ACTA ARITHMETICA
XLII (1983)

Applications of Jacobi's symbol to Lehmer's numbers

by

A. Rotkiewicz (Warszawa)

Introduction. The purpose of this paper is to carry over some ideas included in the papers of Chao Ko ([1], [2]) and G. Terjanian [10] to the study of Lehmer's numbers.

Chao Ko and Terjanian prove the insolubility of some diophantine equations. The common idea of their proofs is to evaluate some Jacobi's symbols in two ways: first — without any assumption about the equation and next with the assumption that the equation has a solution. Different results of these calculations prove the impossibility of the given equations.

According to the theorem of G. Terjanian, the equation $x^{2p}+y^{2p}=z^{2p}$, where p is an odd prime, has no integer solutions if $2p\nmid x$ and $2p\nmid y$. In order to prove this theorem G. Terjanian calculates the symbol

$$\left(\frac{A_m(x,y)}{A_n(x,y)}\right), \quad \text{where } 2\nmid mn,\ A_i(x,y)=\frac{x^i-y^i}{x-y},\ 4\mid x-y.$$

Chao Ko, in order to prove that the Catalan equation $x^2-1=y^p$, where p is an odd prime >3, has no integer solutions, calculates the symbol

$$\left(\frac{Q_p(y)}{Q_q(y)}\right), \quad \text{where } Q_n=\frac{y^n-(-1)^n}{y-(-1)}.$$

We shall apply similar ideas to the diophantine equations $P_n=\square$, $P_p=p\square$ (p is an odd prime), where P_n is the Lehmer number.

$$P_n(\alpha,\beta)=\begin{cases}(\alpha^n-\beta^n)/(\alpha-\beta) & \text{for } n \text{ odd},\\ (\alpha^n-\beta^n)/(\alpha^2-\beta^2) & \text{for } n \text{ even},\end{cases}$$

α and β are roots of the trinomial $z^2-\sqrt{L}z+M$, $L>0$ and M are rational integers.

Before the discussion of the solvability of the equations $P_n=\square$, $P_p=p\square$ we calculate in Section 1 the Jacobi symbol $\left(\frac{P_n}{P_m}\right)$ and then

in Section 2 we apply the result of Section 1 to some diophantine equations connected with Lehmer's numbers.

In Section 2 we note also that the proof of Chao Ko's result that the equation $x^2-1=y^p$, where p is a prime >3, has no solution in integers x and y, repeated in the book of Mordell [5], can be simplified and instead of the discussion of 5 cases for the prime number p: $p=8k-1$, $8k+5$, $24k+11$, $24k+19$, $8k+1$ it is enough to consider only two cases for the prime number p: $p=4k+3$ and $p=4k+1$.

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

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

Then (see [9], p. 332) the following formula holds:

$$(2)\qquad \left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{\varepsilon_1 r_1 - 1}{2} + \frac{r_1-1}{2}\cdot\frac{\varepsilon_2 r_2 - 1}{2} + \dots + \frac{r_{l-2}-1}{2}\cdot\frac{\varepsilon_{l-1} r_{l-1} - 1}{2} + \frac{r_{l-1}-1}{2}\cdot\frac{\varepsilon_l r_l - 1}{2}}.$$

Now we shall find a similar formula for the symbol $\left(\frac{P_n}{P_m}\right)$.

THEOREM 1. *We have*

$$(3)\qquad \left(\frac{P_n}{P_m}\right) = (-1)^{\frac{P_m-1}{2}\cdot\frac{\varepsilon_1 P_{r_1}-1}{2} + \frac{P_{r_1}-1}{2}\cdot\frac{\varepsilon_2 P_{r_2}-1}{2} + \dots + \frac{P_{r_{l-1}}-1}{2}\cdot\frac{\varepsilon_l P_{r_l}-1}{2}} \times$$
$$\times \left(\frac{M}{P_m}\right)^{k_1 + \frac{\varepsilon_1 - 1}{2}} \left(\frac{M}{P_{r_1}}\right)^{k_2 + \frac{\varepsilon_2 - 1}{2}} \dots \left(\frac{M}{P_{r_{l-2}}}\right)^{k_{l-1} + \frac{\varepsilon_{l-1} - 1}{2}} \left(\frac{M}{P_{r_{l-1}}}\right)^{k_l + \frac{\varepsilon_l - 1}{2}},$$

where m, n, r_i, ε_i $(i = 1, 2, \dots, l)$ are numbers defined by conditions (1).

It follows from (3) that this formula will be simpler if $\left(\frac{M}{P_n}\right) = 1$. In this case, in order to calculate $\left(\frac{P_n}{P_m}\right)$ it is sufficient to know P_n modulo 4.

THEOREM 2. *Let $2 \nmid mn$, $K = L - 4M > 0$. Then*

$$(4)\qquad \left(\frac{P_n}{P_m}\right) = \left(\frac{n}{m}\right) \qquad \text{if } 4 \mid L,\ M \equiv 1 \pmod 4,\ \left(\frac{L}{M}\right) = 1,$$

$$(5)\qquad \left(\frac{P_n}{P_m}\right) = 1 \qquad \text{if } 4 \mid L,\ M \equiv -1 \pmod 4,\ \left(\frac{L}{M}\right) = 1,$$

$$(6)\qquad \left(\frac{P_n}{P_m}\right) = \left(\frac{n}{m}\right) \qquad \text{if } 4 \mid M,\ L \equiv -1 \pmod 4,\ \left(\frac{M}{L}\right) = 1,$$

$$(7)\qquad \left(\frac{P_n}{P_m}\right) = 1 \qquad \text{if } 4 \mid M,\ L \equiv 1 \pmod 4,\ \left(\frac{M}{L}\right) = 1,$$

$$(8)\qquad \left(\frac{P_n}{P_m}\right) = (-1)^{s + \frac{\varepsilon_{l-1}}{2}} = (-1)^{\lambda} \qquad \text{if } 2 \| M,\ L \equiv 1 \pmod 4,\ \left(\frac{M}{L}\right) = 1,$$

where s is the number of positive ε_i's in the sequence $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{l-1}$ defined by (1), *λ is the number of terms in the expansion $\frac{n}{m} = a_1 + \frac{1}{|a_2|} + \frac{1}{|a_3|} + \dots + \frac{1}{|a_\lambda|}$ into a simple continued fraction with $a_\lambda > 1$,*

$$(9)\qquad \left(\frac{P_n}{P_m}\right) = (-1)^{\sum_{i=1}^{l} \frac{\left(\frac{-2}{r_{i-1}}\right)-1}{2}\cdot\frac{\varepsilon_i\left(\frac{-2}{r_i}\right)-1}{2}}$$

if $2 \| L$, $M \equiv 1 \pmod 4$, $\left(\frac{L}{M}\right) = 1$, $r_0 = m$.

Now we shall prove the following lemma.

LEMMA 1. *Let $2 \nmid n$. We have:*

(a) *If $4 \mid L$, $M \equiv 1 \pmod 4$ then $P_n \equiv n \pmod 4$.*
(b) *If $4 \mid L$, $M \equiv -1 \pmod 4$ then $P_n \equiv 1 \pmod 4$.*
(c) *If $4 \mid M$, $L \equiv -1 \pmod 4$ then $P_n \equiv n \pmod 4$.*
(d) *If $4 \mid M$, $L \equiv 1 \pmod 4$ then $P_n \equiv 1 \pmod 4$.*
(e) *If $2 \| M$, $L \equiv 1 \pmod 4$ then $P_n \equiv -1 \pmod 4$ for $n \geqslant 3$.*
(f) *If $2 \| M$, $L \equiv 3 \pmod 4$ then $P_n \equiv -n \pmod 4$ for $n \geqslant 3$.*
(g) *If $2 \| L$, $M \equiv 1 \pmod 4$ then $P_n \equiv \left(\frac{-2}{n}\right) \pmod 4$ and*

$$P_n \equiv 1 \pmod 4 \qquad \text{if } n \equiv 1, 3 \pmod 8,$$
$$P_n \equiv -1 \pmod 4 \qquad \text{if } n \equiv 5, 7 \pmod 8.$$

(h) *If* $2\|L$, $M \equiv 3 \pmod 4$ *then* $P_n \equiv \left(\frac{2}{n}\right) \pmod 4$ *and*

$$P_n \equiv 1 \pmod 4 \quad \text{if } n \equiv 1, 7 \pmod 8,$$
$$P_n \equiv -1 \pmod 4 \quad \text{if } n \equiv 3, 5 \pmod 8.$$

Proof of Lemma 1. We have $P_0 = 0$, $P_1 = 1$, $P_2 = 1$, $P_3 = L - M$ and we check Lemma 1 directly in all cases for $n = 1, 3$.

Proof of (a). Suppose that $P_n \equiv n \pmod 4$ for an odd n. We have $P_{n+2} = LP_{n+1} - MP_n$, $2n+2 \equiv 0 \pmod 4$ for odd n. Thus $P_{n+2} \equiv 0 \cdot P_{n+1} - -1 \cdot n \equiv n+2 \pmod 4$ and (a) is proved by induction.

Proof of (b). Suppose that $P_n \equiv 1 \pmod 4$ for an odd n. Then, since $L \equiv 0 \pmod 4$, and $M \equiv -1 \pmod 4$ we see that $P_{n+2} = LP_{n+1} - MP_n \equiv 0+1 \equiv 1 \pmod 4$. This implies (b) by induction.

Proof of (c). Suppose that $P_n \equiv n \pmod 4$ for an odd n. From $M \equiv 0 \pmod 4$, $L \equiv -1 \pmod 4$ we obtain $P_{n+2} = LP_{n+1} - MP_n \equiv LP_{n+1} \pmod 4$. But since $P_{n+1} = P_n - MP_{n-1}$, $2n+2 \equiv 0 \pmod 4$ for an odd n we have $P_{n+2} \equiv L(P_n - MP_{n-1}) \equiv LP_n \equiv -n \equiv n+2 \pmod 4$ and (c) is proved by induction.

Proof of (d). Suppose that $P_n \equiv 1 \pmod 4$ for an odd n. From $M \equiv 0 \pmod 4$, $L \equiv 1 \pmod 4$ we obtain $P_{n+2} = LP_{n+1} - MP_n \equiv LP_{n+1} \equiv L(P_n - MP_{n-1}) \equiv LP_n \equiv 1 \cdot 1 \equiv 1 \pmod 4$ and (d) is proved by induction.

Proof of (e). Suppose that $P_n \equiv -1 \pmod 4$ for an odd n. This is true for $n = 3$. Let $n \geqslant 3$, $2 \nmid n$, $M \equiv 2 \pmod 4$, $L \equiv 1 \pmod 4$. We have $P_{n+1} = P_n - MP_{n-1}$ and $P_{n+2} = LP_{n+1} - MP_n = L(P_n - MP_{n-1}) - M(LP_{n-1} - MP_{n-2}) = LP_n - 2MLP_{n-1} + M^2 P_{n-2} \equiv LP_n \equiv 1(-1) \equiv -1 \pmod 4$ and $P_n \equiv -1 \pmod 4$ for every odd $n \geqslant 3$ by induction.

Proof of (f). Let $2\|M$, $L \equiv 3 \pmod 4$. We have $P_3 = L - M \equiv 3 - 2 \equiv -3 \pmod 4$. Suppose that $P_n \equiv -n \pmod 4$ for an odd n. We have $P_{n+2} = LP_n - 2MLP_{n-1} + M^2 P_{n-2}$, $2n+2 \equiv 0 \pmod 4$, $P_{n+2} \equiv LP_n \equiv (-1)(-n) \equiv -(n+2) \pmod 4$ and $P_n \equiv -n \pmod 4$ for every odd $n \geqslant 3$ by induction.

Proof of (g). Let $2\|L$, $M \equiv 1 \pmod 4$, $(L, M) = 1$. First we note that $P_n \equiv 1 \pmod 2$ for odd n. Indeed $P_3 = L - M$ is odd. Suppose that $P_n \equiv 1 \pmod 2$ for an odd n. Then $P_{n+2} = LP_{n+1} - MP_n \equiv 0 - 1 \pmod 2$ and $P_n \equiv 1 \pmod 2$ for every odd n by induction. Thus $LP_n \equiv 2 \pmod 4$ and for every odd $n \geqslant 7$ we have

$$P_{n+2} = LP_n - 2MLP_{n-1} + M^2 P_{n-2} \equiv LP_n + P_{n-2} \equiv 2 + P_{n-2} \equiv 2 + 2 + P_{n-6} \equiv P_{n-6} \pmod 4.$$

Hence

$$P_{8k+r} \equiv P_r \pmod 4 \quad \text{for} \quad k = 0, 1, 2, \ldots$$

Thus it is sufficient to check the formula

$$P_n \equiv \left(\frac{-2}{n}\right) \pmod 4 \quad \text{for} \quad n = 1, 3, 5 \text{ and } 7.$$

We have $P_1 = 1 \equiv \left(\frac{-2}{1}\right) \pmod 4$, $P_3 = L - M \equiv 2 - 1 \equiv 1 \equiv \left(\frac{-2}{3}\right) \pmod 4$, $P_5 \equiv LP_3 + P_1 \equiv 2 + 1 \equiv -1 \equiv \left(\frac{-2}{5}\right) \pmod 4$, $P_7 \equiv LP_5 + P_3 \equiv 2 + 1 \equiv -1 \equiv \left(\frac{-2}{7}\right) \pmod 4$ and (g) is proved.

Proof of (h). Let $2\|L$, $M \equiv 3 \pmod 4$. As in the proof of (g) we have

$$P_{8k+r} \equiv P_r \pmod 4 \quad \text{for} \quad k = 0, 1, 2, \ldots; r = 1, 3, 5, 7.$$

Thus it is sufficient to check that

$$P_n \equiv \left(\frac{2}{n}\right) \pmod 4 \quad \text{for} \quad n = 1, 3, 5 \text{ and } 7.$$

We have

$$P_1 = 1 \equiv \left(\frac{2}{1}\right) \pmod 4, \quad P_3 = L - M \equiv 2 - 3 \equiv -1 \equiv \left(\frac{2}{3}\right) \pmod 4,$$

$$P_5 \equiv LP_3 + P_1 \equiv 2 + 1 \equiv -1 \equiv \left(\frac{2}{5}\right) \pmod 4,$$

$$P_7 \equiv LP_5 + P_3 \equiv 2 - 1 \equiv 1 \equiv \left(\frac{2}{7}\right) \pmod 4$$

and (h) is proved.

LEMMA 2. *Let* $(n, m) = 1$, $2 \nmid mn$, $n = 2km + \varepsilon r$, $\varepsilon = \pm 1$, $2 \nmid r$, *then*

$$\left(\frac{P_n}{P_m}\right) = \left(\frac{\varepsilon P_r}{P_m}\right)\left(\frac{M}{P_m}\right)^{k + \frac{\varepsilon - 1}{2}}. \tag{10}$$

Proof of Lemma 2. From $(n, m) = 1$ it follows that $(P_n, P_m) = P_{(n,m)} = P_1 = 1$.

I. First we consider the case $n = 2km + r$, where $0 < r < m$. We have

$$\frac{\alpha^{2km+r} - \beta^{2km+r}}{\alpha - \beta} = \alpha^r \left(\frac{\alpha^{2km} - \beta^{2km}}{\alpha - \beta}\right) + \beta^{2km} \left(\frac{\alpha^r - \beta^r}{\alpha - \beta}\right),$$

$$\frac{\alpha^{2km+r} - \beta^{2km+r}}{\alpha - \beta} = \beta^r \left(\frac{\alpha^{2km} - \beta^{2km}}{\alpha - \beta}\right) + \alpha^{2km} \left(\frac{\alpha^r - \beta^r}{\alpha - \beta}\right).$$

Hence

$$2P_{2km+r} = \left(\frac{\alpha^r+\beta^r}{\alpha+\beta}\right)\left(\frac{\alpha^{2km}-\beta^{2km}}{\alpha^2-\beta^2}\right)(\alpha+\beta)^2+(\alpha^{2km}+\beta^{2km})P_r.$$

Let

$$v_n = \begin{cases} \dfrac{\alpha^n+\beta^n}{\alpha+\beta} & \text{for } n \text{ odd}, \\ \alpha^n+\beta^n & \text{for } n \text{ even}. \end{cases}$$

Since $v_0 = 2$, $v_1 = 1$ and $v_{n+2} = Lv_{n+1}-Mv_n$ for n even, $v_{n+2} = v_{n+1}-Mv_n$ for n odd, the numbers v_n are rational integers.

We have

$$2P_{2km+r} = v_rP_{2km}L+v_{2km}P_r$$

and from $P_m|P_{2km}$ it follows that

$$\left(\frac{2P_{2km+r}}{P_m}\right) = \left(\frac{\alpha^{2km}+\beta^{2km}}{P_m}\right)\left(\frac{P_r}{P_m}\right). \tag{11}$$

From $\alpha^{km}-\beta^{km} = (\alpha-\beta)P_{km}$ if $2\nmid km$, $\alpha^{km}-\beta^{km} = (\alpha^2-\beta^2)P_{km}$ if $2|km$, $P_m|P_{km}$, $\alpha-\beta = \sqrt{K}$, $(\alpha+\beta) = \sqrt{L}$ it follows that $P_m^2|(\alpha^{km}-\beta^{km})^2$. Thus

$$\left(\frac{\alpha^{2km}+\beta^{2km}}{P_m}\right) = \left(\frac{(\alpha^{km}-\beta^{km})^2+2M^{km}}{P_m}\right) = \left(\frac{2M^{km}}{P_m}\right) = \left(\frac{2}{P_m}\right)\left(\frac{M}{P_m}\right)^{km}$$

and since $2\nmid m$, we have

$$\left(\frac{\alpha^{2km}+\beta^{2km}}{P_m}\right) = \left(\frac{2}{P_m}\right)\left(\frac{M}{P_m}\right)^k. \tag{12}$$

From (11) and (12) it follows that

$$\left(\frac{P_{2km+r}}{P_m}\right) = \left(\frac{P_r}{P_m}\right)\left(\frac{M}{P_m}\right)^k.$$

II. Now we consider the case $\varepsilon = -1$. Then $n = 2km-r$, where $0 < r < m$. We have

$$\frac{\alpha^{2km-r}-\beta^{2km-r}}{\alpha-\beta} = \alpha^{-r}\frac{\alpha^{2km}-\beta^{2km}}{\alpha-\beta}+\beta^{2km}\frac{\alpha^{-r}-\beta^{-r}}{\alpha-\beta},$$

$$\frac{\alpha^{2km-r}-\beta^{2km-r}}{\alpha-\beta} = \beta^{-r}\frac{\alpha^{2km}-\beta^{2km}}{\alpha-\beta}+\alpha^{2km}\frac{\alpha^{-r}-\beta^{-r}}{\alpha-\beta}.$$

Hence

$$2P_{2km-r} = (\alpha^{-r}+\beta^{-r})\frac{\alpha^{2km}-\beta^{2km}}{\alpha-\beta}+(\alpha^{2km}+\beta^{2km})\frac{\alpha^{-r}-\beta^{-r}}{\alpha-\beta}.$$

Thus

$$2(\alpha\beta)^rP_{2km-r} = (\alpha^r+\beta^r)\frac{\alpha^{2km}-\beta^{2km}}{\alpha-\beta}+(\alpha^{2km}+\beta^{2km})\left[-\left(\frac{\alpha^r-\beta^r}{\alpha-\beta}\right)\right],$$

i.e.

$$2(\alpha\beta)^rP_{2km-r} = \left(\frac{\alpha^r+\beta^r}{\alpha+\beta}\right)\left(\frac{\alpha^{2km}-\beta^{2km}}{\alpha^2-\beta^2}\right)(\alpha+\beta)^2+(\alpha^{2km}+\beta^{2km})\left[-\left(\frac{\alpha^r-\beta^r}{\alpha-\beta}\right)\right],$$

and

$$2M^rP_{2km-r} = v_rP_{2km}L+v_{2km}(-P_r). \tag{13}$$

By formula (12) we have $\left(\frac{v_{2km}}{P_m}\right) = \left(\frac{2}{P_m}\right)\left(\frac{M}{P_m}\right)^k$ and since $P_m|P_{2km}$, from formula (13) we get

$$\left(\frac{2}{P_m}\right)\left(\frac{M}{P_m}\right)^r\left(\frac{P_{2km-r}}{P_m}\right) = \left(\frac{2}{P_m}\right)\left(\frac{M}{P_m}\right)^k\left(\frac{-P_r}{P_m}\right).$$

Since $2\nmid r$ we have $\left(\frac{M}{P_m}\right)^r = \left(\frac{M}{P_m}\right)$. Thus

$$\left(\frac{P_{2km-r}}{P_m}\right) = \left(\frac{-P_r}{P_m}\right)\left(\frac{M}{P_m}\right)^k\left(\frac{M}{P_m}\right)^{-1} = \left(\frac{-P_r}{P_m}\right)\left(\frac{M}{P_m}\right)^{k+\frac{\varepsilon-1}{2}}.$$

This completes the proof of Lemma 2.

Now we shall calculate the symbol $\left(\frac{M}{P_m}\right)$. First we shall prove the following

LEMMA 3. *Let* $2|ML$, $(M, L) = 1$, $2\nmid m$. *Then*

(a) *If* $M \equiv 1 \pmod 4$ *or* $4|L$ *then*

$$\left(\frac{M}{P_m}\right) = \left(\frac{L}{M}\right)^{(m-1)/2}. \tag{14}$$

(b) *If* $L \equiv 1 \pmod 4$ *or* $4|M$ *then*

$$\left(\frac{M}{P_m}\right) = \left(\frac{M}{L}\right)^{(m-1)/2}. \tag{15}$$

(c) *If* $2\|M$, $L \equiv 3 \pmod 4$ *then*

$$\left(\frac{M}{P_m}\right) = -\left(\frac{M}{L}\right)^{(m-1)/2}. \tag{16}$$

(d) *If* $2\|L$, $M \equiv 3 \pmod 4$ *then*

$$\left(\frac{M}{P_m}\right) = \left(\frac{2}{m}\right)\left(\frac{L}{M}\right)^{(m-1)/2}. \tag{17}$$

Proof of Lemma 3. Let $M \equiv 1 \pmod 4$. For $m = 3$ we have

$$\left(\frac{M}{P_3}\right) = \left(\frac{M}{L-M}\right) = \left(\frac{L-M}{M}\right) = \left(\frac{L}{M}\right) = \left(\frac{L}{M}\right)^{\frac{3-1}{2}}.$$

Suppose now that formula (14) holds if m is odd and $m \geqslant 3$.

Since $M \equiv 1 \pmod 4$ we have

$$\left(\frac{M}{P_{m+2}}\right) = \left(\frac{P_{m+2}}{M}\right) = \left(\frac{LP_{m+1}-MP_m}{M}\right) = \left(\frac{LP_{m+1}}{M}\right) = \left(\frac{L}{M}\right)\left(\frac{P_{m+1}}{M}\right)$$
$$= \left(\frac{L}{M}\right)\left(\frac{P_m - MP_{m-1}}{M}\right) = \left(\frac{L}{M}\right)\left(\frac{P_m}{M}\right) = \left(\frac{L}{M}\right)\left(\frac{L}{M}\right)^{(m-1)/2}$$
$$= \left(\frac{L}{M}\right)^{((m+2)-1)/2}$$

and formula (14) follows by induction.

Let now $4 \mid L$, $M \equiv -1 \pmod 4$. By Lemma 1 we have $P_n \equiv 1 \pmod 4$ for n odd and

$$\left(\frac{M}{P_3}\right) = \left(\frac{M}{L-M}\right) = \left(\frac{L-M}{M}\right) = \left(\frac{L}{M}\right) = \left(\frac{L}{M}\right)^{\frac{3-1}{2}}.$$

Suppose now that formula (14) holds for an odd m. Since $P_m \equiv 1 \pmod 4$ we have $\left(\frac{M}{P_{m+2}}\right) = \left(\frac{P_{m+2}}{M}\right)$ and in the same way as in the case $M \equiv 1 \pmod 4$ we prove formula (14) for the odd number $m+2$.

Proof of (b). Let $L \equiv 1 \pmod 4$. Note that $\left(\frac{L}{P_n}\right) = \left(\frac{M}{P_n}\right)$ for odd n. Indeed, from the identity $v_n^2 L - KP_n^2 = 4M^n$ it follows that

$$\left(\frac{v_n^2 L - KP_n^2}{P_n}\right) = \left(\frac{4M}{P_n}\right)^n$$

and since $2 \nmid n$ we have $\left(\frac{L}{P_n}\right) = \left(\frac{M}{P_n}\right)$. Thus

$$\left(\frac{M}{P_3}\right) = \left(\frac{L}{P_3}\right) = \left(\frac{P_3}{L}\right) = \left(\frac{L-M}{L}\right) = \left(\frac{M}{L}\right).$$

Suppose now that formula (15) holds for an odd n. Since $\left(\frac{L}{P_n}\right) = \left(\frac{M}{P_n}\right)$,

$L \equiv 1 \pmod 4$ we have

$$\left(\frac{M}{P_{m+2}}\right) = \left(\frac{L}{P_{m+2}}\right) = \left(\frac{P_{m+2}}{L}\right) = \left(\frac{LP_{m+1}-MP_m}{L}\right) = \left(\frac{-MP_m}{L}\right)$$
$$= \left(\frac{M}{L}\right)\left(\frac{P_m}{L}\right) = \left(\frac{M}{L}\right)\left(\frac{L}{P_M}\right) = \left(\frac{M}{L}\right)\left(\frac{M}{P_m}\right) = \left(\frac{M}{L}\right)\left(\frac{M}{L}\right)^{(m-1)/2}$$
$$= \left(\frac{M}{L}\right)^{((m+2)-1)/2}$$

and formula (15) follows for every odd m by induction.

Let now $4 \mid M$. If $L \equiv 1 \pmod 4$ then as we already proved $\left(\frac{M}{P_m}\right) = \left(\frac{M}{L}\right)^{(m-1)/2}$ and it remains to prove formula (15) in the case $4 \mid M$, $L \equiv 3 \pmod 4$.

Let $m = 3$. Then we have

$$\left(\frac{M}{P_3}\right) = \left(\frac{L}{P_3}\right) = \left(\frac{L}{L-M}\right) = -\left(\frac{L-M}{L}\right) = -\left(\frac{-M}{L}\right) = \left(\frac{M}{L}\right).$$

Suppose now that formula (15) holds for an odd $m \geqslant 3$.

We have $\left(\frac{M}{P_{m+2}}\right) = \left(\frac{L}{P_{m+2}}\right)$. Since $4 \mid M$, $L \equiv 3 \pmod 4$, by Lemma 1 we have $P_n \equiv n \pmod 4$. Thus

$$\left(\frac{L}{P_{m+2}}\right) = (-1)^{((m+2)-1)/2}\left(\frac{P_{m+2}}{L}\right) = (-1)^{(m+1)/2}\left(\frac{LP_{m+1}-MP_m}{L}\right)$$
$$= (-1)^{(m+1)/2}\left(\frac{-MP_m}{L}\right) = (-1)^{(m+1)/2}(-1)\left(\frac{M}{L}\right)\left(\frac{P_m}{L}\right)$$
$$= (-1)^{(m+1)/2}(-1)\left(\frac{M}{L}\right)(-1)^{(m-1)/2}\left(\frac{L}{P_m}\right) = (-1)^{m+1}\left(\frac{M}{L}\right)\left(\frac{M}{P_n}\right)$$
$$= (-1)^{m+1}\left(\frac{M}{L}\right)\left(\frac{M}{L}\right)^{(m-1)/2} = \left(\frac{M}{L}\right)\left(\frac{M}{L}\right)^{(m-1)/2} = \left(\frac{M}{L}\right)^{((m+2)-1)/2}$$

and formula (15) follows by induction.

Proof of formula (16). Since $2 \| M$, $L \equiv 3 \pmod 4$ by Lemma 1 we have $P_m \equiv -m \pmod 4$.

Let $m = 3$. Then

$$\left(\frac{M}{P_3}\right) = \left(\frac{M}{L-M}\right) = \left(\frac{L-M}{L}\right) = -\left(\frac{M}{L}\right)$$

and formula (16) holds for $m = 3$.

Suppose now that formula (16) holds for an odd m. By Lemma 1 we have $P_n \equiv -n \pmod 4$ for odd $n \geqslant 3$ and since $L \equiv 3 \pmod 4$ we have

$$\left(\frac{M}{P_{m+2}}\right) = \left(\frac{L}{P_{m+2}}\right) = (-1)^{(-(m+2)-1)/2}\left(\frac{P_{m+2}}{L}\right)$$

$$= (-1)^{(-m-2-1)/2}\left(\frac{LP_{m+1}-MP_m}{L}\right)$$

$$= (-1)^{(-m-2-1)/2}\left(\frac{-MP_m}{L}\right) = (-1)^{(-m-2-1)/2}(-1)\left(\frac{M}{L}\right)\left(\frac{P_m}{L}\right)$$

$$= (-1)^{(-m-2-1)/2}(-1)\left(\frac{M}{L}\right)(-1)^{(-m-1)/2}\left(\frac{L}{P_m}\right) = (-1)^{-m-2}(-1)\left(\frac{M}{L}\right)\left(\frac{M}{P_m}\right)$$

$$= (-1)^{-m-1}\left(\frac{M}{L}\right)(-1)\left(\frac{M}{L}\right)^{(m-1)/2} = -\left(\frac{M}{L}\right)^{((m+2)-1)/2}.$$

This implies formula (16) by induction.

Proof of (d). For $m = 1$ formula (17) holds. Let $m = 3$. We have

$$\left(\frac{M}{P_3}\right) = \left(\frac{M}{L-M}\right) = -\left(\frac{L-M}{M}\right) = -\left(\frac{L}{M}\right) = \left(\frac{2}{3}\right)\left(\frac{L}{M}\right).$$

Suppose now that formula (17) holds for an odd n. By Lemma 1 we have $P_n \equiv \left(\frac{2}{n}\right) \pmod 4$ for odd n. Thus

$$\left(\frac{M}{P_{m+2}}\right) = (-1)^{\frac{\left(\frac{2}{m+2}\right)-1}{2}}\left(\frac{P_{m+2}}{M}\right) = (-1)^{\frac{\left(\frac{2}{m+2}\right)-1}{2}}\left(\frac{LP_{m+1}-MP_m}{M}\right)$$

$$= (-1)^{\frac{\left(\frac{2}{m+2}\right)-1}{2}}\left(\frac{L}{M}\right)\left(\frac{P_{m+1}}{M}\right) = (-1)^{\frac{\left(\frac{2}{m+2}\right)-1}{2}}\left(\frac{L}{M}\right)\left(\frac{P_m-MP_{m-1}}{M}\right)$$

$$= (-1)^{\frac{\left(\frac{2}{m+2}\right)-1}{2}}\left(\frac{L}{M}\right)\left(\frac{P_m}{M}\right) = (-1)^{\frac{\left(\frac{2}{m+2}\right)-1}{2}}\left(\frac{L}{M}\right)(-1)^{\frac{\left(\frac{2}{m}\right)-1}{2}}\left(\frac{M}{P_m}\right)$$

$$= (-1)^{\frac{\left(\frac{2}{m+2}\right)+\left(\frac{2}{m}\right)-2}{2}}\left(\frac{L}{M}\right)\left(\frac{2}{m}\right)\left(\frac{L}{M}\right)^{\frac{m-1}{2}}$$

$$= (-1)^{\frac{\left(\frac{2}{m+2}\right)+\left(\frac{2}{m}\right)-2}{2}}\left(\frac{2}{m}\right)\left(\frac{L}{M}\right)^{\frac{(m+2)-1}{2}}$$

and it remains to check the formula

$$(18)\qquad (-1)^{\frac{\left(\frac{2}{m+2}\right)+\left(\frac{2}{m}\right)-2}{2}}\left(\frac{2}{m}\right) = \left(\frac{2}{m+2}\right).$$

Since $\left(\frac{2}{m+2}\right) = \left(\frac{2}{m}\right)(-1)^{(m+1)/2}$ to prove (18) it is enough to check that

$$(-1)^{\frac{\left(\frac{2}{m}\right)(1+(-1)^{(m+1)/2})-2}{2}} = (-1)^{\frac{m+1}{2}}.$$

The latter formula is true because if $m \equiv 3 \pmod 4$ then $(-1)^{\frac{\left(\frac{2}{m}\right)\cdot 2-2}{2}} = 1$ and if $m \equiv 1 \pmod 4$ then $(-1)^{\frac{\left(\frac{2}{m}\right)\cdot 0-2}{2}} = -1$. This completes the proof of Lemma 3.

Corollary 1. *Let* $2 \nmid m$, $(L, M) = 1$. *If*

$$2 \mid M \quad \text{and} \quad L \equiv 1 \pmod 4, \quad \left(\frac{M}{L}\right) = 1 \text{ or}$$

$$2 \mid L \quad \text{and} \quad M \equiv 1 \pmod 4, \quad \left(\frac{L}{M}\right) = 1 \text{ or}$$

$$4 \mid L \quad \text{and} \quad \left(\frac{L}{M}\right) = 1 \quad \text{or} \quad 4 \mid M \quad \text{and} \quad \left(\frac{M}{L}\right) = 1$$

then $\left(\frac{M}{P_m}\right) = 1$.

Proof of Corollary 1. By Lemma 3 we have

$$\left(\frac{M}{P_m}\right) = \left(\frac{L}{M}\right)^{\frac{m-1}{2}} \quad \text{or} \quad \left(\frac{M}{P_m}\right) = \left(\frac{M}{L}\right)^{\frac{m-1}{2}}$$

and since $\left(\frac{M}{L}\right) = 1$ for even M and $\left(\frac{L}{M}\right) = 1$ for even L we have $\left(\frac{M}{P_m}\right) = 1$. This completes the proof of Corollary 1.

Proof of Theorem 1. From equations (1) and Lemma 2 it follows that

$$\left(\frac{P_n}{P_m}\right)=\left(\frac{\varepsilon_1 P_{r_1}}{P_m}\right)\left(\frac{M}{P_m}\right)^{k_1+\frac{\varepsilon_1-1}{2}},$$

$$\left(\frac{P_m}{P_{r_1}}\right)=\left(\frac{\varepsilon_2 P_{r_2}}{P_{r_1}}\right)\left(\frac{M}{P_{r_1}}\right)^{k_2+\frac{\varepsilon_2-1}{2}},$$

$$\left(\frac{P_{r_1}}{P_{r_2}}\right)=\left(\frac{\varepsilon_3 P_{r_3}}{P_{r_2}}\right)\left(\frac{M}{P_{r_2}}\right)^{k_3+\frac{\varepsilon_3-1}{2}},$$

(19) $$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\left(\frac{P_{r_{l-3}}}{P_{r_{l-2}}}\right)=\left(\frac{\varepsilon_{l-1}P_{r_{l-1}}}{P_{r_{l-2}}}\right)\left(\frac{M}{P_{r_{l-2}}}\right)^{k_{l-1}+\frac{\varepsilon_{l-1}-1}{2}},$$

$$\left(\frac{P_{r_{l-2}}}{P_{r_{l-1}}}\right)=\left(\frac{\varepsilon_l P_{r_l}}{P_{r_{l-1}}}\right)\left(\frac{M}{P_{r_{l-1}}}\right)^{k_l+\frac{\varepsilon_l-1}{2}}.$$

Since

$$\left(\frac{a}{b}\right)=(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}+\frac{\operatorname{sgn}a-1}{2}\cdot\frac{\operatorname{sgn}b-1}{2}}\left(\frac{b}{a}\right),$$

$$\left(\frac{a}{b}\right)=\left(\frac{a}{|b|}\right)\quad\text{for } ab \text{ odd},$$

$$P_i>0\quad(\text{because } K=L-4M>0)$$

it follows from formulae (19) that

$$\left(\frac{P_n}{P_m}\right)=\left(\frac{\varepsilon_1 P_{r_1}}{P_m}\right)\left(\frac{M}{P_m}\right)^{k_1+\frac{\varepsilon_1-1}{2}}$$

$$=(-1)^{\frac{P_m-1}{2}\cdot\frac{\varepsilon_1 P_{r_1}-1}{2}}\left(\frac{P_m}{P_{r_1}}\right)\left(\frac{M}{P_m}\right)^{k_1+\frac{\varepsilon_1-1}{2}}$$

$$=(-1)^{\frac{P_m-1}{2}\cdot\frac{\varepsilon_1 P_{r_1}-1}{2}}\left(\frac{\varepsilon_2 P_{r_2}}{P_{r_1}}\right)\left(\frac{M}{P_{r_1}}\right)^{k_2+\frac{\varepsilon_2-1}{2}}\left(\frac{M}{P_m}\right)^{k_1+\frac{\varepsilon_1-1}{2}}$$

$$=(-1)^{\frac{P_m-1}{2}\cdot\frac{\varepsilon_1 P_{r_1}-1}{2}+\frac{P_{r_1}-1}{2}\cdot\frac{\varepsilon_2 P_{r_2}-1}{2}}\left(\frac{P_{r_1}}{P_{r_2}}\right)\left(\frac{M}{P_{r_1}}\right)^{k_2+\frac{\varepsilon_2-1}{2}}\left(\frac{M}{P_m}\right)^{k_1+\frac{\varepsilon_1-1}{2}}$$

$$=(-1)^{\frac{P_m-1}{2}\cdot\frac{\varepsilon_1 P_{r_1}-1}{2}+\frac{P_{r_1}-1}{2}\cdot\frac{\varepsilon_2 P_{r_2}-1}{2}+\ldots+\frac{P_{r_{l-2}}-1}{2}\cdot\frac{\varepsilon_{l-1}P_{r_{l-1}}-1}{2}}\times$$

$$\times\left(\frac{P_{r_{l-2}}}{P_{r_{l-1}}}\right)\left(\frac{M}{P_{r_{l-2}}}\right)^{k_{l-1}+\frac{\varepsilon_{l-1}-1}{2}}\cdots\left(\frac{M}{P_{r_1}}\right)^{k_2+\frac{\varepsilon_2-1}{2}}\left(\frac{M}{P_m}\right)^{k_1+\frac{\varepsilon_1-1}{2}}$$

$$=(-1)^{\frac{P_m-1}{2}\cdot\frac{\varepsilon_1 P_{r_1}-1}{2}+\frac{P_{r_1}-1}{2}\cdot\frac{\varepsilon_2 P_{r_2}-1}{2}+\ldots+\frac{P_{r_{l-2}}-1}{2}\cdot\frac{\varepsilon_{l-1}P_{r_{l-1}}-1}{2}}\times$$

$$\times\left(\frac{\varepsilon_l P_{r_l}}{P_{r_{l-1}}}\right)\left(\frac{M}{P_{r_{l-1}}}\right)^{k_l+\frac{\varepsilon_l-1}{2}}\left(\frac{M}{P_{r_{l-2}}}\right)^{k_{l-1}+\frac{\varepsilon_{l-1}-1}{2}}\cdots\left(\frac{M}{P_{r_1}}\right)^{k_2+\frac{\varepsilon_2-1}{2}}\left(\frac{M}{P_m}\right)^{k_1+\frac{\varepsilon_1-1}{2}}$$

$$=(-1)^{\frac{P_m-1}{2}\cdot\frac{\varepsilon_1 P_{r_1}-1}{2}+\frac{P_{r_1}-1}{2}\cdot\frac{\varepsilon_2 P_{r_2}-1}{2}+\ldots+\frac{P_{r_{l-2}}-1}{2}\cdot\frac{\varepsilon_{l-1}P_{r_{l-1}}-1}{2}+\frac{P_{r_{l-1}}-1}{2}\cdot\frac{\varepsilon_l P_{r_l}-1}{2}}\times$$

$$\times\left(\frac{P_{r_{l-1}}}{P_{r_l}}\right)\left(\frac{M}{P_{r_{l-1}}}\right)^{k_l+\frac{\varepsilon_l-1}{2}}\left(\frac{M}{P_{r_{l-2}}}\right)^{k_{l-1}+\frac{\varepsilon_{l-1}-1}{2}}\cdots\left(\frac{M}{P_{r_1}}\right)^{k_2+\frac{\varepsilon_2-1}{2}}\left(\frac{M}{P_m}\right)^{k_1+\frac{\varepsilon_1-1}{2}}.$$

Since

$$\left(\frac{P_{r_{l-1}}}{P_{r_l}}\right)=\left(\frac{P_{r_{l-1}}}{1}\right)=1$$

we have

$$\left(\frac{P_n}{P_m}\right)$$

$$=(-1)^{\frac{P_m-1}{2}\cdot\frac{\varepsilon_1 P_{r_1}-1}{2}+\frac{P_{r_1}-1}{2}\cdot\frac{\varepsilon_2 P_{r_2}-1}{2}+\ldots+\frac{P_{r_{l-2}}-1}{2}\cdot\frac{\varepsilon_{l-1}P_{r_{l-1}}-1}{2}+\frac{P_{r_{l-1}}-1}{2}\cdot\frac{\varepsilon_l P_{r_l}-1}{2}}\times$$

$$\times\left(\frac{M}{P_m}\right)^{k_1+\frac{\varepsilon_1-1}{2}}\left(\frac{M}{P_{r_1}}\right)^{k_2+\frac{\varepsilon_2-1}{2}}\cdots\left(\frac{M}{P_{r_{l-2}}}\right)^{k_{l-1}+\frac{\varepsilon_{l-1}-1}{2}}\left(\frac{M}{P_{r_{l-1}}}\right)^{k_l+\frac{\varepsilon_l-1}{2}}.$$

This completes the proof of Theorem 1.

If now $2\nmid m$, $(L, M)=1$, $2\mid M$ and $L\equiv 1 \pmod 4$, $\left(\frac{M}{L}\right)=1$ or $2\mid L$ and $M\equiv 1 \pmod 4$, $\left(\frac{L}{M}\right)=1$ or $4\mid L$, $\left(\frac{L}{M}\right)=1$ or $4\mid M$, $\left(\frac{M}{L}\right)=1$ then by Corollary 1 we have $\left(\frac{M}{P_m}\right)=1$ and from formula (3) we obtain the formula

$$\left(\frac{P_n}{P_m}\right)=(-1)^{\frac{P_m-1}{2}\cdot\frac{\varepsilon_1 P_{r_1}-1}{2}+\frac{P_{r_1}-1}{2}\cdot\frac{\varepsilon_2 P_{r_2}-1}{2}+\ldots+\frac{P_{r_{l-1}}-1}{2}\cdot\frac{\varepsilon_l P_{r_l}-1}{2}}. \tag{20}$$

Proof of Theorem 2. First we consider the case $4\mid L$, $M\equiv 1 \pmod 4$, $\left(\frac{L}{M}\right)=1$ or $4\mid M$, $L\equiv 3 \pmod 4$, $\left(\frac{M}{L}\right)=1$. By Lemma 1 we have $P_n\equiv n \pmod 4$. Thus

$$\frac{P_m-1}{2}\cdot\frac{\varepsilon_1 P_{r_1}-1}{2}\equiv\frac{m-1}{2}\cdot\frac{\varepsilon_1 r_1-1}{2} \pmod 2,$$

$$\frac{P_{r_1}-1}{2}\cdot\frac{\varepsilon_2 P_{r_2}-1}{2}\equiv\frac{r_1-1}{2}\cdot\frac{\varepsilon_2 r_2-1}{2} \pmod 2,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\frac{P_{r_{l-1}}-1}{2}\cdot\frac{\varepsilon_l P_{r_l}-1}{2}\equiv\frac{r_{l-1}-1}{2}\cdot\frac{\varepsilon_l r_l-1}{2} \pmod 2$$

and from formula (20) we get

$$\left(\frac{P_n}{P_m}\right)=(-1)^{\frac{m-1}{2}\cdot\frac{\varepsilon_1 r_1-1}{2}+\frac{r_1-1}{2}\cdot\frac{\varepsilon_2 r_2-1}{2}+\ldots+\frac{r_{l-1}-1}{2}\cdot\frac{\varepsilon_l r_l-1}{2}}.$$

By formula (2) we have

$$\left(\frac{n}{m}\right)=(-1)^{\frac{m-1}{2}\cdot\frac{\varepsilon_1 r_1-1}{2}+\frac{r_1-1}{2}\cdot\frac{\varepsilon_2 r_2-1}{2}+\ldots+\frac{r_{l-1}-1}{2}\cdot\frac{\varepsilon_l r_l-1}{2}}.$$

Thus $\left(\frac{P_n}{P_m}\right)=\left(\frac{n}{m}\right)$.

Now let $4\mid L$, $M\equiv -1 \pmod 4$, $\left(\frac{L}{M}\right)=1$ or $4\mid M$, $L\equiv 1 \pmod 4$, $\left(\frac{M}{L}\right)=1$. By Lemma 1 we have $P_n\equiv 1 \pmod 4$ and from formula (20)

we obtain

$$\left(\frac{P_n}{P_m}\right)=(-1)^{\frac{1-1}{2}\cdot\frac{\varepsilon_1-1}{2}+\frac{1-1}{2}\cdot\frac{\varepsilon_2-1}{2}+\ldots+\frac{1-1}{2}\cdot\frac{\varepsilon_l-1}{2}}=1.$$

Now we shall consider the last two cases.

First we consider the case: $2\|L$, $M\equiv 1 \pmod 4$, $\left(\frac{L}{M}\right)=1$.

By Lemma 1 we have $P_n\equiv\left(\frac{-2}{n}\right) \pmod 4$. From Corollary 1 it follows that $\left(\frac{M}{P_n}\right)=1$ and from formula (20) we obtain

$$\left(\frac{P_n}{P_m}\right)=(-1)^{\frac{\left(\frac{-2}{m}\right)-1}{2}\cdot\frac{\varepsilon_1\left(\frac{-2}{r_1}\right)-1}{2}+\frac{\left(\frac{-2}{r_1}\right)-1}{2}\cdot\frac{\varepsilon_2\left(\frac{-2}{r_2}\right)-1}{2}+\ldots+\frac{\left(\frac{-2}{r_{l-1}}\right)-1}{2}\cdot\frac{\varepsilon_l\left(\frac{-2}{r_l}\right)-1}{2}}$$

$$=(-1)^{\sum_{i=1}^{l}\frac{\left(\frac{-2}{r_{i-1}}\right)-1}{2}\cdot\frac{\varepsilon_i\left(\frac{-2}{r_i}\right)-1}{2}},$$

where $m=r_0$.

It remains to consider the case $2\|M$, $L\equiv 1 \pmod 4$, $\left(\frac{M}{L}\right)=1$.

By Corollary 1 in this case we have $\left(\frac{M}{P_n}\right)=1$. By Lemma 1 we have $P_n\equiv -1 \pmod 4$ for $n\geqslant 3$ and it follows from formula (20) that

$$\left(\frac{P_n}{P_m}\right)=(-1)^{\left(\frac{-1-1}{2}\right)\left(\frac{-\varepsilon_1-1}{2}\right)+\left(\frac{-1-1}{2}\right)\left(\frac{-\varepsilon_2-1}{2}\right)+\ldots+\left(\frac{-1-1}{2}\right)\left(\frac{-\varepsilon_{l-1}-1}{2}\right)+\left(\frac{-1-1}{2}\right)\left(\frac{\varepsilon_l-1}{2}\right)}$$

$$=(-1)^{s+\frac{\varepsilon_l-1}{2}},$$

where s is the number of positive ε_i's in the sequence $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{l-1}$.

On the other hand let $P_n=(y^n-1)/(y-1)$, where $2\|y$. Then $M=y\cdot 1\equiv 2 \pmod 4$, $L=(\alpha+\beta)^2\equiv(y+1)^2\equiv 1 \pmod 4$ and

$$\left(\frac{P_n}{P_m}\right)=(-1)^{s+\frac{\varepsilon_l-1}{2}}.$$

Let

$$\frac{n}{m}=k_1+\frac{1}{|k_2}+\frac{1}{|k_3}+\ldots+\frac{1}{|k_\lambda}, \quad \text{where } k_\lambda>1.$$

Suppose that $n=km+r$. Then

$$\frac{y^n-1}{y-1}=\left(\frac{y^{km}-1}{y-1}\right)y^r+\frac{y^r-1}{y-1}.$$

For example for $y = 2$ we have $2^n - 1 = (2^{km} - 1)2^r + 2^r - 1$. Thus

$$\left(\frac{P_n}{P_m}\right) = \left(\frac{P_r}{P_m}\right), \quad \left(\frac{2^n-1}{2^m-1}\right) = \left(\frac{2^r-1}{2^m-1}\right).$$

Let

$$\begin{aligned}
n &= k_1 m + r_1, && 0 < r_1 < m,\\
m &= k_2 r_1 + r_2, && 0 < r_2 < r_1,\\
r_1 &= k_3 r_2 + r_3, && 0 < r_3 < r_2,\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
r_{\lambda-4} &= k_{\lambda-2} r_{\lambda-3} + r_{\lambda-2}, && 0 < r_{\lambda-2} < r_{\lambda-3},\\
r_{\lambda-3} &= k_{\lambda-1} r_{\lambda-2} + r_{\lambda-1}, && 0 < r_{\lambda-1} = 1 < r_{\lambda-2},\\
r_{\lambda-2} &= k_\lambda r_{\lambda-1} + 0.
\end{aligned}$$

Hence

$$\begin{aligned}
\left(\frac{P_n}{P_m}\right) = \left(\frac{P_{r_1}}{P_m}\right) &= (-1)^{\frac{P_m-1}{2}\cdot\frac{P_{r_1}-1}{2}}\left(\frac{P_m}{P_{r_1}}\right) = (-1)^{\frac{P_m-1}{2}\cdot\frac{P_{r_1}-1}{2}}\left(\frac{P_{r_2}}{P_{r_1}}\right)\\
&= (-1)^{\frac{P_m-1}{2}\cdot\frac{P_{r_1}-1}{2}+\frac{P_{r_1}-1}{2}\cdot\frac{P_{r_2}-1}{2}+\dots+\frac{P_{r_{\lambda-3}}-1}{2}\cdot\frac{P_{r_{\lambda-2}}-1}{2}}\left(\frac{P_{r_{\lambda-3}}}{P_{r_{\lambda-2}}}\right)\\
&= (-1)^{\frac{P_m-1}{2}\cdot\frac{P_{r_1}-1}{2}+\frac{P_{r_1}-1}{2}\cdot\frac{P_{r_2}-1}{2}+\dots+\frac{P_{r_{\lambda-3}}-1}{2}\cdot\frac{P_{r_{\lambda-2}}-1}{2}}\left(\frac{P_{r_{\lambda-1}}}{P_{r_{\lambda-2}}}\right)\\
&= (-1)^{\frac{P_m-1}{2}\cdot\frac{P_{r_1}-1}{2}+\frac{P_{r_1}-1}{2}\cdot\frac{P_{r_2}-1}{2}+\dots+\frac{P_{r_{\lambda-3}}-1}{2}\cdot\frac{P_{r_{\lambda-2}}-1}{2}}.
\end{aligned}$$

We have

$$P_i \equiv -1 \pmod 4 \quad \text{for } i = 2, 3, \dots$$

Thus

$$\left(\frac{P_n}{P_m}\right) = (-1)^{\lambda-2} = (-1)^\lambda.$$

This completes the proof of Theorem 2.

If we substitute L^2 for L in the trinomial $x^2 - \sqrt{L}x + M$ we get the trinomial $x^2 - \sqrt{L^2}x + M = x^2 - Lx + M$. The number $L_n = \dfrac{\alpha^n - \beta^n}{\alpha - \beta}$, where α and β are different roots of the trinomial $x^2 - Lx + M$, is the nth Lucas's number connected with the trinomial. We have $\left(\dfrac{L^2}{M}\right) = 1$ for M odd and $\left(\dfrac{M}{L^2}\right) = 1$ if $2 \nmid L$. If $2 \mid L$ then $4 \mid L^2$. If $L \equiv \pm 1 \pmod 4$ then $L^2 \equiv 1 \pmod 4$ and Theorem 2 implies the following Theorem 2' on Lucas numbers L_n.

THEOREM 2'. *Let* $L_n = \dfrac{\alpha^n - \beta^n}{\alpha - \beta}$, *where* α *and* β *are different roots of the trinomial* $x^2 - Lx + M$ ($L > 0$ *and* M *are rational integers and* $K = L^2 - 4M > 0$). *Let* $2 \nmid nm$, $(m, n) = 1$, $(L, M) = 1$. *Then*

(a) *If* $2 \mid L$, $M \equiv 1 \pmod 4$ *then* $\left(\dfrac{L_n}{L_m}\right) = \left(\dfrac{n}{m}\right)$.

(b) *If* $2 \mid L$, $M \equiv -1 \pmod 4$ *or* $4 \mid M$, $L \equiv \pm 1 \pmod 4$ *then* $\left(\dfrac{L_n}{L_m}\right) = 1$.

(c) *If* $2 \| M$, $L \equiv \pm 1 \pmod 4$ *then* $\left(\dfrac{L_n}{L_m}\right) = (-1)^\lambda$, *where* λ *is the number of terms in the formula* $\dfrac{n}{m} = k_1 + \dfrac{1}{|k_2|} + \dots + \dfrac{1}{|k_\lambda|}$, *which represents the expansion of the rational number* $\dfrac{n}{m}$ *into a simple continued fraction with* $k_\lambda > 1$.

2. Applications of Jacobi's symbol $\left(\dfrac{P_n}{P_m}\right)$ to some diophantine equations connected with Lehmer's numbers. First we shall give a new proof of Chao Ko's theorem (see [1], [2], [5]) according to which the equation $x^2 - 1 = y^p$, where p is a prime > 3, has no solution in integers x and y ($y \neq 0$).

Let $x^2 - 1 = y^p$, where p is a prime > 3. By a theorem of Nagell (see [6]) we have $p \mid x$, $2 \mid y$, hence

$$y + 1 = p\,\square, \quad \text{where } 2 \nmid \square$$

and

$$y \equiv p - 1 \pmod 4.$$

First we consider the case

I. $p = 4k + 3$. Then from $y \equiv (p-1) \pmod 4$ it follows that $y \equiv 2 \pmod 4$.

Since $p > 3$, we have $p = 3k + a$, where $a = 1, 2$ and

(21)

$$1=\left(\frac{\square}{y^2+y+1}\right)=\left(\frac{y^p+1}{y^2+y+1}\right)=\left(\frac{(y^3-1+1)^k y^a+1}{y^2+y+1}\right)=\left(\frac{y^a+1}{y^2+y+1}\right).$$

If $a=1$ then

$$\left(\frac{y^a+1}{y^2+y+1}\right)=\left(\frac{y+1}{y^2+y+1}\right)=-\left(\frac{y^2+y+1}{y+1}\right)=-1$$

and we obtain a contradiction with (21).

If $a=2$ then

$$\left(\frac{y^a+1}{y^2+y+1}\right)=\left(\frac{y^2+1}{y^2+y+1}\right)=\left(\frac{2}{y^2+1}\right)\left(\frac{y/2}{y^2+1}\right)=(-1)\left(\frac{y^2+1}{y/2}\right)=-1$$

and we obtain again a contradiction with (21).

II. Suppose that $p=4k+1$. Let $L_n=\dfrac{(-y)^n-1}{-y-1}$ and let q be an odd prime number such that $\left(\dfrac{q}{p}\right)=-1$. From $y\equiv p-1 \pmod 4$ it follows that $y\equiv 0 \pmod 4$.

By Theorem 2′ we have $\left(\dfrac{L_p}{L_q}\right)=1$.

On the other hand, since $y+1=p\square$, we have

$$1=\left(\frac{L_p}{L_q}\right)=\left(\frac{p}{pl+q}\right)=\left(\frac{pl+q}{p}\right)=\left(\frac{q}{p}\right)=-1$$

$$\left(L_q=\frac{y^q+1}{y+1}=y^{q-1}-y^{q-2}+\ldots+(-y)+1\equiv 1+1+\ldots+1\equiv q \pmod p\right).$$

Thus the equation $y^p+1=x^2$ has no solution in positive integers x and y and theorem of Chao Ko is proved. Now let $p_{\max}(n)$ denote the greatest prime factor of n and let $K=L-4M>0$.

The following theorems hold

THEOREM 3. *Let* $(L,M)=1$, $K=L-4M>0$. *If* $4\mid L$, $M\equiv 1 \pmod 4$, $\left(\dfrac{L}{M}\right)=1$ *or* $L\equiv 3 \pmod 4$, $4\mid M$, $\left(\dfrac{M}{L}\right)=1$, $2\nmid n\neq\square$ *then* $P_n\neq\square$.

THEOREM 4. *Let* $p_{\max}(n)\nmid K=L-4M>0$ *for* $n\neq 2^s$. *Let* $n\neq 2^{2k+1}$, $n\neq 1$. *If* $4\mid L$, $M\equiv 1 \pmod 4$, $\left(\dfrac{L}{M}\right)=1$ *or* $4\mid M$, $L\equiv 3 \pmod 4$, $\left(\dfrac{M}{L}\right)=1$ *then* $P_n\neq\square$.

THEOREM 3′. *Let* $2\nmid n$, $n\neq\square$, $n>1$, $K=L^2-4M>0$. *If* $(L,M)=1$, $2\mid L$, $M\equiv 1 \pmod 4$ *then* $L_n\neq\square$.

THEOREM 4′. *Let* $n\neq 1, 2^k$, $p_{\max}(n)\nmid K=L^2-4M>0$ *for* $n\neq 2^e$. *If* $(L,M)=1$, $2\mid L$, $M\equiv 1 \pmod 4$ *then* $L_n\neq\square$.

First we note that the theorem of G. Terjanian (see [10]), stated in the introduction is a particular case of Theorem 3′.

Indeed, if $x^{2p}+y^{2p}=z^{2p}$ then $2\mid xy$. Without loss of generality we can assume that $2\mid y$. Then $4\mid z^2-x^2$, $2\nmid zx$, hence $x^2z^2\equiv 1 \pmod 4$, $2\mid z^2+x^2$ and if we put in Theorem 3′ $L=z^2+x^2$, $M=z^2x^2$ we obtain

$$L_p=\frac{(z^2)^p-(x^2)^p}{z^2-x^2}=\frac{z^{2p}-x^{2p}}{z^2-x^2}\neq\square.$$

But if $x^{2p}+y^{2p}=z^{2p}$, where $p\nmid y$, then $\dfrac{z^{2p}-x^{2p}}{z^2-x^2}=\square$.

This completes the proof of G. Terjanian's theorem.

Proof of Theorem 3. Let $2\nmid n$, $n\neq\square$. Suppose that $P_n=\square$. By Theorem 2 we have $\left(\dfrac{n}{m}\right)=\left(\dfrac{P_n}{P_m}\right)=\left(\dfrac{\square}{P_m}\right)=1$ for every odd m. On the other hand, for a given odd number n, let m be an odd number such that $\left(\dfrac{n}{m}\right)=-1$. (It is easy to see that such an odd number m exists.) Then $\left(\dfrac{P_n}{P_m}\right)=\left(\dfrac{n}{m}\right)=-1$ and we get a contradiction. This completes the proof of Theorem 3.

Proof of Theorem 4. Let $p=p_{\max}(n)\nmid K=K=(\alpha-\beta)^2=L-4M>0$, $p^t\| n$.

I. Let $2\nmid n$. Then

$$P_n=\frac{\alpha^n-\beta^n}{\alpha-\beta}=Q_pQ_{p^2}\ldots Q_{p^t}\prod_{\substack{1\leqslant i\mid n\\ i\neq p^\varepsilon,\,1\leqslant\varepsilon\leqslant t}}Q_i,$$

where

$$Q_k=\prod_{i\mid k}(\alpha^i-\beta^i)^{\mu(k/i)}=\prod_{(m,k)=1}(\alpha-\zeta_k^m\beta),$$

μ is the Möbius function, ζ_k is a primitive kth root of unity.

First we prove that $(Q_i,Q_{p^j})=1$ for $1<i\mid n$, $i\neq p^s$, $1\leqslant s\leqslant t$, $j=1,2,\ldots$ Indeed, we have $(Q_i,Q_{p^j})=1$ or $(Q_i,Q_{p^j})=$ greatest prime factor of the number ip^j. In the latter case, since $p=p_{\max}(n)$, we would have $p\mid Q_i$, $p\mid Q_{p^j}$, $i\neq p^s$, $i\mid n$. But this is impossible, because the only numbers Q_m which can be divisible by p in this case are

$$Q_p, Q_{p^2}, Q_{p^3}, \ldots \text{ (see Lehmer [4])}.$$

Thus

$$\Big(p, \prod_{\substack{1<i|n\\ i\neq p^s, 1\leqslant s\leqslant t}} Q_i\Big) = 1 \quad \text{and} \quad \Big(Q_p Q_{p^2}\dots Q_{p^t}, \prod_{\substack{1<i|n\\ i\neq p^s, 1\leqslant s\leqslant t}} Q_i\Big) = 1.$$

II. Let $2|n \neq 2^\lambda$. Then

$$P_n = \frac{\alpha^n-\beta^n}{\alpha^2-\beta^2} = Q_p Q_{p^2}\dots Q_{p^t} \prod_{\substack{1<i|n\\ i\neq p^s, 1\leqslant s\leqslant t}} Q_i,$$

where also

$$\Big(Q_p Q_{p^2}\dots Q_{p^t}, \prod_{\substack{1<i|n\\ i\neq p^s, 1\leqslant s\leqslant t}} Q_i\Big) = 1.$$

But from $p\nmid K = (\alpha-\beta)^2$ it follows that

$$p\nmid Q_p Q_{p^2}\dots Q_{p^t} \quad \text{and} \quad (Q_{p^\varepsilon}, Q_{p^r}) = 1 \quad \text{for } \varepsilon \neq r$$

(see [4]).

Thus, if $P_n = \square$ in both cases we should have $\dfrac{\alpha^p-\beta^p}{\alpha-\beta} = \square$, but this by Theorem 3 is impossible.

III. Let $n = 2^{2k}$. Then

$$P_n = \frac{\alpha^{2^{2k}}-\beta^{2^{2k}}}{\alpha^2-\beta^2} = (\alpha^2+\beta^2)(\alpha^{2^2}+\beta^{2^2})\dots(\alpha^{2^{2k-1}}+\beta^{2^{2k-1}}).$$

If $L \equiv 3 \pmod 4$, $M \equiv 0 \pmod 4$ then $P_4 = \alpha^2+\beta^2 = L-2M \equiv 3 \pmod 4$. Hence $P_4 \neq \square$ and since $(\alpha^{2^i}+\beta^{2^i}, \alpha^{2^j}+\beta^{2^j}) = 1$ for $i \neq j$ we have $P_n \neq \square$. Now let $4|L$. Then $2\| \alpha^{2^i}+\beta^{2^i}$ for $i = 1, 2, \dots$

If $P_n = \square$ then

$$\alpha^2+\beta^2 = 2\square, \quad \alpha^{2^2}+\beta^{2^2} = 2\square, \quad \dots, \quad \alpha^{2^{2k-1}}+\beta^{2^{2k-1}} = 2\square,$$

hence

$$P_n = 2^{2k-1}\square = \square,$$

which is impossible.

This completes the proof of Theorem 4.

THEOREM 5. *Let α and β be different roots of the trinomial $x^2-\sqrt{L}x+M$, where $K = L-4M > 0$, $(L, M) = 1$. If $4|M$, $L \equiv 1 \pmod 4$, $\left(\dfrac{M}{L}\right) = 1$ or $4|L$, $M \equiv -1 \pmod 4$, $\left(\dfrac{L}{M}\right) = 1$, p is an odd prime number then $P_p = \dfrac{\alpha^p-\beta^p}{\alpha-\beta} \neq p\square$.*

Proof of Theorem 5. By the identity of Kummer (see [3]) we have

$$\frac{a^n \pm b^n}{a\pm b} = (a\pm b)^{n-1} \mp n(a\pm b)^{n-3}ab + \frac{n(n-3)}{1\cdot 2}\times \tag{22}$$

$$\times (a\pm b)^{n-5}a^2b^2 \mp \dots (\mp 1)^k \frac{n(n-k-1)(n-k-2)\dots(n-2k+1)}{1\cdot 2\dots k}\times$$

$$\times (a\pm b)^{n-2k-1}a^kb^k + \dots (\mp 1)^{(n-1)/2} n(ab)^{(n-1)/2}.$$

Hence

$$\frac{\alpha^q-\beta^q}{\alpha-\beta} = (\alpha-\beta)^2\lambda + qM^{(q-1)/2}, \tag{23}$$

where λ is some rational integer and q an odd number.

Now let $q \equiv 1 \pmod 4$ be a prime number such that $\left(\dfrac{p}{q}\right) = -1$. Then also $\left(\dfrac{q}{p}\right) = -1$.

If $P_p = \dfrac{\alpha^p-\beta^p}{\alpha-\beta} = p\square$ then $p|P_p$, hence $p|(\alpha-\beta)^2$ and by formula (23) we have

$$P_q \equiv qM^{(q-1)/2} \pmod p. \tag{24}$$

By Lemma 1 we have $P_q \equiv 1 \pmod 4$. By Theorem 2 we have $\left(\dfrac{P_p}{P_q}\right) = 1$.

If $P_p = \dfrac{\alpha^p-\beta^p}{\alpha-\beta} = p\square$ then

$$1 = \left(\frac{P_p}{P_q}\right) = \left(\frac{p\square}{P_q}\right) = \left(\frac{p}{P_q}\right) = \left(\frac{P_q}{p}\right) = \left(\frac{q(M^{(q-1)/4})^2}{p}\right) = \left(\frac{q}{p}\right) = -1,$$

which is impossible. Thus $P_p \neq p\square$ and Theorem 5 is proved.

THEOREM 5′. *Let $K = L_1^2-4M > 0$, $(L_1, M) = 1$, α and β be different roots of the trinomial z^2-L_1z+M, where $2\nmid L_1$, $4|M$ or $2|L_1$, $M \equiv -1 \pmod 4$ and let p be an odd prime. Then*

$$L_p = \frac{\alpha^p-\beta^p}{\alpha-\beta} \neq p\square.$$

Proof of Theorem 5′. Put in Theorem 5: $L = L_1^2$. Then L

$\equiv 1 \pmod 4$, $4 \mid M$, $\left(\frac{M}{L_1^2}\right) = 1$ or $4 \mid L$, $M \equiv -1 \pmod 4$, $\left(\frac{L_1^2}{M}\right) = 1$ and by Theorem 5 we have $L_p \neq p\square$.

THEOREM 5''. *Let x and y be rational integers, $(x, y) = 1$, $xy \equiv 0$ or $3 \pmod 4$. If $n > 1$ is odd we have*

$$\frac{x^n - y^n}{x - y} \neq n\square.$$

Proof. Assume that

$$\frac{x^n - y^n}{x - y} = n\square \tag{25}$$

and let p be the least prime factor of n. We have

$$\frac{x^n - y^n}{x - y} = \prod_{1<k\mid n} Q_k(x, y), \tag{26}$$

where Q_k is defined in the proof of Theorem 4. Since p is the least prime factor of n, it follows from (25) and (26) that $p \mid x - y$ and

$$\frac{x^p - y^p}{x - y} = p q_1^{\alpha_1} q_2^{\alpha_2} \dots q_t^{\alpha_t} \bar{q}_1^{\beta_1} \bar{q}_2^{\beta_2} \dots \bar{q}_r^{\beta_r} \tag{27}$$

where $q_i \mid n$ $(i = 1, 2, \dots, t)$ and $(\bar{q}_j, n) = 1$ $(j = 1, 2, \dots, r)$. We have

$$(Q_i(x, y), Q_j(x, y)) \mid \text{the greatest prime factor of } ij \mid n,$$

hence in view of (25) and (26) it follows that $\beta_i \equiv 0 \pmod 2$ for $i = 1, 2, \dots, r$. Further $q_i \mid Q_j(x, y)$ if and only if $j = p q_i^l$, $l = 0, 1, 2, \dots$ Let

$$q_i^{\gamma_i} \parallel n \quad (i = 1, 2, \dots, t). \tag{28}$$

Then

$$q_i^{\gamma_i} \parallel Q_{pq_i}(x, y) Q_{pq_i^2}(x, y) \dots Q_{pq_i^{\gamma_i}}(x, y)$$

hence

$$q_i^{\alpha_i + \gamma_i} \parallel \frac{x^n - y^n}{x - y}$$

and from (25) and (28) it follows that $\alpha_i \equiv 0 \pmod 2$ for $i = 1, 2, \dots, t$. Thus by (27)

$$\frac{x^p - y^p}{x - y} = p\square$$

which is impossible by Theorem 5'.

The special case of Theorem 5'' with $x = x_1^2$, $y = -y_1^2$ has been proved earlier by Professor G. Terjanian.

Let $2 \parallel M$, $L \equiv 1 \pmod 4$, $K = L - 4M > 0$, $(L, M) = 1$, $\left(\frac{M}{L}\right) = 1$. Suppose that

$$P_p = \frac{\alpha^p - \beta^p}{\alpha - \beta} = p\square. \tag{29}$$

By Lemma 1 we have $P_p \equiv -1 \pmod 4$. Thus it must be $p \equiv 3 \pmod 4$. Let q be an odd number $\equiv 1 \pmod 4$. Let $\frac{p}{q} = c_1 + \frac{1}{|c_2} + \dots + \frac{1}{|c_\lambda}$, where $c_\lambda > 1$. By formula (23) we have

$$\frac{\alpha^q - \beta^q}{\alpha - \beta} = (\alpha - \beta)^2 F + q M^{(q-1)/2}, \quad \text{where } F \text{ is a rational integer.}$$

From $p \mid P_p$ it follows that $p \mid (\alpha - \beta)^2$ and $P_q \equiv q M^{(q-1)/2} \pmod p$. By Theorem 2 we have

$$(-1)^\lambda = \left(\frac{P_p}{P_q}\right) = \left(\frac{p\square}{P_q}\right) = \left(\frac{p}{P_q}\right) = -\left(\frac{P_q}{p}\right) = -\left(\frac{q(M^{(q-1)/4})^2}{p}\right) = -\left(\frac{q}{p}\right).$$

Now, if we can find an odd number q such that $(-1)^\lambda = \left(\frac{q}{p}\right)$ the impossibility of (29) would follow.

But that is possible (see [7]). If $p - 1 = 2l$, where $l \equiv 1 \pmod 4$, $l > 1$, then $\frac{2l+1}{l} = 2 + \frac{1}{|l}$, $\lambda = 2$ and for $q = l$ we have

$$\left(\frac{q}{p}\right) = \left(\frac{l}{2l+1}\right) = \left(\frac{1+2l}{l}\right) = 1 = (-1)^\lambda.$$

If $p - 1 = 2l$, where $l \equiv 3 \pmod 4$ then $2l - 1 = p - 2 = 8k + 5$, $\frac{p}{p-2} = 1 + \frac{1}{|(p-3)/2} + \frac{1}{|2}$, $\lambda = 3$ and for $q = p - 2$ we have

$$\left(\frac{q}{p}\right) = \left(\frac{p-2}{p}\right) = \left(\frac{p}{p-2}\right) = \left(\frac{2}{p-2}\right) = (-1)^\lambda.$$

Thus the following theorem holds.

THEOREM 6. *Let α and β be different roots of the trinomial $x^2 - \sqrt{L}x + M$, where $K = L - 4M > 0$, $(L, M) = 1$. If $2 \parallel M$, $L \equiv 1 \pmod 4$, $\left(\frac{M}{L}\right) = 1$ then*

$$P_p = \frac{\alpha^p - \beta^p}{\alpha - \beta} \neq p\square.$$

In the same way as Theorem 5' implies Theorem 5'' Theorem 6 implies the following

THEOREM 6'. *Let x, y be rational integers, $(x, y) = 1$, $2 \| xy$. If $n > 1$ is not divisible by 3 then*

$$\frac{x^n - y^n}{x - y} \neq n \square.$$

PROBLEMS

(a) Let $p > 3$, $\neq 9$, be a given odd number. Does there exist an odd number q such that $(-1)^\lambda = \left(\frac{q}{p}\right)$ and

$$\frac{p}{q} = c_1 + \frac{1}{|c_2|} + \ldots + \frac{1}{|c_\lambda|}, \quad \text{where } c_\lambda > 1.$$

(b) Let $N(p)$ and $\bar{N}(p)$ denote the number of positive integers n such that $\left(\frac{n}{p}\right) = (-1)^\lambda$, $n < p$ and $\left(\frac{n}{p}\right) = (-1)^{\lambda+1}$, $n < p$ respectively, where $\frac{p}{n} = d_1 + \frac{1}{|d_2|} + \ldots + \frac{1}{|d_\lambda|}$ and $d_\lambda > 1$.

Find the lower and upper bound for the functions $N(p)$ and $\bar{N}(p)$.

(c) Is it true that $\lim_{p \to \infty} \frac{N(p)}{\bar{N}(p)} = 1$?

The affirmative answer to the questions (a) and (c) is strongly supported by the results of numerical computations.

References

[1] Chao Ko, *On the diophantine equation $x^2 = y^n + 1$, $xy \neq 0$*, Scientia Sinica (Notes) 14 (1965), pp. 457–460.

[2] – Acta Scientiarum Naturalium Universitatis Szechuanensis 2 (1960), pp. 57–64.

[3] E. E. Kummer, *De aequatione $x^{2\lambda} + y^{2\lambda} = z^{2\lambda}$ per numeros integros*, Journ. Reine Angew. Math. 17 (1837), pp. 203–209.

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

[5] L. J. Mordell, *Diophantine equations*, Academic Press, London and New York, 1969, pp. 302–304.

[6] T. Nagell, *Sur l'impossibilité de l'équation indéterminée $x^p + 1 = y^2$*, Norsk. Mat. Forenings Skrifter 1 (1921), No 4.

[7] A. Rotkiewicz, *On the equation $x^p + y^p = z^2$*, Bull. Acad. Polon. Sci., Sér. Sci. Math. 30 (1982), pp. 211–214.

[8] A. Schinzel, *On primitive factors of Lehmer numbers I*, Acta Arith. 8 (1963), pp. 213–223.

[9] W. Sierpiński, *Elementary theory of numbers*, Warszawa 1964.

[10] G. Terjanian, *Sur l'équation $x^{2p} + y^{2p} = z^{2p}$*, C.R. Acad. Sci. Paris, 285 (1977), pp. 973–975.

INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
ul. Śniadeckich 8, 00-950 Warszawa

DEPARTMENT OF MATHEMATICS AND NATURAL SCIENCES
WARSAW UNIVERSITY BRANCH
15-424 Białystok

Received on 26. 6. 1981
and in revised form on 9. 12. 1981 (1259)