

Case 4.2: $[p\equiv -1 \pmod 3,\ P(2k-1)] \Rightarrow P(2k)$. In this case we choose $q = r_0 = 3^{2k}$. First we consider the case where $p \equiv -1-2\cdot 3^{2k-1} \pmod{3^{2k}}$. Note that

$$p = 2\cdot 3^{2k}k_1 - (2\cdot 3^{2k-1}+1),$$
$$3^{2k} = 2(2\cdot 3^{2k-1}+1)-(3^{2k-1}+2), \qquad 2\cdot 3^{2k-1}+1 = 2(3^{2k-1}+2)-3,$$
$$3^{2k-1}+2 = 6k_4-1, \quad 2\nmid k_4.$$

Therefore $\lambda_1 = 1; 3$ and $\lambda_2 = 0$, a contradiction.

Next we consider the case where $p \equiv -1+2\cdot 3^{2k-1} \pmod{3^{2k}}$, and choose $q = r_0 = 3^{2k}$. We have

$$p = 2\cdot 3^{2k}k_1 + (2\cdot 3^{2k-1}-1),$$
$$3^{2k} = 2(2\cdot 3^{2k-1}-1)-(3^{2k-1}-2), \qquad 2\cdot 3^{2k-1}-1 = 2(3^{2k-1}-2)+3,$$
$$3^{2k-1}-2 = 6k_4+1, \qquad 2\mid k_4.$$

Hence $\lambda_1 = 1; 2\cdot 3^{2k-1}-1$ and $\lambda_2 = 0$, a contradiction again.

Case 4.3: $[p\equiv 3 \pmod 5, Q(2k)] \Rightarrow Q(2k+1)$. Otherwise, we have $p \equiv 8+5^{2k},\ 8-5^{2k},\ 8-3\cdot 5^{2k},\ 8+3\cdot 5^{2k} \pmod{5^{2k+1}}$, so we divide the proof into four subcases.

Subcase 4.3.1: $p\equiv 8-3\cdot 5^{2k} \pmod{5^{2k+1}}$. Since $p\equiv -1 \pmod 3$ and $p\equiv 1 \pmod 7$, choosing $q = r_0 = 105\cdot 5^{2k}$, we have $p\equiv -63\cdot 5^{2k}+8 \pmod{210\cdot 5^{2k}}$ and

$$p = 210\cdot 5^{2k}k_1 - (63\cdot 5^{2k}-8),$$
$$105\cdot 5^{2k} = 2(63\cdot 5^{2k}-8)-(21\cdot 5^{2k}-16),$$
$$63\cdot 5^{2k}-8 = 4(21\cdot 5^{2k}-16)-(21\cdot 5^{2k}-56),$$
$$(21\cdot 5^{2k}-16)-(21\cdot 5^{2k}-56)-(21\cdot 5^{2k}-96)-\cdots$$
$$\cdots - 109-69-29-11-7-3-1.$$

Hence $\lambda_1 = 2; 11, 3$ and $\lambda_2 = 1; 21\cdot 5^{2k}-16$, a contradiction.

Subcase 4.3.2: $p\equiv 8+3\cdot 5^{2k} \pmod{5^{2k+1}}$. Since $p\equiv -1 \pmod 3$ and $p\equiv 1 \pmod 7$, choosing $q = r_0 = 105\cdot 5^{2k}$, we have $p\equiv 63\cdot 5^{2k}+8$

(mod $210 \cdot 5^{2k}$) and

$$p = 210 \cdot 5^{2k} k_1 + (63 \cdot 5^{2k} + 8),$$
$$105 \cdot 5^{2k} = 2(63 \cdot 5^{2k} + 8) - (21 \cdot 5^{2k} + 16),$$
$$63 \cdot 5^{2k} + 8 = 2(21 \cdot 5^{2k} + 16) + (21 \cdot 5^{2k} - 24),$$
$$(21 \cdot 5^{2k} + 16) - (21 \cdot 5^{2k} - 24) - (21 \cdot 5^{2k} - 64) - \cdots$$
$$\cdots - 101 - 61 - 21 - 19 - 17 - 15 - 13 - 11 - 9 - 7 - 5 - 3 - 1.$$

Hence $\lambda_1 = 3; 19, 11, 3$ and $\lambda_2 = 0$, again a contradiction.

Subcase 4.3.3: $p \equiv 8 - 5^{2k} \pmod{5^{2k+1}}$. Since $p \equiv -1 \pmod 3$, choosing $q = r_0 = 15 \cdot 5^{2k}$, we have $p \equiv 9 \cdot 5^{2k} + 8 \pmod{30 \cdot 5^{2k}}$ and

$$p = 30 \cdot 5^{2k} k_1 + (9 \cdot 5^{2k} + 8),$$
$$15 \cdot 5^{2k} = 2(9 \cdot 5^{2k} + 8) - (3 \cdot 5^{2k} + 16),$$
$$9 \cdot 5^{2k} + 8 = 2(3 \cdot 5^{2k} + 16) + (3 \cdot 5^{2k} - 24),$$
$$(3 \cdot 5^{2k} + 16) - (3 \cdot 5^{2k} - 24) - (3 \cdot 5^{2k} - 64) - \cdots - 91 - 51 - 11,$$
$$51 = 4 \times 11 + 7, \quad 11 - 7 - 3 - 1.$$

Hence $\lambda_1 = 1; 3$ and $\lambda_2 = 0$, again a contradiction.

Subcase 4.3.4: $p \equiv 8 + 5^{2k} \pmod{5^{2k+1}}$. Since $p \equiv 1 \pmod 3$, choosing $q = r_0 = 15 \cdot 5^{2k}$, we have $p \equiv -9 \cdot 5^{2k} + 8 \pmod{30 \cdot 5^{2k}}$ and

$$p = 30 \cdot 5^{2k} k_1 - (9 \cdot 5^{2k} - 8),$$
$$15 \cdot 5^{2k} = 2(9 \cdot 5^{2k} - 8) - (3 \cdot 5^{2k} - 16),$$
$$9 \cdot 5^{2k} - 8 = 4(3 \cdot 5^{2k} - 16) - (3 \cdot 5^{2k} - 56),$$
$$(3 \cdot 5^{2k} - 16) - (3 \cdot 5^{2k} - 56) - (3 \cdot 5^{2k} - 96) - \cdots - 99 - 59 - 19,$$
$$59 = 4 \times 19 - 17, \quad 19 - 17 - 15 - 13 - 11 - 9 - 7 - 5 - 3 - 1.$$

Hence $\lambda_1 = 2; 11, 3$ and $\lambda_2 = 1; 3 \cdot 5^{2k} - 16$, a contradiction again.

Case 4.4: $[p \equiv 3 \pmod 5, Q(2k-1)] \Rightarrow Q(2k)$. Otherwise, we have $p \equiv 8 + 5^{2k-1}, 8 - 5^{2k-1}, 8 - 3 \cdot 5^{2k-1}, 8 + 3 \cdot 5^{2k-1} \pmod{5^{2k}}$, so we also divide the proof into four subcases.

Subcase 4.4.1: $p \equiv 8 - 3 \cdot 5^{2k-1} \pmod{5^{2k}}$. Choosing $q = r_0 = 5^{2k}$, we have

$$p = 2 \cdot 5^{2k} k_1 - (3 \cdot 5^{2k-1} - 8),$$
$$5^{2k} = 2(3 \cdot 5^{2k-1} - 8) - (5^{2k-1} - 16),$$
$$3 \cdot 5^{2k-1} - 8 = 4(5^{2k-1} - 16) - (5^{2k-1} - 56),$$

$$(5^{2k-1}-16)-(5^{2k-1}-56)-(5^{2k-1}-96)-\cdots$$
$$\cdots-109-69-29-11-7-3-1.$$

Hence $\lambda_1 = 2$; 11, 3 and $\lambda_2 = 1$; $5^{2k-1} - 16$, a contradiction.

SUBCASE 4.4.2: $p \equiv 8 + 3 \cdot 5^{2k-1} \pmod{5^{2k}}$. Choosing $q = r_0 = 5^{2k}$, we have

$$p = 2 \cdot 5^{2k} k_1 + (3 \cdot 5^{2k-1} + 8),$$
$$5^{2k} = 2(3 \cdot 5^{2k-1} + 8) - (5^{2k-1} + 16),$$
$$3 \cdot 5^{2k-1} + 8 = 2(5^{2k-1} + 16) + (5^{2k-1} - 24),$$
$$(5^{2k-1}+16)-(5^{2k-1}-24)-(5^{2k-1}-64)-\cdots$$
$$\cdots-101-61-21-19-17-15-13-11-9-7-5-3-1.$$

Hence $\lambda_1 = 3; 19, 11, 3$ and $\lambda_2 = 0$, a contradiction again.

SUBCASE 4.4.3: $p \equiv 8 - 5^{2k-1} \pmod{5^{2k}}$. Choose $q = r_0 = 18 \cdot 5^{2k}$. Since $p \equiv -1 \pmod 9$, we have $p \equiv 9 \cdot 5^{2k-1} + 8 \pmod{90 \cdot 5^{2k-1}}$ and

$$p = 90 \cdot 5^{2k-1} k_1 + (9 \cdot 5^{2k-1} + 8),$$
$$45 \cdot 5^{2k-1} = 4(9 \cdot 5^{2k-1} + 8) + (9 \cdot 5^{2k-1} - 32),$$
$$9 \cdot 5^{2k-1} + 8 = 2(9 \cdot 5^{2k-1} - 32) - (9 \cdot 5^{2k-1} - 72),$$
$$(9 \cdot 5^{2k-1}+8)-(9 \cdot 5^{2k-1}-32)-(9 \cdot 5^{2k-1}-72)-\cdots-93-53-13,$$
$$53 = 4 \times 13 + 1.$$

Hence $\lambda_1 = 0$ and $\lambda_2 = 1; 9 \cdot 5^{2k-1} + 8$, a contradiction again.

SUBCASE 4.4.4: $p \equiv 8 + 5^{2k-1} \pmod{5^{2k}}$. Choosing $q = r_0 = 5^{2k}$, we have

$$p = 2 \cdot 5^{2k} k_1 + (5^{2k-1} + 8),$$
$$5^{2k} = 4(5^{2k-1} + 8) + (5^{2k-1} - 32),$$
$$5^{2k-1} + 8 = 2(5^{2k-1} - 32) - (5^{2k-1} - 72),$$
$$(5^{2k-1}+8)-(5^{2k-1}-32)-(5^{2k-1}-72)-\cdots-93-53-13,$$
$$53 = 4 \times 13 + 1.$$

Hence $\lambda_1 = 0$ and $\lambda_2 = 1; 5^{2k-1} + 8$, again a contradiction. Therefore we have proved Theorem 1.1 for the case $p \equiv -1 \pmod 8$.

If $n > 1$ is an odd integer with $P_n = x^2$, by Lemma 2.1 and $P_n = x^2$, we have $n \equiv \pm 1 \pmod 8$ and $\left(\frac{P_n}{P_q}\right) = 1$ for any positive integer q coprime with n. From the proof of the above two subsections, we see that P_n is not a square when $n > 1$ is an odd integer with $\gcd(n, 105) = 1$. Since $3, 5 \not\equiv \pm 1 \pmod 8$ and $7 \not\equiv -1 \pmod 9$, we derive that P_p is not a square for $p = 3, 5, 7$. Combining the above arguments, we have proved Theorem 1.1.

4. Proof of Theorem 1.2

4.1. *The solutions to equations $P_p = px^2$.* Suppose $P_p = px^2$, where p is an odd prime and x is a positive integer. By equation (23) in [11], we have

$$P_n = (\alpha-\beta)^2\lambda_n + nM^{(n-1)/2} \quad \text{for all odd } n > 0, \tag{4.1}$$

where λ_n is some rational integer. Since $P_p = px^2$, it follows that $p \mid P_p$. By a result of Lehmer (see [5] and [15]), we have $p \mid (\alpha-\beta)^2$. Now let q be any odd integer. By (4.1) and the fact that $p \mid (\alpha-\beta)^2$, it follows that

$$P_q \equiv qM^{(q-1)/2} \pmod p.$$

We therefore deduce the following sequence of equalities of Jacobi symbols:

$$\begin{aligned}\left(\frac{P_q}{P_p}\right) &= \left(\frac{P_q}{px^2}\right) = \left(\frac{P_q}{p}\right) = \left(\frac{qM^{(q-1)/2}}{p}\right)\\ &= \left(\frac{q}{p}\right)\cdot\left(\frac{M^{(q-1)/2}}{p}\right) = \left(\frac{q}{p}\right)\cdot\left(\frac{2}{p}\right)^{(q-1)/2}.\end{aligned} \tag{4.2}$$

For the last equality of (4.2), we have used Lemma 2.1. Thus, we have shown that the equation $P_p = px^2$ implies that

$$\left(\frac{q}{p}\right)\cdot\left(\frac{2}{p}\right)^{(q-1)/2} = \left(\frac{P_q}{P_p}\right) \quad \text{for all odd } q > 0. \tag{4.3}$$

We note that by Lemma 2.1, we can restrict to the cases $p \equiv 1, 3 \pmod 8$. In what follows, we investigate the relation (4.3). Hence it suffices to choose an integer r_1 such that $q = 2p + r_1$ or $q = 4p + r_1$ according to whether $r_1 \equiv 3 \pmod 4$ or $1 \pmod 4$, and

$$\left(\frac{q}{p}\right) \neq (-1)^{\lambda_1(p,q)+\lambda_2(p,q)}.$$

4.2. *The case $p \equiv 1 \pmod 8$.* To begin, we prove the following three claims.

Claim 5.1. $p \equiv \pm 1 \pmod 9$.

We choose $r_1 = 9$. Then for $p \equiv \pm 5 \pmod 9$, we have

$$q = 4p + 9, \qquad p = 18k_2 \pm 5, \qquad 9 = 2\times 5 - 1.$$

By Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = -1$ since $\lambda_1 = 1; 5, \lambda_2 = 0$. On the other hand, by the assumption, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = 1$, a contradiction.

For $p \equiv \pm 7 \pmod 9$, we have

$$q = 4p+9, \qquad p = 18k_2 \pm 7, \qquad 9 = 2\times 7 - 5, \qquad 7 = 2\times 5 - 3, \qquad 5 = 2\times 3 - 1.$$

By Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = -1$ since $\lambda_1 = 1; 3$ and $\lambda_2 = 0$. On the other hand, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = 1$, again a contradiction. Claim 5.1 is proved.

Claim 5.2. $p \equiv 1, 3 \pmod 5$.

Now we choose $r_1 = 5$. For $p \equiv -1 \pmod 5$, we have

$$q = 4p + 5, \quad p = 10k_2 - 1, \quad 2 \nmid k_2,$$

by Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = -1$ since $\lambda_1 = 1; 5$ and $\lambda_2 = 0$. On the other hand, by the assumption, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{5}{p}\right) = 1$, a contradiction.

For $p \equiv 7 \pmod{10}$, we have

$$q = 4p + 5, \quad p = 10k_2 - 3, \quad 2 \mid k_2, \quad 5 = 2 \times 3 - 1.$$

By Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = 1$ since $\lambda_1 = 1; 3$ and $\lambda_2 = 1; 5$. By the assumption, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{5}{p}\right) = -1$, a contradiction again, which proves Claim 5.2.

Claim 5.3. $p \equiv 1, 3, 5 \pmod 7$.

In this case, we choose $r_1 = 7$. If $p \equiv -1 \pmod 7$, then we have the division

$$q = 2p + 7, \quad p = 14k_2 - 1.$$

By Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = 1$ since $\lambda_1 = 0$ and $\lambda_2 = 0$. On the other hand, by the assumption, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{7}{p}\right) = \left(\frac{p}{7}\right) = -1$, a contradiction.

If $p \equiv -3 \pmod 7$, then

$$q = 2p + 7, \quad p = 14k_2 - 3, \quad 7 = 2 \times 3 + 1.$$

Therefore by Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = -1$ since $\lambda_1 = 1; 3$ and $\lambda_2 = 0$, while by the assumption, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{7}{p}\right) = \left(\frac{p}{7}\right) = 1$, again a contradiction.

If $p \equiv -5 \pmod 7$, then

$$q = 2p + 7, \quad p = 14k_2 - 5, \quad 7 = 2 \times 5 - 3, \quad 5 = 2 \times 3 - 1.$$

Therefore by Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = -1$ since $\lambda_1 = 1; 3$ and $\lambda_2 = 0$, while by the assumption, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{7}{p}\right) = \left(\frac{p}{7}\right) = 1$, a contradiction again, which proves Claim 5.3.

By the above three claims, we divide the proof into nine cases. For positive integers k and l, we use $P(k)$ and $Q(l)$ to denote the properties that

$$3^k \mid (p-1) \quad \text{and} \quad 5^l \mid (p-8).$$

Case 5.1: $[p \equiv 1 \pmod 5,\, p \equiv 1 \pmod 3,\, P(2k)] \Rightarrow P(2k+1)$. If $p \equiv 1 \pmod 5$, $p \equiv 1 \pmod{3^{2k}}$, $p \not\equiv 1 \pmod{3^{2k+1}}$, we choose $r_0 = 15 \cdot 3^{2k}$. First we consider the case where $p \equiv 1 + 2 \cdot 3^{2k} \pmod{3^{2k+1}}$. Then $p \equiv 1 - 10 \cdot 3^{2k}$

(mod $10\cdot 3^{2k+1}$). We have

$$q = 2p + 15\cdot 3^{2k},\qquad p = 10\cdot 3^{2k+1}k_2 - (10\cdot 3^{2k}-1),$$
$$15\cdot 3^{2k} = 2(10\cdot 3^{2k}-1) - (5\cdot 3^{2k}-2),\qquad 10\cdot 3^{2k}-1 = 2(5\cdot 3^{2k}-2)+3,$$
$$5\cdot 3^{2k}-2 = 6k_5+1,\qquad 2\nmid k_5.$$

By Corollary 2.3, $\big(\frac{P_q}{P_p}\big) = -1$ since $\lambda_1 = 1; 3$ and $\lambda_2 = 0$. By the assumption, $\big(\frac{P_q}{P_p}\big) = \big(\frac{q}{p}\big) = \big(\frac{15}{p}\big) = 1$, a contradiction.

Next we consider the case where $p \equiv 1 - 2\cdot 3^{2k} \pmod{3^{2k+1}}$, hence $p \equiv 1 + 10\cdot 3^{2k} \pmod{10\cdot 3^{2k+1}}$, and so

$$q = 2p + 15\cdot 3^{2k},\qquad p = 10\cdot 3^{2k+1}k_2 + (10\cdot 3^{2k}+1),$$
$$15\cdot 3^{2k} = 2(10\cdot 3^{2k}+1) - (5\cdot 3^{2k}+2),\qquad 10\cdot 3^{2k}+1 = 2(5\cdot 3^{2k}+2)-3,$$
$$5\cdot 3^{2k}+2 = 6k_5-1,\qquad 2\mid k_5.$$

By Corollary 2.3, $\big(\frac{P_q}{P_p}\big) = -1$ since $\lambda_1 = 1; 10\cdot 3^{2k}+1$ and $\lambda_2 = 0$. On the other hand, $\big(\frac{P_q}{P_p}\big) = \big(\frac{q}{p}\big) = \big(\frac{15}{p}\big) = 1$, again a contradiction.

Case 5.2: $[p \equiv 3 \pmod 5,\ p \equiv 1 \pmod 3,\ 2\mid k,\ P(2k)] \Rightarrow P(2k+1)$. Choose $r_0 = 15\cdot 3^{2k}$. We first consider the case where $p \equiv 1 + 2\cdot 3^{2k} \pmod{3^{2k+1}}$. Then $p \equiv 1 + 2\cdot 3^{2k} \pmod{10\cdot 3^{2k+1}}$, and so

$$q = 2p + 15\cdot 3^{2k},\qquad p = 10\cdot 3^{2k+1}k_2 + (2\cdot 3^{2k}+1),$$
$$15\cdot 3^{2k} = 8(2\cdot 3^{2k}+1) - (3^{2k}+8),\qquad 2\cdot 3^{2k}+1 = 2(3^{2k}+8)-15,$$
$$3^{2k}+8 = 30k_5-1,\qquad 2\nmid k_5.$$

By Corollary 2.3, $\big(\frac{P_q}{P_p}\big) = 1$ since $\lambda_1 = 0$ and $\lambda_2 = 0$, while by the assumption, $\big(\frac{P_q}{P_p}\big) = \big(\frac{q}{p}\big) = \big(\frac{15}{p}\big) = -1$, a contradiction.

Next we consider the case where $p \equiv 1 - 2\cdot 3^{2k} \pmod{3^{2k+1}}$. It follows that $p \equiv 1 - 8\cdot 3^{2k} \pmod{10\cdot 3^{2k+1}}$, and so

$$q = 2p + 15\cdot 3^{2k},\qquad p = 10\cdot 3^{2k+1}k_2 - (8\cdot 3^{2k}-1),$$
$$15\cdot 3^{2k} = 2(8\cdot 3^{2k}-1) - (3^{2k}-2),\qquad 8\cdot 3^{2k}-1 = 8(3^{2k}-2)+15,$$
$$3^{2k}-2 = 30k_5-11,\qquad 15-11-7-3-1.$$

Therefore by Corollary 2.3, $\big(\frac{P_q}{P_p}\big) = 1$ since $\lambda_1 = 2; 11, 3$ and $\lambda_2 = 0$. By the assumption, $\big(\frac{P_q}{P_p}\big) = \big(\frac{q}{p}\big) = \big(\frac{15}{p}\big) = -1$, a contradiction again.

Case 5.3: $[p \equiv 3 \pmod 5,\ p \equiv 1 \pmod 3,\ 2\nmid k,\ P(2k)] \Rightarrow P(2k+1)$. Choosing $r_0 = 15\cdot 3^{2k}$, first we consider the case where $p \equiv 1 + 2\cdot 3^{2k}$

(mod 3^{2k+1}). Then $p \equiv 1 + 8 \cdot 3^{2k} \pmod{10 \cdot 3^{2k+1}}$ and so

$$q = 2p + 15 \cdot 3^{2k}, \quad p = 10 \cdot 3^{2k+1}k_2 + (8 \cdot 3^{2k} + 1),$$
$$15 \cdot 3^{2k} = 2(8 \cdot 3^{2k} + 1) - (3^{2k} + 2), \quad 8 \cdot 3^{2k} + 1 = 8(3^{2k} + 2) - 15,$$
$$3^{2k} + 2 = 30k_5 + 11, \quad 2 \mid k_5, \quad 15 - 11 - 7 - 3 - 1.$$

By Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = 1$ since $\lambda_1 = 2; 11, 3$ and $\lambda_2 = 0$, while by the assumption, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{15}{p}\right) = -1$, a contradiction.

Next we consider the case where $p \equiv 1 - 2 \cdot 3^{2k} \pmod{3^{2k+1}}$, hence $p \equiv 1 - 2 \cdot 3^{2k} \pmod{10 \cdot 3^{2k+1}}$. We have

$$q = 2p + 15 \cdot 3^{2k}, \quad p = 10 \cdot 3^{2k+1}k_2 - (2 \cdot 3^{2k} - 1),$$
$$15 \cdot 3^{2k} = 8(2 \cdot 3^{2k} - 1) - (3^{2k} - 8), \quad 2 \cdot 3^{2k} - 1 = 2(3^{2k} - 8) + 15,$$
$$3^{2k} - 8 = 30k_5 + 1.$$

By Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = 1$ since $\lambda_1 = 0$ and $\lambda_2 = 0$. On the other hand, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{15}{p}\right) = -1$, a contradiction again.

Case 5.4: $[p \equiv 1 \pmod 3, P(2k-1)] \Rightarrow P(2k)$. Choosing $r_0 = 3^{2k}$, first we consider the case where $p \equiv 1 + 2 \cdot 3^{2k-1} \pmod{3^{2k}}$. We have

$$q = 4p + 3^{2k}, \quad p = 2 \cdot 3^{2k}k_2 + (2 \cdot 3^{2k-1} + 1),$$
$$3^{2k} = 2(2 \cdot 3^{2k-1} + 1) - (3^{2k-1} + 2), \quad 2 \cdot 3^{2k-1} + 1 = 2(3^{2k} + 2) - 3,$$
$$3^{2k-1} + 2 = 6k_5 - 1, \quad 2 \nmid k_5.$$

By Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = -1$ since $\lambda_1 = 1; 3$ and $\lambda_2 = 0$, while by the assumption, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = 1$, a contradiction.

Next we consider the case where $p \equiv 1 - 2 \cdot 3^{2k} \pmod{3^{2k+1}}$. We have

$$q = 4p + 3^{2k}, \quad p = 2 \cdot 3^{2k}k_2 - (2 \cdot 3^{2k-1} - 1),$$
$$3^{2k} = 2(2 \cdot 3^{2k-1} - 1) - (3^{2k-1} - 2), \quad 2 \cdot 3^{2k-1} - 1 = 2(3^{2k-1} - 2) + 3,$$
$$3^{2k-1} - 2 = 6k_5 + 1, \quad 2 \mid k_5.$$

Therefore by Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = -1$ since $\lambda_1 = 1; 2 \cdot 3^{2k-1} - 1$ and $\lambda_2 = 0$. By the assumption, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = 1$, again a contradiction.

Case 5.5: $p \equiv -1 \pmod 3$, $p \equiv 1 \pmod 5$. Choosing $r_0 = 15$, we have

$$q = 2p + 15, \quad p = 30k_2 + 11, \quad 2 \mid k_2, \quad 15 - 11 - 7 - 3 - 1.$$

Therefore by Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = 1$ since $\lambda_1 = 2; 11, 3$ and $\lambda_2 = 0$. By the assumption, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{15}{p}\right) = \left(\frac{p}{15}\right) = -1$, a contradiction.

Case 5.6: $p \equiv -1 \pmod 9$, $p \equiv 3 \pmod 7$. Choosing $r_0 = 63$, we have

$$q = 2p + 63, \quad p = 126k_2 + 17,$$
$$63 = 4 \times 17 - 5, \quad 17 = 4 \times 5 - 3, \quad 5 = 2 \times 3 - 1.$$

Therefore by Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = 1$ since $\lambda_1 = 1; 3$ and $\lambda_2 = 1; 5$. By the assumption, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{63}{p}\right) = \left(\frac{p}{7}\right) = -1$, a contradiction.

Case 5.7: $p \equiv -1 \pmod 3$, $p \equiv 3 \pmod 5$, $p \equiv 5 \pmod 7$. In this case we choose $p \equiv -37 \pmod{105}$,

$$q = 4p + 105, \quad p = 210k_2 - 37, \quad 105 - 37 - 31 - 25 - 19 - 13 - 7 - 1.$$

Therefore by Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = 1$ since $\lambda_1 = 2; 37, 13$ and $\lambda_2 = 0$. By the assumption, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{105}{p}\right) = -1$, a contradiction.

Case 5.8: $[p \equiv 8 \pmod 5,\ p \equiv 1 \pmod 7,\ Q(2k)] \Rightarrow Q(2k+1)$. Otherwise, we have $p \equiv 8 + 5^{2k}, 8 - 5^{2k}, 8 - 3 \cdot 5^{2k}, 8 + 3 \cdot 5^{2k} \pmod{5^{2k+1}}$, so we divide the proof into four subcases.

Subcase 5.8.1: $p \equiv 8 + 3 \cdot 5^{2k} \pmod{5^{2k+1}}$. Since $p \equiv -1 \pmod 3$ and $p \equiv 1 \pmod 7$, we have $p \equiv 63 \cdot 5^{2k} + 8 \pmod{210 \cdot 5^{2k}}$ and

$$q = 4p + 105 \cdot 5^{2k}, \quad p = 210 \cdot 5^{2k} k_2 + (63 \cdot 5^{2k} + 8),$$
$$105 \cdot 5^{2k} = 2(63 \cdot 5^{2k} + 8) - (21 \cdot 5^{2k} + 16),$$
$$63 \cdot 5^{2k} + 8 = 2(21 \cdot 5^{2k} + 16) + (21 \cdot 5^{2k} - 24),$$
$$(21 \cdot 5^{2k} + 16) - (21 \cdot 5^{2k} - 24) - (21 \cdot 5^{2k} - 64) - \cdots$$
$$\cdots - 101 - 61 - 21 - 19 - 17 - 15 - 13 - 11 - 9 - 7 - 5 - 3 - 1.$$

Hence $\lambda_1 = 3; 19, 11, 3$ and $\lambda_2 = 0$; on the other hand, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{105}{p}\right) = 1$, a contradiction.

Subcase 5.8.2: $p \equiv 8 - 3 \cdot 5^{2k} \pmod{5^{2k+1}}$. Since $p \equiv -1 \pmod 3$, we have $p \equiv -3 \cdot 5^{2k} + 8 \pmod{30 \cdot 5^{2k}}$ and

$$q = 2p + 15 \cdot 5^{2k}, \quad p = 30 \cdot 5^{2k} k_2 - (3 \cdot 5^{2k} - 8),$$
$$15 \cdot 5^{2k} = 6(3 \cdot 5^{2k} - 8) - (3 \cdot 5^{2k} - 48),$$
$$3 \cdot 5^{2k} - 8 = 2(3 \cdot 5^{2k} - 48) - (3 \cdot 5^{2k} - 88),$$
$$(3 \cdot 5^{2k} - 8) - (3 \cdot 5^{2k} - 48) - (3 \cdot 5^{2k} - 88) - \cdots - 67 - 27 - 13 - 1.$$

Hence $\lambda_1 = 1; 13$ and $\lambda_2 = 0$; on the other hand, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{15}{p}\right) = 1$, again a contradiction.

Subcase 5.8.3: $p \equiv 8 - 5^{2k} \pmod{5^{2k+1}}$. We have

$$q = 4p + 5^{2k+1}, \quad p = 10 \cdot 5^{2k} k_2 - (5^{2k} - 8), \quad 2 \nmid k_2,$$
$$5^{2k+1} = 6(5^{2k} - 8) - (5^{2k} - 48),$$
$$5^{2k} - 8 = 2(5^{2k} - 48) - (5^{2k} - 88),$$
$$(5^{2k} - 8) - (5^{2k} - 48) - (5^{2k} - 88) - \cdots - 97 - 57 - 17,$$
$$57 = 4 \times 17 - 11, \quad 17 - 11 - 5 - 1.$$

Hence $\lambda_1 = 2; 5^{2k+1}, 5$ and $\lambda_2 = 0$; on the other hand, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{5}{p}\right) = -1$, again a contradiction.

Subcase 5.8.4: $p \equiv 8 + 5^{2k} \pmod{5^{2k+1}}$. Since $p \equiv -1 \pmod 3$ and $p \equiv 1 \pmod 7$, we have $p \equiv 21 \cdot 5^{2k} + 8 \pmod{210 \cdot 5^{2k}}$ and

$$q = 4p + 105 \cdot 5^{2k}, \quad p = 210 \cdot 5^{2k} k_2 + (21 \cdot 5^{2k} + 8),$$
$$105 \cdot 5^{2k} = 4(21 \cdot 5^{2k} + 8) + (21 \cdot 5^{2k} - 32),$$
$$21 \cdot 5^{2k} + 8 = 2(21 \cdot 5^{2k} - 32) - (21 \cdot 5^{2k} - 72),$$
$$(21 \cdot 5^{2k} + 8) - (21 \cdot 5^{2k} - 32) - (21 \cdot 5^{2k} - 72) - \cdots - 93 - 53 - 13,$$
$$53 = 4 \times 13 + 1.$$

Hence $\lambda_1 = 0$ and $\lambda_2 = 1; 21 \cdot 5^{2k} + 8$; on the other hand, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{105}{p}\right) = 1$, a contradiction again.

Case 5.9: $[p \equiv 8 \pmod 5, Q(2k-1)] \Rightarrow Q(2k)$. Otherwise, we have $p \equiv 8 + 5^{2k-1}$, $8 - 5^{2k-1}$, $8 - 3 \cdot 5^{2k-1}$, $8 + 3 \cdot 5^{2k-1} \pmod{5^{2k}}$, so we also divide the proof into four subcases.

Subcase 5.9.1: $p \equiv 8 - 3 \cdot 5^{2k-1} \pmod{5^{2k}}$. We have

$$q = 4p + 5^{2k}, \quad p = 10 \cdot 5^{2k-1} k_2 - (3 \cdot 5^{2k-1} - 8),$$
$$5^{2k} = 2(3 \cdot 5^{2k-1} - 8) - (5^{2k-1} - 16),$$
$$3 \cdot 5^{2k-1} - 8 = 4(5^{2k-1} - 16) - (5^{2k-1} - 56),$$
$$(5^{2k-1} - 16) - (5^{2k-1} - 56) - (5^{2k-1} - 96) - \cdots$$
$$\cdots - 109 - 69 - 29 - 11 - 7 - 3 - 1.$$

Hence $\lambda_1 = 2; 11, 3$ and $\lambda_2 = 1; 5^{2k-1} - 16$; on the other hand, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{25}{p}\right) = 1$, a contradiction.

Subcase 5.9.2: $p \equiv 8 + 3 \cdot 5^{2k-1} \pmod{5^{2k}}$. We have

$$q = 4p + 5^{2k}, \quad p = 2 \cdot 5^{2k} k_2 + (3 \cdot 5^{2k-1} + 8),$$
$$5^{2k} = 2(3 \cdot 5^{2k-1} + 8) - (5^{2k-1} + 16),$$
$$3 \cdot 5^{2k-1} + 8 = 2(5^{2k-1} + 16) + (5^{2k-1} - 24),$$

$$(5^{2k-1}+16)-(5^{2k-1}-24)-(5^{2k-1}-64)-\cdots$$
$$\cdots-101-61-21-19-17-15-13-11-9-7-5-3-1.$$

Hence $\lambda_1=3; 19, 11, 3$ and $\lambda_2=0$; on the other hand, $\left(\frac{P_q}{P_p}\right)=\left(\frac{q}{p}\right)=\left(\frac{25}{p}\right)=1$, a contradiction again.

SUBCASE 5.9.3: $p\equiv 8-5^{2k-1} \pmod{5^{2k}}$. Since $p\equiv -1 \pmod 9$, we have $p\equiv 9\cdot 5^{2k-1}+8 \pmod{90\cdot 5^{2k-1}}$ and

$$q=4p+9\cdot 5^{2k},\quad p=90\cdot 5^{2k-1}k_2+(9\cdot 5^{2k-1}+8),$$
$$45\cdot 5^{2k-1}=4(9\cdot 5^{2k-1}+8)+(9\cdot 5^{2k-1}-32),$$
$$9\cdot 5^{2k-1}+8=2(9\cdot 5^{2k-1}-32)-(9\cdot 5^{2k-1}-72),$$
$$(9\cdot 5^{2k-1}+8)-(9\cdot 5^{2k-1}-32)-(9\cdot 5^{2k-1}-72)-\cdots-93-53-13,$$
$$53=4\times 13+1.$$

Hence $\lambda_1=0$ and $\lambda_2=1; 9\cdot 5^{2k-1}+8$; on the other hand, $\left(\frac{P_q}{P_p}\right)=\left(\frac{q}{p}\right)=\left(\frac{9}{p}\right)=1$, a contradiction again.

SUBCASE 5.9.4: $p\equiv 8+5^{2k-1} \pmod{5^{2k}}$. We have

$$q=4p+5^{2k},\quad p=2\cdot 5^{2k}k_2+(5^{2k-1}+8),$$
$$5^{2k}=4(5^{2k-1}+8)+(5^{2k-1}-32),$$
$$5^{2k-1}+8=2(5^{2k-1}-32)-(5^{2k-1}-72),$$
$$(5^{2k-1}+8)-(5^{2k-1}-32)-(5^{2k-1}-72)-\cdots-93-53-13,$$
$$53=4\times 13+1.$$

Hence $\lambda_1=0$ and $\lambda_2=1; 5^{2k-1}+8$; on the other hand, $\left(\frac{P_q}{P_p}\right)=\left(\frac{q}{p}\right)=\left(\frac{25}{p}\right)=1$, again a contradiction.

4.3. *The case* $p\equiv 3 \pmod 8$. The proof of this case is similar to the case $p\equiv 1 \pmod 8$. For the sake of completeness, we present the details.

CLAIM 6.1. $p\equiv \pm 1 \pmod 9$.

We choose $r_1=9$. Then for $p\equiv \pm 5 \pmod 9$, we have

$$q=4p+9,\quad p=18k_2\pm 5,\quad 9=2\times 5-1.$$

By Corollary 2.3, $\left(\frac{P_q}{P_p}\right)=-1$ since $\lambda_1=1; 5$ and $\lambda_2=0$. On the other hand, by the assumption, $\left(\frac{P_q}{P_p}\right)=\left(\frac{q}{p}\right)=1$, a contradiction.

For $p\equiv \pm 7 \pmod 9$, we have

$$q=4p+9,\quad p=18k_2\pm 7,\quad 9=2\times 7-5,\quad 7=2\times 5-3,\quad 5=2\times 3-1.$$

By Corollary 2.3, $\left(\frac{P_q}{P_p}\right)=-1$ since $\lambda_1=1; 3$ and $\lambda_2=0$. On the other hand, we have $\left(\frac{P_q}{P_p}\right)=\left(\frac{q}{p}\right)=1$, again a contradiction. Claim 6.1 is proved.

Claim 6.2. $p \equiv 1, 3 \pmod 5$.

Now we choose $r_1 = 5$. For $p \equiv -1 \pmod 5$, we have

$$q = 4p + 5, \quad p = 10k_2 - 1, \quad 2 \mid k_2.$$

By Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = -1$ since $\lambda_1 = 0$ and $\lambda_2 = 1; p$. On the other hand, by the assumption, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{5}{p}\right) = 1$, a contradiction.

For $p \equiv 7 \pmod{10}$, we have

$$q = 4p + 5, \quad p = 10k_2 - 3, \quad 2 \mid k_2, \quad 5 = 2 \times 3 - 1.$$

By Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = 1$ since $\lambda_1 = 1; 3$ and $\lambda_2 = 1; p$. By the assumption, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{5}{p}\right) = -1$, a contradiction again, which proves Claim 6.2.

Claim 6.3. $p \equiv 1, 3, 5 \pmod 7$.

In this case, we choose $r_1 = 7$. If $p \equiv -1 \pmod 7$, then we have the division

$$q = 2p + 7, \quad p = 14k_2 - 1.$$

By Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = -1$ since $\lambda_1 = 1; p$ and $\lambda_2 = 0$. On the other hand, by the assumption, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right) = 1$, a contradiction.

If $p \equiv -3 \pmod 7$, then

$$q = 2p + 7, \quad p = 14k_2 - 3, \quad 7 = 2 \times 3 + 1.$$

Therefore by Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = 1$ since $\lambda_1 = 2; p, 3$ and $\lambda_2 = 0$, while by the assumption, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right) = -1$, again a contradiction.

If $p \equiv -5 \pmod 7$, then

$$q = 2p + 7, \quad p = 14k_2 - 5, \quad 7 = 2 \times 5 - 3, \quad 5 = 2 \times 3 - 1.$$

Therefore by Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = 1$ since $\lambda_1 = 1; p, 3$ and $\lambda_2 = 0$, while by the assumption, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right) = -1$, a contradiction again, which proves Claim 6.3.

By the above three claims, we divide the proof into nine cases. For positive integers k and l, we use $P(k)$ and $Q(l)$ to denote the properties that

$$3^k \mid (p - 1) \quad \text{and} \quad 5^l \mid (p - 8).$$

Case 6.1: $[p \equiv 1 \pmod 5,\ p \equiv 1 \pmod 3,\ P(2k)] \Rightarrow P(2k + 1)$. If $p \equiv 1 \pmod 5$, $p \equiv 1 \pmod{3^{2k}}$, $p \not\equiv 1 \pmod{3^{2k+1}}$, we choose $r_0 = 15 \cdot 3^{2k}$. First we consider the case where $p \equiv 1 + 2 \cdot 3^{2k} \pmod{3^{2k+1}}$. Then $p \equiv 1 - 10 \cdot 3^{2k}$

(mod $10\cdot 3^{2k+1}$). We have

$$q=2p+15\cdot 3^{2k},\qquad p=10\cdot 3^{2k+1}k_2-(10\cdot 3^{2k}-1),$$
$$15\cdot 3^{2k}=2(10\cdot 3^{2k}-1)-(5\cdot 3^{2k}-2),\qquad 10\cdot 3^{2k}-1=2(5\cdot 3^{2k}-2)+3,$$
$$5\cdot 3^{2k}-2=6k_5+1,\qquad 2\nmid k_5.$$

By Corollary 2.3, $\left(\frac{P_q}{P_p}\right)=1$ since $\lambda_1=2; p,3$ and $\lambda_2=0$. By the assumption, $\left(\frac{P_q}{P_p}\right)=\left(\frac{q}{p}\right)=\left(\frac{15}{p}\right)=-1$, a contradiction.

Next we consider the case where $p\equiv 1-2\cdot 3^{2k} \pmod{3^{2k+1}}$, hence $p\equiv 1+10\cdot 3^{2k} \pmod{10\cdot 3^{2k+1}}$, and so

$$q=2p+15\cdot 3^{2k},\qquad p=10\cdot 3^{2k+1}k_2+(10\cdot 3^{2k}+1),$$
$$15\cdot 3^{2k}=2(10\cdot 3^{2k}+1)-(5\cdot 3^{2k}+2),\qquad 10\cdot 3^{2k}+1=2(5\cdot 3^{2k}+2)-3,$$
$$5\cdot 3^{2k}+2=6k_5-1,\qquad 2\mid k_5.$$

By Corollary 2.3, $\left(\frac{P_q}{P_p}\right)=1$ since $\lambda_1=1; p, 10\cdot 3^{2k}+1$ and $\lambda_2=0$. On the other hand, $\left(\frac{P_q}{P_p}\right)=\left(\frac{q}{p}\right)=\left(\frac{15}{p}\right)=-1$, again a contradiction.

Case 6.2: $[p\equiv 3 \pmod 5,\ p\equiv 1 \pmod 3,\ 2\mid k,\ P(2k)]\Rightarrow P(2k+1)$. Choosing $r_0=15\cdot 3^{2k}$, we first consider the case where $p\equiv 1+2\cdot 3^{2k}$ (mod 3^{2k+1}). Then $p\equiv 1+2\cdot 3^{2k} \pmod{10\cdot 3^{2k+1}}$, and so

$$q=2p+15\cdot 3^{2k},\qquad p=10\cdot 3^{2k+1}k_2+(2\cdot 3^{2k}+1),$$
$$15\cdot 3^{2k}=8(2\cdot 3^{2k}+1)-(3^{2k}+8),\qquad 2\cdot 3^{2k}+1=2(3^{2k}+8)-15,$$
$$3^{2k}+8=30k_5-1,\qquad 2\nmid k_5.$$

By Corollary 2.3, $\left(\frac{P_q}{P_p}\right)=-1$ since $\lambda_1=1; p$ and $\lambda_2=0$, while by the assumption, $\left(\frac{P_q}{P_p}\right)=\left(\frac{q}{p}\right)=\left(\frac{15}{p}\right)=1$, a contradiction.

Next we consider the case where $p\equiv 1-2\cdot 3^{2k} \pmod{3^{2k+1}}$. It follows that $p\equiv 1-8\cdot 3^{2k} \pmod{10\cdot 3^{2k+1}}$, and so

$$q=2p+15\cdot 3^{2k},\qquad p=10\cdot 3^{2k+1}k_2-(8\cdot 3^{2k}-1),$$
$$15\cdot 3^{2k}=2(8\cdot 3^{2k}-1)-(3^{2k}-2),\qquad 8\cdot 3^{2k}-1=8(3^{2k}-2)+15,$$
$$3^{2k}-2=30k_5-11,\qquad 15-11-7-3-1.$$

Therefore by Corollary 2.3, $\left(\frac{P_q}{P_p}\right)=-1$ since $\lambda_1=3; p, 11, 3$ and $\lambda_2=0$. By the assumption, $\left(\frac{P_q}{P_p}\right)=\left(\frac{q}{p}\right)=\left(\frac{15}{p}\right)=1$, a contradiction again.

Case 6.3: $[p\equiv 3 \pmod 5,\ p\equiv 1 \pmod 3,\ 2\nmid k,\ P(2k)]\Rightarrow P(2k+1)$. Choosing $r_0=15\cdot 3^{2k}$, first we consider the case of $p\equiv 1+2\cdot 3^{2k} \pmod{3^{2k+1}}$.

Then $p \equiv 1 + 8 \cdot 3^{2k} \pmod{10 \cdot 3^{2k+1}}$ and so

$$q = 2p + 15 \cdot 3^{2k}, \quad p = 10 \cdot 3^{2k+1} k_2 + (8 \cdot 3^{2k} + 1),$$
$$15 \cdot 3^{2k} = 2(8 \cdot 3^{2k} + 1) - (3^{2k} + 2), \quad 8 \cdot 3^{2k} + 1 = 8(3^{2k} + 2) - 15,$$
$$3^{2k} + 2 = 30k_5 + 11, \quad 2 \mid k_5, \quad 15 - 11 - 7 - 3 - 1.$$

By Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = -1$ since $\lambda_1 = 3; p, 11, 3$ and $\lambda_2 = 0$, while by the assumption, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{15}{p}\right) = 1$, a contradiction.

Next we consider the case where $p \equiv 1 - 2 \cdot 3^{2k} \pmod{3^{2k+1}}$, hence $p \equiv 1 - 2 \cdot 3^{2k} \pmod{10 \cdot 3^{2k+1}}$. We have

$$q = 2p + 15 \cdot 3^{2k}, \quad p = 10 \cdot 3^{2k+1} k_2 - (2 \cdot 3^{2k} - 1),$$
$$15 \cdot 3^{2k} = 8(2 \cdot 3^{2k} - 1) - (3^{2k} - 8), \quad 2 \cdot 3^{2k} - 1 = 2(3^{2k} - 8) + 15,$$
$$3^{2k} - 8 = 30k_5 + 1.$$

By Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = -1$ since $\lambda_1 = 1; p$ and $\lambda_2 = 0$. On the other hand, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{15}{p}\right) = 1$, a contradiction again.

Subcase 6.4: $[p \equiv 1 \pmod 3,\ P(2k-1)] \Rightarrow P(2k)$. Choosing $r_0 = 3^{2k}$, first we consider the case where $p \equiv 1 + 2 \cdot 3^{2k-1} \pmod{3^{2k}}$. We have

$$q = 4p + 3^{2k}, \quad p = 2 \cdot 3^{2k} k_2 + (2 \cdot 3^{2k-1} + 1),$$
$$3^{2k} = 2(2 \cdot 3^{2k-1} + 1) - (3^{2k-1} + 2), \quad 2 \cdot 3^{2k-1} + 1 = 2(3^{2k} + 2) - 3,$$
$$3^{2k-1} + 2 = 6k_5 - 1, \quad 2 \nmid k_5.$$

By Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = -1$ since $\lambda_1 = 1; 3$ and $\lambda_2 = 0$, while by the assumption, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = 1$, a contradiction.

Next we consider the case where $p \equiv 1 - 2 \cdot 3^{2k} \pmod{3^{2k+1}}$. We have

$$q = 4p + 3^{2k}, \quad p = 2 \cdot 3^{2k} k_2 - (2 \cdot 3^{2k-1} - 1),$$
$$3^{2k} = 2(2 \cdot 3^{2k-1} - 1) - (3^{2k-1} - 2), \quad 2 \cdot 3^{2k-1} - 1 = 2(3^{2k-1} - 2) + 3,$$
$$3^{2k-1} - 2 = 6k_5 + 1, \quad 2 \mid k_5.$$

Therefore by Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = -1$ since $\lambda_1 = 1; 2 \cdot 3^{2k-1}$ and $\lambda_2 = 0$. By the assumption, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = 1$, again a contradiction.

Case 6.5: $p \equiv -1 \pmod 3$, $p \equiv 1 \pmod 5$. Choosing $r_0 = 15$, we have

$$q = 2p + 15, \quad p = 30k_2 + 11, \quad 2 \mid k_2, \quad 15 - 7 - 3 - 1.$$

Therefore by Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = -1$ since $\lambda_1 = 3; p, 11, 3$ and $\lambda_2 = 0$. By the assumption, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{15}{p}\right) = -\left(\frac{p}{15}\right) = 1$, a contradiction.

CASE 6.6: $p \equiv -1 \pmod 9$, $p \equiv 3 \pmod 7$. Choosing $r_0 = 63$, we have

$$q = 2p + 63, \quad p = 126k_2 + 17,$$
$$63 = 4 \times 17 - 5, \quad 17 = 4 \times 5 - 3, \quad 5 = 2 \times 3 - 1.$$

Therefore by Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = -1$ since $\lambda_1 = 2; p, 3$ and $\lambda_2 = 1; 5$. By the assumption, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{63}{p}\right) = -\left(\frac{p}{7}\right) = 1$, a contradiction.

CASE 6.7: $p \equiv -1 \pmod 3$, $p \equiv 3 \pmod 5$, $p \equiv 5 \pmod 7$. In this case we choose $p \equiv -37 \pmod{105}$,

$$q = 4p + 105, \quad p = 210k_2 - 37, \quad 105 - 37 - 31 - 25 - 19 - 13 - 7 - 1.$$

Therefore by Corollary 2.3, $\left(\frac{P_q}{P_p}\right) = 1$ since $\lambda_1 = 2; 37, 13$ and $\lambda_2 = 0$. By the assumption, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{105}{p}\right) = -1$, a contradiction.

CASE 6.8: $[p \equiv 8 \pmod 5,\ p \equiv 1 \pmod 7,\ Q(2k)] \Rightarrow Q(2k+1)$. Otherwise, $p \equiv 8 + 5^{2k}, 8 - 5^{2k}, 8 - 3 \cdot 5^{2k}, 8 + 3 \cdot 5^{2k} \pmod{5^{2k+1}}$, so we divide the proof into four subcases.

SUBCASE 6.8.1: $p \equiv 8 + 3 \cdot 5^{2k} \pmod{5^{2k+1}}$. Since $p \equiv -1 \pmod 3$ and $p \equiv 1 \pmod 7$, we have $p \equiv 63 \cdot 5^{2k} + 8 \pmod{210 \cdot 5^{2k}}$ and

$$q = 4p + 105 \cdot 5^{2k}, \quad p = 210 \cdot 5^{2k} k_2 + (63 \cdot 5^{2k} + 8),$$
$$105 \cdot 5^{2k} = 2(63 \cdot 5^{2k} + 8) - (21 \cdot 5^{2k} + 16),$$
$$63 \cdot 5^{2k} + 8 = 2(21 \cdot 5^{2k} + 16) + (21 \cdot 5^{2k} - 24),$$
$$(21 \cdot 5^{2k} + 16) - (21 \cdot 5^{2k} - 24) - (21 \cdot 5^{2k} - 64) - \cdots$$
$$\cdots - 101 - 61 - 21 - 19 - 17 - 15 - 13 - 11 - 9 - 7 - 5 - 3 - 1.$$

Hence $\lambda_1 = 3; 19, 11, 3$ and $\lambda_2 = 0$; on the other hand, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{105}{p}\right) = 1$, a contradiction.

SUBCASE 6.8.2: $p \equiv 8 - 3 \cdot 5^{2k} \pmod{5^{2k+1}}$. Since $p \equiv -1 \pmod 3$, we have $p \equiv -3 \cdot 5^{2k} + 8 \pmod{30 \cdot 5^{2k}}$ and

$$q = 2p + 15 \cdot 5^{2k}, \quad p = 30 \cdot 5^{2k} k_2 - (3 \cdot 5^{2k} - 8),$$
$$15 \cdot 5^{2k} = 6(3 \cdot 5^{2k} - 8) - (3 \cdot 5^{2k} - 48),$$
$$3 \cdot 5^{2k} - 8 = 2(3 \cdot 5^{2k} - 48) - (3 \cdot 5^{2k} - 88),$$
$$(3 \cdot 5^{2k} - 8) - (3 \cdot 5^{2k} - 48) - (3 \cdot 5^{2k} - 88) - \cdots - 67 - 27 - 13 - 1.$$

Hence $\lambda_1 = 2; p, 13$ and $\lambda_2 = 0$; on the other hand, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{15}{p}\right) = -1$, again a contradiction.

Subcase 6.8.3: $p \equiv 8 - 5^{2k} \pmod{5^{2k+1}}$. We have

$$q = 4p + 5^{2k+1}, \quad p = 10 \cdot 5^{2k} k_2 - (5^{2k} - 8), \quad 2 \mid k_2,$$
$$5^{2k+1} = 6(5^{2k} - 8) - (5^{2k} - 48), \quad 5^{2k} - 8 = 2(5^{2k} - 48) - (5^{2k} - 88),$$
$$(5^{2k} - 8) - (5^{2k} - 48) - (5^{2k} - 88) - \cdots - 97 - 57 - 17,$$
$$57 = 4 \times 17 - 11, \quad 17 - 11 - 5 - 1.$$

Hence $\lambda_1 = 1; 5$ and $\lambda_2 = 1; p$; on the other hand, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{5}{p}\right) = -1$, again a contradiction.

Subcase 6.8.4: $p \equiv 8 + 5^{2k} \pmod{5^{2k+1}}$. Since $p \equiv -1 \pmod 3$ and $p \equiv 1 \pmod 7$, we have $p \equiv 21 \cdot 5^{2k} + 8 \pmod{210 \cdot 5^{2k}}$ and

$$q = 4p + 105 \cdot 5^{2k}, \quad p = 210 \cdot 5^{2k} k_2 + (21 \cdot 5^{2k} + 8),$$
$$105 \cdot 5^{2k} = 4(21 \cdot 5^{2k} + 8) + (21 \cdot 5^{2k} - 32),$$
$$21 \cdot 5^{2k} + 8 = 2(21 \cdot 5^{2k} - 32) - (21 \cdot 5^{2k} - 72),$$
$$(21 \cdot 5^{2k} + 8) - (21 \cdot 5^{2k} - 32) - (21 \cdot 5^{2k} - 72) - \cdots - 93 - 53 - 13,$$
$$53 = 4 \times 13 + 1.$$

Hence $\lambda_1 = 0$ and $\lambda_2 = 1; 21 \cdot 5^{2k} + 8$; on the other hand, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{105}{p}\right) = 1$, a contradiction again.

Case 6.9: $[p \equiv 8 \pmod 5, Q(2k-1)] \Rightarrow Q(2k)$. Otherwise, $p \equiv 8 + 5^{2k-1}, 8 - 5^{2k-1}, 8 - 3 \cdot 5^{2k-1}, 8 + 3 \cdot 5^{2k-1} \pmod{5^{2k}}$, so we also divide the proof into four subcases.

Subcase 6.9.1: $p \equiv 8 - 3 \cdot 5^{2k-1} \pmod{5^{2k}}$. We have

$$q = 4p + 5^{2k}, \quad p = 10 \cdot 5^{2k-1} k_2 - (3 \cdot 5^{2k-1} - 8),$$
$$5^{2k} = 2(3 \cdot 5^{2k-1} - 8) - (5^{2k-1} - 16),$$
$$3 \cdot 5^{2k-1} - 8 = 4(5^{2k-1} - 16) - (5^{2k-1} - 56),$$
$$(5^{2k-1} - 16) - (5^{2k-1} - 56) - (5^{2k-1} - 96) - \cdots$$
$$\cdots - 109 - 69 - 29 - 11 - 7 - 3 - 1.$$

Hence $\lambda_1 = 2; 11, 3$ and $\lambda_2 = 1; 5^{2k-1} - 16$; on the other hand, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{25}{p}\right) = 1$, a contradiction.

Subcase 6.9.2: $p \equiv 8 + 3 \cdot 5^{2k-1} \pmod{5^{2k}}$. We have

$$q = 4p + 5^{2k}, \quad p = 2 \cdot 5^{2k} k_2 + (3 \cdot 5^{2k-1} + 8),$$
$$5^{2k} = 2(3 \cdot 5^{2k-1} + 8) - (5^{2k-1} + 16),$$
$$3 \cdot 5^{2k-1} + 8 = 2(5^{2k-1} + 16) + (5^{2k-1} - 24),$$
$$(5^{2k-1} + 16) - (5^{2k-1} - 24) - (5^{2k-1} - 64) - \cdots$$
$$\cdots - 101 - 61 - 21 - 19 - 17 - 15 - 13 - 11 - 9 - 7 - 5 - 3 - 1.$$

Hence $\lambda_1 = 3; 19, 11, 3$ and $\lambda_2 = 0$; on the other hand, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{25}{p}\right) = 1$, a contradiction again.

SUBCASE 6.9.3: $p \equiv 8 - 5^{2k-1} \pmod{5^{2k}}$. Since $p \equiv -1 \pmod 9$, we have $p \equiv 9 \cdot 5^{2k-1} + 8 \pmod{90 \cdot 5^{2k-1}}$ and

$$\begin{gathered} q = 4p + 9 \cdot 5^{2k}, \quad p = 90 \cdot 5^{2k-1}k_2 + (9 \cdot 5^{2k-1} + 8), \\ 45 \cdot 5^{2k-1} = 4(9 \cdot 5^{2k-1} + 8) + (9 \cdot 5^{2k-1} - 32), \\ 9 \cdot 5^{2k-1} + 8 = 2(9 \cdot 5^{2k-1} - 32) - (9 \cdot 5^{2k-1} - 72), \\ (9 \cdot 5^{2k-1} + 8) - (9 \cdot 5^{2k-1} - 32) - (9 \cdot 5^{2k-1} - 72) - \cdots - 93 - 53 - 13, \\ 53 = 4 \times 13 + 1. \end{gathered}$$

Hence $\lambda_1 = 0$ and $\lambda_2 = 1; 9 \cdot 5^{2k-1} + 8$; on the other hand, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{9}{p}\right) = 1$, a contradiction again.

SUBCASE 6.9.4: $p \equiv 8 + 5^{2k-1} \pmod{5^{2k}}$. We have

$$\begin{gathered} q = 4p + 5^{2k}, \quad p = 2 \cdot 5^{2k}k_2 + (5^{2k-1} + 8), \\ 5^{2k} = 4(5^{2k-1} + 8) + (5^{2k-1} - 32), \\ 5^{2k-1} + 8 = 2(5^{2k-1} - 32) - (5^{2k-1} - 72), \\ (5^{2k-1} + 8) - (5^{2k-1} - 32) - (5^{2k-1} - 72) - \cdots - 93 - 53 - 13, \\ 53 = 4 \times 13 + 1. \end{gathered}$$

Hence $\lambda_1 = 0$ and $\lambda_2 = 1; 5^{2k-1} + 8$; on the other hand, $\left(\frac{P_q}{P_p}\right) = \left(\frac{q}{p}\right) = \left(\frac{25}{p}\right) = 1$, again a contradiction.

Thus we complete the proof of Theorem 1.2.

5. Proof of Theorem 1.4. Assume that $a_k = x^2$ for some odd integer $k > 1$ and some positive integer x. Let p be a prime factor of k. Then

$$\gcd(a_{k/p}, a_k/a_{k/p}) = \gcd(1, p) = 1 \text{ or } p. \tag{5.1}$$

Since

$$a_{k/p} \cdot \frac{a_k}{a_{k/p}} = x^2,$$

it follows from (5.1) that either $a_{k/p} = py^2$ or $a_{k/p} = y^2$ for some positive integer y. If

$$\alpha_1 = \frac{a_{k/p}\sqrt{a} + b_{k/p}\sqrt{b}}{\sqrt{2}} \quad \text{and} \quad \beta_1 = \frac{b_{k/p}\sqrt{b} - a_{k/p}\sqrt{a}}{\sqrt{2}},$$

then α_1 and β_1 are the roots of the quadratic equation

$$X^2 - \sqrt{2b_{k/p}^2 a}\, X - 1 = 0,$$

and

$$P_p = \frac{a_k}{a_{k/p}} = \frac{\alpha_1^p - \beta_1^p}{\alpha_1 - \beta_1}$$

is the pth term of the Lehmer sequence defined by $L = 2b_{k/p}^2 b$ and $M = -1$. Since $(L, M) \equiv (2, 3) \pmod 4$, by Theorems 1.1 and 1.2, the equation $P_p = y^2$ is impossible, while the equation $P_p = py^2$ implies $p = 3$. This implies that $p = 3$ is the only prime divisor of k, say $k = 3^t$ for some positive integer t.

If $t > 1$, since $a_{k/3} = 3z^2$, we have

$$a_{k/9} \cdot \frac{a_{k/3}}{a_{k/9}} = 3z^2;$$

it follows that $a_{k/9} = h^2$ for some positive integer h, and so $a_3 = 3u^2$, $a_9/a_3 = 3v^2$ by repeating the above argument and by Theorems 1.1 and 1.2. Hence

$$3v^2 = a_9/a_3 = 2a_3^2 a - 1 = 18u^2 a - 1,$$

which is impossible by modulo 3.

If $t = 1$, we have $a_1 = 3h^2, a_3/a_1 = 3t^2$. Since

$$\frac{a_3}{a_1} = \frac{aa_1^2 + 3bb_1^2}{2} = 18ah^2 - 3 = 3t^2,$$

upon division by 3 one obtains $6ah^2 - 1 = t^2$, which is not possible modulo 3. This completes the proof of Theorem 1.4.

Acknowledgments. Research of P. Z. Yuan was supported by the Guangdong Provincial Natural Science Foundation (No. 8151027501000114) and NSF of China (No. 10571180).

References

[1] S. Akhtari, A. Togbé and P. G. Walsh, *On the equation* $aX^4 - bY^2 = 2$, Acta Arith. 131 (2008), 145–169.

[2] —, —, —, *Addendum on the equation* $aX^4 - bY^2 = 2$, ibid. 137 (2009), 199–202.

[3] J. H. E. Cohn, *On square Fibonacci numbers*, J. London Math. Soc. 39 (1964), 537–540.

[4] —, *Squares in some recurrent sequences*, Pacific J. Math. 41 (1972), 631–646.

[5] D. H. Lehmer, *An extended theory of Lucas functions*, Ann. of Math. 31 (1930), 419–438.

[6] W. Ljunggren, *Einige Eigenschaften der Einheiten reeller quadratischer und reinbiquadratischer Zahl-Körper usw*, Oslo Vid.-Akad. Skrifter, 1936, no. 12.

[7] —, *Über die Gleichung* $x^4 - Dy^2 = 1$, Arch. Math. Naturvid. 45 (1942), 61–70.

[8] —, *Ein Satz ber die diophantische Gleichung* $Ax^2 - By^4 = C$ $(C = 1, 2, 4)$, in: Tolfte Skandinaviska Matematikerkongressen (Lund, 1953), Lunds Univ. Mat. Inst., Lund, 1954, 188–194.

[9] W. Ljunggren, *On the diophantine equation* $Ax^4 - By^2 = C$ $(C = 1, 4)$, Math. Scand. 21 (1967), 149–158.
[10] F. Luca and P. G. Walsh, *Squares in Lehmer sequences and some Diophantine applications*, Acta Arith. 100 (2001), 47–62.
[11] A. Rotkiewicz, *Applications of Jacobi's symbol to Lehmer's numbers*, ibid. 42 (1983), 163–187.
[12] W. Sierpiński, *Elementary Theory of Numbers*, PWN, Warszawa, 1964.
[13] P. M. Voutier, *A further note on "On the equation* $aX^4 - bY^2 = 2$*"*, Acta Arith. 137 (2009), 203–206.
[14] P. G. Walsh, *Diophantine equations of the form* $aX^4 - bY^2 = 1$, in: Algebraic Number Theory and Diophantine Analysis (Graz, 1998), de Gruyter, Berlin, 2000, 531–554.
[15] P. Yuan, *A note on the divisibility of the generalized Lucas sequences*, Fibonacci Quart. 40 (2002), 153–156.

School of Mathematics
South China Normal University
Guangzhou 510631, P.R. China
E-mail: mcsypz@mail.sysu.edu.cn

Mathematics Department
Winston-Salem State University
Winston-Salem, NC 27110, U.S.A.
E-mail: yuanli7983@gmail.com

Received on 6.11.2008
and in revised form on 11.1.2009 (5849)