ACTA ARITHMETICA
LX.4 (1992)

Fibonacci numbers and Fermat's last theorem

by

ZHI-HONG SUN and ZHI-WEI SUN* (Nanjing)

Let $\{F_n\}$ be the Fibonacci sequence defined by $F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$ $(n \ge 1)$. It is well known that $F_{p-(\frac{5}{p})} \equiv 0 \pmod p$ for any odd prime p, where $(-)$ denotes the Legendre symbol. In 1960 D. D. Wall [13] asked whether $p^2 \mid F_{p-(\frac{5}{p})}$ is always impossible; up to now this is still open.

In this paper the sum $\sum_{k\equiv r \pmod{10}} \binom{n}{k}$ is expressed in terms of Fibonacci numbers. As applications we obtain a new formula for the Fibonacci quotient $F_{p-(\frac{5}{p})}/p$ and a criterion for the relation $p \mid F_{(p-1)/4}$ (if $p \equiv 1 \pmod 4$), where $p \ne 5$ is an odd prime. We also prove that the affirmative answer to Wall's question implies the first case of FLT (Fermat's last theorem); from this it follows that the first case of FLT holds for those exponents which are (odd) Fibonacci primes or Lucas primes.

1. Introduction to Fibonacci and Lucas numbers. For later convenience we introduce in this section some basic properties of the Fibonacci sequence $\{F_n\}$ and its companion — the Lucas sequence $\{L_n\}$.

The $\{F_n\}$ and $\{L_n\}$ are given by

$$F_0 = 0\,,\ F_1 = 1\,,\ F_{n+1} = F_n + F_{n-1} \qquad (n = 1, 2, 3, \ldots)$$

and

$$L_0 = 2\,,\ L_1 = 1\,,\ L_{n+1} = L_n + L_{n-1} \qquad (n = 1, 2, 3, \ldots)\,.$$

It is well known that

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \qquad \text{and} \qquad L_n = \alpha^n + \beta^n$$

where $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$ are the roots of the equation $x^2 - x - 1 = 0$.

* Research supported by the National Nature Science Foundation of P. R. China.

From the explicit formulae of F_n and L_n, one can easily obtain

THEOREM A. *For $n = 0, 1, 2, \ldots$ we have*

(i) $L_n = 2F_{n+1} - F_n,\ 5F_n = 2L_{n+1} - L_n$;
(ii) $L_n^2 - 5F_n^2 = 4(-1)^n$;
(iii) $F_{2n} = F_nL_n,\ L_{2n} = L_n^2 - 2(-1)^n$.

Here, part (i) can also be proved by induction, part (ii) is formula 10.14.7 of [2, p. 149], part (iii) can be found in [4, p. 61].

Let $(n_1, \ldots, n_k)$ and $[n_1, \ldots, n_k]$ respectively denote the g.c.d. and l.c.m. of positive integers $n_1, \ldots, n_k$. For Fibonacci numbers we have the nice

THEOREM B. *Let m, n be positive integers. Then*

(i) $F_{mn} = \sum_{i=1}^{n} \binom{n}{i} F_{m-1}^{n-i} F_m^i F_i \equiv 0 \pmod{F_m}$,
(ii) $(F_m, F_n) = F_{(m,n)}$.

Here part (i) is due to H. Siebeck (cf. [1, p. 394]), a generalization was given by Sun [11]. Part (ii) is a theorem of E. Lucas (see Theorem III of [1, p. 396]), a proof can be found in [2, pp. 148–149].

Concerning divisibility we have

THEOREM C. *Let p be a prime.*

(i) *If $p \neq 2$ then $F_{p-(\frac{5}{p})} \equiv 0 \pmod p$.*

(ii) *Let λ, m, n be positive integers. Suppose $p^\lambda \| F_m$ (i.e. $p^\lambda \mid F_m$ and $p^{\lambda+1} \nmid F_m$). Then $p \mid n$ if and only if $p^{\lambda+1} \mid F_{mn}$.*

Proof. The first part is well known (cf. [1, p. 394]), for a proof one may see [2, p. 150].

Now let us consider part (ii). By part (i) of Theorem B,

$$F_{mn} \equiv nF_{m-1}^{n-1}F_m \pmod{F_m^2}.$$

Since $m > 1$ (because $p \mid F_m$), $(F_{m-1}, F_m) = F_{(m-1,m)} = 1$, $p^\lambda \| F_m$ and $p^{\lambda+1} \mid F_m^2$, we have

$$p^{\lambda+1} \mid F_{mn} \Leftrightarrow p^{\lambda+1} \mid nF_{m-1}^{n-1}F_m \Leftrightarrow p \mid n.$$

This concludes the proof.

Remark 1. It follows from Theorem C (and the fact $2 \mid F_3$) that any prime-power divides some positive Fibonacci numbers. Let $d = p_1^{\lambda_1} \ldots p_r^{\lambda_r}$ ($p_1 < p_2 < \ldots < p_r$) be in standard form, and suppose $p_i^{\lambda_i} \mid F_{n_i}$ for each $i = 1, \ldots, r$. Since F_{n_i} divides $F_{[n_1,\ldots,n_k]}$, $p_i^{\lambda_i} \mid F_{[n_1,\ldots,n_k]}$ for all $i = 1, \ldots, r$ and hence $d \mid F_{[n_1,\ldots,n_k]}$. Thus, any positive integer d is a divisor of some positive Fibonacci number.

2. On the sum $\sum_{k\equiv r \pmod{10}} \binom{n}{k}$**.** For integers $m>0$, $n>0$ and r we let

$$T^n_{r(m)} = \sum_{\substack{k=0\\ k\equiv r \pmod m}}^{n} \binom{n}{k} \quad \text{and} \quad \Delta_m(r,n) = mT^n_{[n/2]+r(m)} - 2^n$$

where $[\,\cdot\,]$ is the greatest integer function. By using the properties of binomial coefficients one can easily prove that

$$T^n_{r(m)} = T^n_{n-r(m)}\,, \qquad T^{n+1}_{r(m)} = T^n_{r(m)} + T^n_{r-1(m)}\,.$$

From this we have

LEMMA 1. *Let m, n be positive integers and r, s, t be integers satisfying $r+s\equiv 0 \pmod m$ and $r+t\equiv 2 \pmod m$. If n is odd then*

$$\Delta_m(r,n+2) = \Delta_m(s,n) + 2\Delta_m(r,n) + \Delta_m(t,n)\,.$$

Proof.

$$\begin{aligned}
\Delta_m(s,n) &+ 2\Delta_m(r,n) + \Delta_m(t,n)\\
&= m(T^n_{[n/2]+s(m)} + 2T^n_{[n/2]+r(m)} + T^n_{[n/2]+t(m)}) - 4\cdot 2^n\\
&= m(T^n_{(n-1)/2-r(m)} + 2T^n_{(n-1)/2+r(m)} + T^n_{(n-1)/2+2-r(m)}) - 2^{n+2}\\
&= m(T^n_{(n-1)/2+r+1(m)} + T^n_{(n-1)/2+r(m)} + T^n_{(n-1)/2+r(m)}\\
&\qquad\qquad + T^n_{(n-1)/2+r-1(m)}) - 2^{n+2}\\
&= m(T^{n+1}_{(n-1)/2+r+1(m)} + T^{n+1}_{(n-1)/2+r(m)}) - 2^{n+2} = \Delta_m(r,n+2)\,.
\end{aligned}$$

Now we can give

THEOREM 1. *Let $p>0$ be an odd number.*

(a) *If* $p\equiv 1 \pmod 4$ *then*

$$\begin{aligned}
\Delta_{10}(0,p) &= L_{p+1} + 5^{(p+3)/4}F_{(p+1)/2}\,,\\
\Delta_{10}(2,p) &= -L_{p-1} + 5^{(p+3)/4}F_{(p-1)/2}\,,\\
\Delta_{10}(4,p) &= -L_{p-1} - 5^{(p+3)/4}F_{(p-1)/2}\,,\\
\Delta_{10}(6,p) &= L_{p+1} - 5^{(p+3)/4}F_{(p+1)/2}\,.
\end{aligned}$$

(b) *If* $p\equiv 3 \pmod 4$ *then*

$$\begin{aligned}
\Delta_{10}(0,p) &= L_{p+1} + 5^{(p+1)/4}L_{(p+1)/2}\,,\\
\Delta_{10}(2,p) &= -L_{p-1} + 5^{(p+1)/4}L_{(p-1)/2}\,,\\
\Delta_{10}(4,p) &= -L_{p-1} - 5^{(p+1)/4}L_{(p-1)/2}\,,\\
\Delta_{10}(6,p) &= L_{p+1} - 5^{(p+1)/4}L_{(p+1)/2}\,.
\end{aligned}$$

(c) $\varDelta_{10}(8,p)=-2L_p$.

Proof. One can easily verify the following simple facts:

$$\begin{aligned}
&\varDelta_{10}(0,1)=8=L_2+5F_1\,, && \varDelta_{10}(0,3)=22=L_4+5L_2\,;\\
&\varDelta_{10}(2,1)=-2=-L_0+5F_0\,, && \varDelta_{10}(2,3)=2=-L_2+5L_1\,;\\
&\varDelta_{10}(4,1)=-2=-L_0-5F_0\,, && \varDelta_{10}(4,3)=-8=-L_2-5L_1\,;\\
&\varDelta_{10}(6,1)=-2=L_2-5F_1\,, && \varDelta_{10}(6,3)=-8=L_4-5L_2\,;\\
&\varDelta_{10}(8,1)=-2=-2L_1\,, && \varDelta_{10}(8,3)=-8=-2L_3\,.
\end{aligned}$$

Thus Theorem 1 holds for $p=1,3$.

Now let us suppose the odd p is not less than 3, and assume that the theorem is true for p. Applying Theorem A we get

$$\begin{aligned}
3F_{(p+1)/2}+F_{(p-1)/2}&=2F_{(p+1)/2}+F_{(p+3)/2}\\
&=2F_{(p+5)/2}-F_{(p+3)/2}=L_{(p+3)/2}\,,\\
3L_{(p+1)/2}+L_{(p-1)/2}&=2L_{(p+1)/2}+L_{(p+3)/2}\\
&=2L_{(p+5)/2}-L_{(p+3)/2}=5F_{(p+3)/2}\,,\\
2F_{(p-1)/2}+F_{(p+1)/2}&=2F_{(p+3)/2}-F_{(p+1)/2}=L_{(p+1)/2}\,,\\
2L_{(p-1)/2}+L_{(p+1)/2}&=2L_{(p+3)/2}-L_{(p+1)/2}=5F_{(p+1)/2}\,.
\end{aligned}$$

By Lemma 1 and the (inductive) hypothesis we have

$$\begin{aligned}
&\varDelta_{10}(0,p+2)=\varDelta_{10}(0,p)+2\varDelta_{10}(0,p)+\varDelta_{10}(2,p)\\
&=\begin{cases}3(L_{p+1}+5^{(p+3)/4}F_{(p+1)/2})-L_{p-1}+5^{(p+3)/4}F_{(p-1)/2}\\ \qquad =L_{p+3}+5^{(p+3)/4}L_{(p+3)/2}\quad \text{if } p\equiv 1 \pmod 4\,,\\ 3(L_{p+1}+5^{(p+1)/4}L_{(p+1)/2})-L_{p-1}+5^{(p+1)/4}L_{(p-1)/2}\\ \qquad =L_{p+3}+5^{(p+5)/4}F_{(p+3)/2}\quad \text{if } p\equiv 3 \pmod 4\,.\end{cases}
\end{aligned}$$

(Note that $3L_{p+1}-L_{p-1}=2L_{p+1}+L_p=L_{p+1}+L_{p+2}=L_{p+3}$.) Also,

$$\begin{aligned}
&\varDelta_{10}(2,p+2)=\varDelta_{10}(8,p)+2\varDelta_{10}(2,p)+\varDelta_{10}(0,p)\\
&=\begin{cases}-2L_p-2L_{p-1}+2\cdot 5^{(p+3)/4}F_{(p-1)/2}+L_{p+1}+5^{(p+3)/4}F_{(p+1)/2}\\ \qquad =-L_{p+1}+5^{(p+3)/4}L_{(p+1)/2}\quad \text{if } p\equiv 1 \pmod 4\,,\\ -2L_p-2L_{p-1}+2\cdot 5^{(p+1)/4}L_{(p-1)/2}+L_{p+1}+5^{(p+1)/4}L_{(p+1)/2}\\ \qquad =-L_{p+1}+5^{(p+5)/4}F_{(p+1)/2}\quad \text{if } p\equiv 3 \pmod 4\,;\end{cases}
\end{aligned}$$

$$\begin{aligned}
&\varDelta_{10}(4,p+2)=\varDelta_{10}(6,p)+2\varDelta_{10}(4,p)+\varDelta_{10}(8,p)\\
&=\begin{cases}L_{p+1}-5^{(p+3)/4}F_{(p+1)/2}-2L_{p-1}-2\cdot 5^{(p+3)/4}F_{(p-1)/2}-2L_p\\ \qquad =-L_{p+1}-5^{(p+3)/4}L_{(p+1)/2}\quad \text{if } p\equiv 1 \pmod 4\,,\\ L_{p+1}-5^{(p+3)/4}L_{(p+1)/2}-2L_{p-1}-2\cdot 5^{(p+1)/4}L_{(p-1)/2}-2L_p\\ \qquad =-L_{p+1}-5^{(p+5)/4}F_{(p+1)/2}\quad \text{if } p\equiv 3 \pmod 4\,;\end{cases}
\end{aligned}$$

$$\Delta_{10}(6,p+2)=\Delta_{10}(4,p)+2\Delta_{10}(6,p)+\Delta_{10}(6,p)$$
$$=\begin{cases} -L_{p-1}-5^{(p+3)/4}F_{(p-1)/2}+3L_{p+1}-3\cdot 5^{(p+3)/4}F_{(p+1)/2} \\ \qquad = L_{p+3}-5^{(p+3)/4}L_{(p+3)/2} \quad \text{if } p\equiv 1 \pmod 4, \\ -L_{p-1}-5^{(p+1)/4}L_{(p-1)/2}+3L_{p+1}-3\cdot 5^{(p+1)/4}L_{(p+1)/2} \\ \qquad = L_{p+3}-5^{(p+5)/4}F_{(p+3)/2} \quad \text{if } p\equiv 3 \pmod 4; \end{cases}$$

$$\Delta_{10}(8,p+2)=\Delta_{10}(2,p)+2\Delta_{10}(8,p)+\Delta_{10}(4,p)$$
$$=\begin{cases} -L_{p-1}+5^{(p+3)/4}F_{(p-1)/2}-4L_p-L_{p-1}-5^{(p+3)/4}F_{(p-1)/2} \\ \qquad = -2(2L_p+L_{p-1})=-2L_{p+2} \quad \text{if } p\equiv 1 \pmod 4, \\ -L_{p-1}+5^{(p+1)/4}L_{(p-1)/2}-4L_p-L_{p-1}-5^{(p+1)/4}L_{(p-1)/2} \\ \qquad = -2(2L_p+L_{p-1})=-2L_{p+2} \quad \text{if } p\equiv 3 \pmod 4. \end{cases}$$

This shows that the theorem holds for $p+2$.

By the above, Theorem 1 is proved by induction.

Remark 2. For the values of $\Delta_m(r,n)$ ($r\in\mathbb{Z}, n\in\mathbb{Z}^+$) in the cases $m=3,4,5,6,8,12$, one may consult [6]–[10].

3. Congruences with Fibonacci numbers

LEMMA 2. *Let p be a prime and let $m>0$ and r be integers. Then*

$$T^p_{r(m)} \equiv p \sum_{\substack{k=1 \\ k\equiv r \ (\mathrm{mod}\ m)}}^{p-1} \frac{(-1)^{k-1}}{k} + \varepsilon \pmod{p^2}$$

where ε denotes the number of elements in $\{0,p\}$ which are congruent to r modulo m.

Proof. Since

$$k!\binom{p-1}{k}=(p-1)(p-2)\dots(p-k)\equiv(-1)^k k! \pmod p,$$

we have

$$\binom{p-1}{k}\equiv(-1)^k \pmod p \quad \text{for every } k=1,\dots,p-1.$$

Therefore

$$T^p_{r(m)}=\varepsilon+\sum_{\substack{k=1 \\ k\equiv r \ (\mathrm{mod}\ m)}}^{p-1}\frac{p}{k}\binom{p-1}{k-1}\equiv\varepsilon+p\sum_{\substack{k=1 \\ k\equiv r \ (\mathrm{mod}\ m)}}^{p-1}\frac{(-1)^{k-1}}{k} \pmod{p^2}.$$

By Lemma 2, provided that p is a prime we have

$$\frac{2^p-2}{p}=\frac{T^p_{0(1)}-2}{p}\equiv\sum_{k=1}^{p-1}\frac{(-1)^{k-1}}{k} \pmod p$$

which was first given by G. Eisenstein (cf. [1, p. 105]).

THEOREM 2. *Let $p \neq 2,5$ be a prime and let*

$$K_p(r) = \sum_{\substack{k=1 \\ k\equiv r \pmod 5}}^{p-1} \frac{1}{k}.$$

Then

$$pK_p(0) \equiv -pK_p(p) \equiv \begin{cases} 1 + (-1)^{[(p-5)/10]} 5^{(p-1)/4} F_{(p+(\frac{5}{p}))/2} \pmod{p^2} & \text{if } p \equiv 1 \pmod 4, \\ 1 + (-1)^{[(p-5)/10]} 5^{(p-3)/4} L_{(p+(\frac{5}{p}))/2} \pmod{p^2} & \text{if } p \equiv 3 \pmod 4; \end{cases}$$

$$pK_p(2p) \equiv -pK_p(4p) \equiv \begin{cases} (-1)^{[(p-5)/10]} \left(\frac{5}{p}\right) 5^{(p-1)/4} F_{(p-(\frac{5}{p}))/2} \pmod{p^2} & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{[(p-5)/10]} \left(\frac{5}{p}\right) 5^{(p-3)/4} L_{(p-(\frac{5}{p}))/2} \pmod{p^2} & \text{if } p \equiv 3 \pmod 4; \end{cases}$$

$$K_p(3p) \equiv 0 \pmod p.$$

Proof. Note that

$$K_p(p-r) = \sum_{\substack{k=1 \\ k\equiv p-r \pmod 5}}^{p-1} \frac{1}{k} \equiv \sum_{\substack{k=1 \\ p-k\equiv r \pmod 5}}^{p-1} \frac{-1}{p-k} = -K_p(r) \pmod p.$$

So we have

$$K_p(0) \equiv -K_p(p) \pmod p, \quad K_p(2p) \equiv -K_p(-p) = -K_p(4p) \pmod p,$$
$$K_p(3p) \equiv -K_p(-2p) = -K_p(3p) \pmod p \quad \text{hence} \quad K_p(3p) \equiv 0 \pmod p.$$

By Theorem 1, if an integer m is not divisible by 5 then

$$\Delta_{10}(8+2m,p) - \Delta_{10}(8-2m,p)$$
$$= \begin{cases} \pm[\Delta_{10}(0,p) - \Delta_{10}(6,p)] = \begin{cases} \pm 2\cdot 5^{(p+3)/4} F_{(p+1)/2} & \text{if } p\equiv 1 \pmod 4, \\ \pm 2\cdot 5^{(p+1)/4} L_{(p+1)/2} & \text{if } p\equiv 3 \pmod 4, \end{cases} & \text{when } m \equiv \pm 1 \pmod 5; \\ \pm[\Delta_{10}(2,p) - \Delta_{10}(4,p)] = \begin{cases} \pm 2\cdot 5^{(p+3)/4} F_{(p-1)/2} & \text{if } p\equiv 1 \pmod 4, \\ \pm 2\cdot 5^{(p+1)/4} L_{(p-1)/2} & \text{if } p\equiv 3 \pmod 4, \end{cases} & \text{when } m \equiv \pm 2 \pmod 5 \end{cases}$$

$$= \begin{cases} (-1)^{[2m/5]} \cdot 10 \cdot 5^{(p-1)/4} F_{(p+(\frac{m}{5}))/2} & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{[2m/5]} \cdot 10 \cdot 5^{(p-3)/4} L_{(p+(\frac{m}{5}))/2} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

For $m_1 = (p + (-1)^{(p+1)/2} 5)/4$ and $m_2 = 3m_1$ we have

$$\left(\frac{m_1}{5}\right) = \left(\frac{4m_1}{5}\right) = \left(\frac{p}{5}\right) = \left(\frac{5}{p}\right), \quad \left(\frac{m_2}{5}\right) = \left(\frac{3}{5}\right)\left(\frac{m_1}{5}\right) = -\left(\frac{5}{p}\right),$$

$$(-1)^{[2m_1/5]} = (-1)^{(p-1)/2} \cdot (-1)^{[(p-5)/10]},$$

$$\begin{aligned} (-1)^{[2m_2/5]} &= (-1)^{[6m_1/5]} \\ &= \begin{cases} -1 = 1 \cdot (-1) & \text{if } m_1 \equiv 1 \pmod 5, \\ 1 = (-1) \cdot (-1) & \text{if } m_1 \equiv -1 \pmod 5, \\ 1 = 1 \cdot 1 & \text{if } m_1 \equiv 2 \pmod 5, \\ -1 = (-1) \cdot 1 & \text{if } m_1 \equiv -2 \pmod 5 \end{cases} \\ &= (-1)^{[2m_1/5]} \left(\frac{3m_1}{5}\right) = -(-1)^{(p-1)/2} \cdot (-1)^{[(p-5)/10]} \left(\frac{5}{p}\right), \end{aligned}$$

and therefore

$$\frac{(-1)^{(p-1)/2}}{10} [\Delta_{10}(8 + 2m_1, p) - \Delta_{10}(8 - 2m_1, p)]$$

$$= \begin{cases} (-1)^{[2m_1/5]} 5^{(p-1)/4} F_{(p+(\frac{m_1}{5}))/2} \\ \qquad = (-1)^{[(p-5)/10]} 5^{(p-1)/4} F_{(p+(\frac{5}{p}))/2} \text{ if } p \equiv 1 \pmod 4, \\ -(-1)^{[2m_1/5]} 5^{(p-3)/4} L_{(p+(\frac{m_1}{5}))/2} \\ \qquad = (-1)^{[(p-5)/10]} 5^{(p-3)/4} L_{(p+(\frac{5}{p}))/2} \quad \text{if } p \equiv 3 \pmod 4; \end{cases}$$

$$\frac{(-1)^{(p+1)/2}}{10} [\Delta_{10}(8 + 2m_2, p) - \Delta_{10}(8 - 2m_2, p)]$$

$$= \begin{cases} -(-1)^{[2m_2/5]} 5^{(p-1)/4} F_{(p+(\frac{m_2}{5}))/2} \\ \qquad = (-1)^{[(p-5)/10]} \left(\frac{5}{p}\right) 5^{(p-1)/4} F_{(p-(\frac{5}{p}))/2} \quad \text{if } p \equiv 1 \pmod 4, \\ (-1)^{[2m_2/5]} 5^{(p-3)/4} L_{(p+(\frac{m_2}{5}))/2} \\ \qquad = (-1)^{[(p-5)/10]} \left(\frac{5}{p}\right) 5^{(p-3)/4} L_{(p-(\frac{5}{p}))/2} \quad \text{if } p \equiv 3 \pmod 4. \end{cases}$$

To complete the proof, we notice that

$$\begin{aligned} pK_p(0) &= p \sum_{\substack{k=1 \\ 10 \mid k+5}}^{p-1} \frac{(-1)^{k-1}}{k} - p \sum_{\substack{k=1 \\ 10 \mid k}}^{p-1} \frac{(-1)^{k-1}}{k} \\ &\equiv T^p_{-5(10)} - (T^p_{0(10)} - 1) \pmod{p^2} \quad \text{(by Lemma 2)} \\ &= 1 + T^p_{p+5(10)} - T^p_{0(10)} = 1 - (T^p_{p(10)} - T^p_{5(10)}) \end{aligned}$$

$$
\begin{aligned}
&= 1 + (-1)^{(p-1)/2}\big[T^p_{p+\frac{3+(-1)^{(p+1)/2}}{2}\cdot 5(10)} - T^p_{\frac{3+(-1)^{(p-1)/2}}{2}\cdot 5(10)}\big] \\
&= 1 + \frac{(-1)^{(p-1)/2}}{10}\Big[\varDelta_{10}\Big(\frac{p+1}{2} + \frac{3+(-1)^{(p+1)/2}}{2}\cdot 5, p\Big) \\
&\qquad\qquad - \varDelta_{10}\Big(\frac{1-p}{2} + \frac{3+(-1)^{(p-1)/2}}{2}\cdot 5, p\Big)\Big] \\
&= 1 + \frac{(-1)^{(p-1)/2}}{10}\Big[\varDelta_{10}\Big(8 + \frac{p+(-1)^{(p+1)/2}5}{2}, p\Big) \\
&\qquad\qquad - \varDelta_{10}\Big(8 - \frac{p+(-1)^{(p+1)/2}5}{2}, p\Big)\Big] \\
&= 1 + \frac{(-1)^{(p-1)/2}}{10}[\varDelta_{10}(8+2m_1,p) - \varDelta_{10}(8-2m_1,p)]
\end{aligned}
$$

and that

$$
\begin{aligned}
pK_p(2p) &= p \sum_{\substack{k=1 \\ k\equiv 2p+5 \pmod{10}}}^{p-1} \frac{(-1)^{k-1}}{k} - p \sum_{\substack{k=1 \\ k\equiv 2p \pmod{10}}}^{p-1} \frac{(-1)^{k-1}}{k} \\
&\equiv T^p_{2p+5(10)} - T^p_{2p(10)} \pmod{p^2} \quad \text{(by Lemma 2)} \\
&= T^p_{2p+5(10)} - T^p_{-p(10)} = -(T^p_{2p(10)} - T^p_{-p+5(10)}) \\
&= (-1)^{(p+1)/2}\big[T^p_{2p+\frac{1+(-1)^{(p+1)/2}}{2}\cdot 5(10)} - T^p_{-p+\frac{1+(-1)^{(p+1)/2}}{2}\cdot 5(10)}\big] \\
&= \frac{(-1)^{(p+1)/2}}{10}\Big[\varDelta_{10}\Big(\frac{p+1}{2} + p + \frac{1+(-1)^{(p+1)/2}}{2}\cdot 5, p\Big) \\
&\qquad\qquad - \varDelta_{10}\Big(\frac{p+1}{2} - 2p + \frac{1+(-1)^{(p+1)/2}}{2}\cdot 5, p\Big)\Big] \\
&= \frac{(-1)^{(p+1)/2}}{10}\Big[\varDelta_{10}\Big(8 + \frac{p+(-1)^{(p+1)/2}5}{2}\cdot 3, p\Big) \\
&\qquad\qquad - \varDelta_{10}\Big(8 - \frac{p+(-1)^{(p+1)/2}5}{2}\cdot 3, p\Big)\Big] \\
&= \frac{(-1)^{(p+1)/2}}{10}[\varDelta_{10}(8+2m_2,p) - \varDelta_{10}(8-2m_2,p)].
\end{aligned}
$$

COROLLARY 1. *Let $p \ne 2, 5$ be a prime, and $q_p(5) = (5^{p-1}-1)/p$.*

(a) *If $p \equiv 1 \pmod 4$ then*

$$F_{(p+(\frac{5}{p}))/2} \equiv (-1)^{[(p-5)/10]}\Big(\frac{5}{p}\Big)5^{(p-1)/4}[p(K_p(0) + \tfrac{1}{2}q_p(5)) - 1] \pmod{p^2}$$

and

$$F_{(p-(\frac{5}{p}))/2} \equiv (-1)^{[(p-5)/10]} 5^{(p-1)/4} pK_p(2p) \pmod{p^2}.$$

(b) *If* $p \equiv 3 \pmod 4$ *then*

$$L_{(p+(\frac{5}{p}))/2} \equiv (-1)^{[(p-5)/10]} \left(\frac{5}{p}\right) 5^{(p+1)/4} [p(K_p(0) + \tfrac{1}{2}q_p(5)) - 1] \pmod{p^2}$$

and

$$L_{(p-(\frac{5}{p}))/2} \equiv (-1)^{[(p-5)/10]} 5^{(p+1)/4} pK_p(2p) \pmod{p^2}.$$

Proof. Observe that

$$\begin{aligned}\frac{1}{2}pq_p(5) &= \frac{1}{2}\left(5^{(p-1)/2} + \left(\frac{5}{p}\right)\right)\left(5^{(p-1)/2} - \left(\frac{5}{p}\right)\right)\\ &\equiv \frac{1}{2}\cdot 2\left(\frac{5}{p}\right)\left(5^{(p-1)/2} - \left(\frac{5}{p}\right)\right) = \left(\frac{5}{p}\right)5^{(p-1)/2} - 1 \pmod{p^2}.\end{aligned}$$

Now let us prove part (b). (Part (a) can be proved similarly.) Suppose $p \equiv 3 \pmod 4$. From Theorem 2 and the above observation we have

$$\begin{aligned}&\left(\frac{5}{p}\right)5^{(p+1)/4}p(K_p(0) + \tfrac{1}{2}q_p(5))\\ &\qquad \equiv 5^{(p+1)/4}(pK_p(0) + \tfrac{1}{2}pq_p(5))/5^{(p-1)/2} \pmod{p^2}\\ &\qquad \equiv 5^{(p+1)/4}\biggl(1 + (-1)^{[(p-5)/10]}5^{(p-3)/4}L_{(p+(\frac{5}{p}))/2}\\ &\qquad\qquad + \left(\frac{5}{p}\right)5^{(p-1)/2} - 1\biggr)\bigg/5^{(p-1)/2} \pmod{p^2}\\ &\qquad = (-1)^{[(p-5)/10]}L_{(p+(\frac{5}{p}))/2} + \left(\frac{5}{p}\right)5^{(p+1)/4}\end{aligned}$$

and

$$\begin{aligned}5^{(p+1)/4}pK_p(2p) &\equiv \left(\frac{5}{p}\right)5^{(p+1)/4}pK_p(2p)/5^{(p-1)/2} \pmod{p^2}\\ &\equiv \left(\frac{5}{p}\right)5^{(p+1)/4}\left((-1)^{[(p-5)/10]}\left(\frac{5}{p}\right)5^{(p-3)/4}L_{(p-(\frac{5}{p}))/2}\right)\bigg/5^{(p-1)/2} \pmod{p^2}\\ &= (-1)^{[(p-5)/10]}L_{(p-(\frac{5}{p}))/2}.\end{aligned}$$

This yields the desired result.

Corollary 2. *Let* $p \neq 2, 5$ *be a prime. We have*

(i) $2K_p(0) - K_p(2p) + \frac{1}{2}q_p(5) \equiv 0 \pmod p$.

(ii) *If* $p \equiv 1 \pmod 4$ *then*

$$L_{(p+(\frac{5}{p}))/2} \equiv (-1)^{[(p-5)/10]} 5^{(p-1)/4} [p(3K_p(2p) - K_p(0)) - 1] \pmod{p^2},$$

$$L_{(p-(\frac{5}{p}))/2} \equiv (-1)^{[(p-5)/10]}\left(\frac{5}{p}\right)5^{(p-1)/4}(\tfrac{1}{2}pq_p(5)-2) \pmod{p^2}.$$

(iii) *If* $p \equiv 3 \pmod 4$ *then*

$$F_{(p+(\frac{5}{p}))/2} \equiv (-1)^{[(p-5)/10]}5^{(p-3)/4}[p(3K_p(2p)-K_p(0))-1] \pmod{p^2},$$

$$F_{(p-(\frac{5}{p}))/2} \equiv (-1)^{[(p-5)/10]}\left(\frac{5}{p}\right)5^{(p-3)/4}(\tfrac{1}{2}pq_p(5)-2) \pmod{p^2}.$$

Proof. By part (i) of Theorem A one has

$$\begin{aligned}
L_{(p-1)/2} &= 2F_{(p+1)/2} - F_{(p-1)/2}, \\
L_{(p+1)/2} &= 2F_{(p+3)/2} - F_{(p+1)/2} = 2F_{(p-1)/2} + F_{(p+1)/2}, \\
5F_{(p-1)/2} &= 2L_{(p+1)/2} - L_{(p-1)/2}, \\
5F_{(p+1)/2} &= 2L_{(p+3)/2} - L_{(p+1)/2} = 2L_{(p-1)/2} + L_{(p+1)/2}.
\end{aligned}$$

It follows from Corollary 1 that

$$\begin{aligned}
&(-1)^{[(p-5)/10]}\left(\frac{5}{p}\right)5^{[(p-1)/4]}[p(2K_p(0)+q_p(5)-K_p(2p))-2] \\
&\equiv \begin{cases} 2F_{(p+(\frac{5}{p}))/2} - \left(\frac{5}{p}\right)F_{(p-(\frac{5}{p}))/2} = L_{(p-(\frac{5}{p}))/2} \pmod{p^2} \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{if } p\equiv 1 \pmod 4, \\ \frac{1}{5}\left(2L_{(p+(\frac{5}{p}))/2} - \left(\frac{5}{p}\right)L_{(p-(\frac{5}{p}))/2}\right) = F_{(p-(\frac{5}{p}))/2} \pmod{p^2} \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{if } p\equiv 3 \pmod 4 \end{cases}
\end{aligned}$$

and that

$$\begin{aligned}
&(-1)^{[(p-5)/10]}5^{[(p-1)/4]}[p(2K_p(2p)+K_p(0)+\tfrac{1}{2}q_p(5))-1] \\
&\equiv \begin{cases} 2F_{(p-(\frac{5}{p}))/2} + \left(\frac{5}{p}\right)F_{(p+(\frac{5}{p}))/2} = L_{(p+(\frac{5}{p}))/2} \pmod{p^2} \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{if } p\equiv 1 \pmod 4, \\ \frac{1}{5}\left(2L_{(p-(\frac{5}{p}))/2} + \left(\frac{5}{p}\right)L_{(p+(\frac{5}{p}))/2}\right) = F_{(p+(\frac{5}{p}))/2} \pmod{p^2} \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{if } p\equiv 3 \pmod 4. \end{cases}
\end{aligned}$$

For (i)–(iii) to hold it is sufficient to prove

$$2K_p(0) - K_p(2p) + q_p(5) \equiv \left(\frac{5}{p}\right)\frac{5^{(p-1)/2}-(\frac{5}{p})}{p} \ (\equiv \tfrac{1}{2}q_p(5)) \pmod p,$$

i.e.,

$$[1-p(2K_p(0)+q_p(5)-K_p(2p))]5^{(p-1)/2} \equiv \left(\frac{5}{p}\right) \pmod{p^2}.$$

To show this we note that

$$
\begin{aligned}
&4[1-p(2K_p(0)+q_p(5)-K_p(2p))]5^{(p-1)/2}\\
&\equiv \begin{cases} \Big((-1)^{[(p-5)/10]}\Big(\dfrac{5}{p}\Big)5^{(p-1)/4}[p(2K_p(0)+q_p(5) \\ \qquad -K_p(2p))-2]\Big)^2 - 5\cdot 0^2 \pmod{p^2} \ \text{ if } p\equiv 1 \pmod 4\,, \\ 5\Big((-1)^{[(p-5)/10]}\Big(\dfrac{5}{p}\Big)5^{(p-3)/4}[p(2K_p(0)+q_p(5) \\ \qquad -K_p(2p))-2]\Big)^2 - 0^2 \pmod{p^2} \ \text{ if } p\equiv 3 \pmod 4 \end{cases}\\
&\equiv \begin{cases} L^2_{(p-(\frac{5}{p}))/2} - 5F^2_{(p-(\frac{5}{p}))/2} \pmod{p^2} & \text{if } p\equiv 1 \pmod 4\,, \\ 5F^2_{(p-(\frac{5}{p}))/2} - L^2_{(p-(\frac{5}{p}))/2} \pmod{p^2} & \text{if } p\equiv 3 \pmod 4 \end{cases}
\end{aligned}
$$

(By Corollary 1, $p \mid F_{(p-(\frac{5}{p}))/2}$ if $p\equiv 1 \pmod 4$, $p\mid L_{(p-(\frac{5}{p}))/2}$ if $p\equiv 3 \pmod 4$.)

$$
\begin{aligned}
&= (-1)^{(p-1)/2}(L^2_{(p-(\frac{5}{p}))/2} - 5F^2_{(p-(\frac{5}{p}))/2})\\
&= 4(-1)^{(p-1)/2+(p-(\frac{5}{p}))/2} \qquad \text{(by Theorem A)}\\
&= 4(-1)^{(1-(\frac{5}{p}))/2} = 4\Big(\frac{5}{p}\Big)\,.
\end{aligned}
$$

This concludes the proof.

Corollary 3. *Let $p\neq 2,5$ be a prime. Then*

$$\frac{F_{p-(\frac{5}{p})}}{p} \equiv -2\sum_{\substack{k=1\\ k\equiv 2p \pmod 5}}^{p-1}\frac{1}{k} \equiv 2\sum_{\substack{k=1\\ 5\mid p+k}}^{p-1}\frac{1}{k} \pmod p\,.$$

Proof. By Theorem A and Corollaries 1, 2 we have

$$
\begin{aligned}
F_{p-(\frac{5}{p})} &= F_{(p-(\frac{5}{p}))/2}L_{(p-(\frac{5}{p}))/2} \equiv -2\Big(\frac{5}{p}\Big)5^{(p-1)/2}pK_p(2p)\\
&\equiv -2pK_p(2p) \equiv 2pK_p(-p) \pmod{p^2}\,.
\end{aligned}
$$

This yields the desired result.

Remark 3. For the Fibonacci quotient $F_{p-(\frac{5}{p})}/p$ ($p\neq 2,5$ is a prime), H. C. Williams [14] obtained the following formula:

$$\frac{F_{p-(\frac{5}{p})}}{p} \equiv \frac{2}{5}\sum_{k=1}^{p-1-[p/5]}\frac{(-1)^k}{k} \pmod p\,.$$

Compared with Williams' result, our Corollary 3 seems simple and beautiful.

4. A criterion for $p\mid F_{(p-1)/4}$. Let $p\ne 5$ be a prime of the form $4k+1$. By Corollary 1 if $p\equiv 13$ or $17\pmod{20}$ then

$$\begin{aligned}F_{(p-1)/4}L_{(p-1)/4}&=F_{(p-1)/2}=F_{(p+(\frac{5}{p}))/2}\\&\equiv -(-1)^{[(p-5)/10]}\left(\frac{5}{p}\right)5^{(p-1)/4}\not\equiv 0\pmod p\end{aligned}$$

and thus $p\nmid F_{(p-1)/4}$; if $p\equiv 1$ or $9\pmod{20}$ then

$$F_{(p-1)/4}L_{(p-1)/4}=F_{(p-1)/2}=F_{(p-(\frac{5}{p}))/2}\equiv 0\pmod p$$

and hence either $p\mid F_{(p-1)/4}$ or $p\mid L_{(p-1)/4}$.

Lemma 3. *Let $p\equiv 1$ or $9\pmod{20}$ be a prime. Then*

$$p\mid F_{(p-1)/4}\quad\textit{if and only if}\quad (-5)^{(p-1)/4}\equiv(-1)^{[(p+5)/10]}\pmod p\,.$$

Proof. By Theorem A we have

$$\begin{aligned}2F_{(p+1)/2}-F_{(p-1)/2}&=L_{(p-1)/2}=L^2_{(p-1)/4}-2(-1)^{(p-1)/4}\\&=5F^2_{(p-1)/4}+2(-1)^{(p-1)/4}\,.\end{aligned}$$

Since $p\equiv 1$ or $9\pmod{20}$, $p\mid F_{(p-1)/2}$ follows from Corollary 1. If $p\nmid F_{(p-1)/4}$ then $p\mid L_{(p-1)/4}$ (because $F_{(p-1)/2}=F_{(p-1)/4}L_{(p-1)/4}$) and hence (by the above)

$$2F_{(p+1)/2}-0\equiv 0^2-2(-1)^{(p-1)/4}\pmod p\,.$$

If $p\mid F_{(p-1)/4}$ then we have

$$2F_{(p+1)/2}-0\equiv 5\cdot 0^2+2(-1)^{(p-1)/4}\pmod p\,.$$

Now it is clear that

$$p\mid F_{(p-1)/4}\quad\text{iff}\quad F_{(p+1)/2}\equiv(-1)^{(p-1)/4}\pmod p\,.$$

By Corollary 1

$$\begin{aligned}F_{(p+1)/2}&=F_{(p+(\frac{5}{p}))/2}\equiv -(-1)^{[(p-5)/10]}\left(\frac{5}{p}\right)5^{(p-1)/4}\\&=(-1)^{[(p+5)/10]}5^{(p-1)/4}\pmod p\,.\end{aligned}$$

Therefore

$$p\mid F_{(p-1)/4}\quad\text{iff}\quad (-5)^{(p-1)/4}\equiv(-1)^{[(p+5)/10]}\pmod p\,.$$

Theorem 3. *Let p be a prime such that $p\equiv 1$ or $9\pmod{20}$ and hence $p=x^2+5y^2$ for some integers x, y. Then $p\mid F_{(p-1)/4}$ if and only if $4\mid xy$.*

Proof. Since p is a prime different from 5, without loss of generality we may suppose that x and y are positive integers. Obviously p, x, y are pairwise coprime.

Observe that $x^2 = p - 5y^2 \equiv p \pmod 5$. If $p \equiv 1 \pmod{20}$ then $x \equiv 1$ or $-1 \pmod 5$ and hence

$$\left(\frac{x}{5}\right) = 1 = (-1)^{[(p+5)/10]}\,.$$

If $p \equiv 9 \pmod{20}$ then $x^2 \equiv p \equiv 4 \pmod 5$, $x \equiv 2$ or $-2 \pmod 5$ and therefore

$$\left(\frac{x}{5}\right) = -1 = (-1)^{[(p+5)/10]}\,.$$

Suppose $x = 2^\alpha u$ $(2 \nmid u)$, $y = 2^\beta v$ $(2 \nmid v)$. Since

$$\left(\frac{x}{p}\right) \equiv (x^2)^{(p-1)/4} \equiv (-5y^2)^{(p-1)/4} \equiv (-5)^{(p-1)/4}\left(\frac{y}{p}\right) \pmod p\,,$$

by using Jacobi's symbol we have

$$\begin{aligned}
(-5)^{(p-1)/4} &\equiv \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = \left(\frac{2}{p}\right)^{\alpha+\beta}\left(\frac{u}{p}\right)\left(\frac{v}{p}\right) \pmod p\\
&= \left(\frac{2}{p}\right)^{\alpha+\beta}\left(\frac{p}{u}\right)\left(\frac{p}{v}\right) = \left(\frac{2}{p}\right)^{\alpha+\beta}\left(\frac{5y^2}{u}\right)\left(\frac{x^2}{v}\right)\\
&= \left(\frac{2}{p}\right)^{\alpha+\beta}\left(\frac{5}{u}\right) = \left(\frac{2}{p}\right)^{\alpha+\beta}\left(\frac{u}{5}\right) = (-1)^\alpha\left(\frac{2}{p}\right)^{\alpha+\beta}\left(\frac{2^\alpha u}{5}\right)\\
&= (-1)^\alpha\left(\frac{2}{p}\right)^{\alpha+\beta}\left(\frac{x}{5}\right) = (-1)^{\alpha+(\alpha+\beta)(p^2-1)/8}\cdot(-1)^{[(p+5)/10]}\,.
\end{aligned}$$

Applying Lemma 3 we get

$$p \mid F_{(p-1)/4} \quad \text{iff} \quad \alpha + (\alpha+\beta)\frac{p^2-1}{8} \equiv 0 \pmod 2\,.$$

C a s e 1. x is odd. In this case $\alpha = 0$, $\beta > 0$. (y must be even.) If $\beta = 1$ then $p = x^2 + 5y^2 = u^2 + 20v^2 \equiv 1 + 20 \cdot 1 \equiv 5 \pmod 8$ and hence

$$\alpha + (\alpha+\beta)\frac{p^2-1}{8} = \frac{p^2-1}{8} \equiv 1 \pmod 2\,.$$

If $\beta \geq 2$ then $p = x^2 + 5y^2 = u^2 + 5 \cdot 2^{2\beta}v^2 \equiv 1 + 5 \cdot 0 \equiv 1 \pmod 8$ and thus

$$\alpha + (\alpha+\beta)\frac{p^2-1}{8} = \frac{p^2-1}{8}\beta \equiv 0 \pmod 2\,.$$

C a s e 2. x is even. In this case $\alpha > 0$ and $\beta = 0$. (y must be odd.) If $\alpha = 1$ then $p = 4u^2 + 5v^2 \equiv 4 \cdot 1 + 5 \cdot 1 \equiv 1 \pmod 8$ and

$$\alpha + (\alpha+\beta)\frac{p^2-1}{8} = 1 + \frac{p^2-1}{8} \equiv 1 \pmod 2\,.$$

If $\alpha \geq 2$ then $p = 2^{2\alpha}u^2 + 5v^2 \equiv 0 + 5 \cdot 1 \equiv 5 \pmod 8$ and

$$\alpha + (\alpha+\beta)\frac{p^2-1}{8} = \alpha\left(1 + \frac{p^2-1}{8}\right) \equiv 0 \pmod 2\,.$$

Combining the above we get

$$p \mid F_{(p-1)/4} \Leftrightarrow \alpha + (\alpha+\beta)\frac{p^2-1}{8} \equiv 0 \pmod 2 \Leftrightarrow \alpha+\beta \geq 2 \Leftrightarrow 4 \mid xy\,.$$

This completes the proof.

Remark 4. In a quite different way E. Lehmer [3] proved Theorem 3 in the cases $p \equiv 1,\ 9 \pmod{40}$.

5. Connections with Fermat's last theorem. Fermat's last theorem (FLT) states that for every $n = 3, 4, 5, \ldots$ there are no integer solutions to the equation

$$x^n + y^n = z^n, \qquad xyz \neq 0\,.$$

Since the case $n = 4$ was settled by Fermat, without loss of generality we may consider FLT with odd prime exponents. Let p be an odd prime, if $x^p + y^p = z^p$ has no integer solution with $p \nmid xyz$ then we say that the first case of FLT (FLT1) holds for the exponent p, otherwise FTL1 fails for p.

In 1909 A. Wieferich (cf. [5]) proved that if $2^{p-1} \not\equiv 1 \pmod{p^2}$ (p is an odd prime) then FLT1 holds for the exponent p. In 1914 H. S. Vandiver [12] obtained the following result.

LEMMA 4. *If* FLT1 *fails for an odd prime* p, *then we have*

(a) $p \mid q_p(5)$, *i.e.* $5^{p-1} \equiv 1 \pmod{p^2}$,

(b) $5K_p(0) = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{[p/5]} \equiv 0 \pmod p$.

Now we are ready to give

THEOREM 4. *Suppose that* FLT1 *fails for an odd prime* p. *Then*

(i) $F_{p-(\frac{5}{p})} \equiv 0 \pmod{p^2}$,

(ii) $L_{p-(\frac{5}{p})} \equiv 2\left(\frac{5}{p}\right) \pmod{p^4}$,

(iii) $1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{[p/10]} \equiv 0 \pmod p$.

Proof. Since FLT holds for the exponents 3, 5 we have $p > 5$. By Lemma 4 and Corollary 2,

$$K_p(0) \equiv 0 \equiv q_p(5) \pmod p \quad \text{and} \quad K_p(2p) \equiv 2K_p(0) + \tfrac{1}{2}q_p(5) \equiv 0 \pmod p.$$

Therefore part (i) follows from Corollary 3.

As for part (ii), note that

$$L_{p-(\frac{5}{p})} = L^2_{(p-(\frac{5}{p}))/2} - 2(-1)^{(p-(\frac{5}{p}))/2} = 5F^2_{(p-(\frac{5}{p}))/2} + 2(-1)^{(p-(\frac{5}{p}))/2}$$

(by Theorem A). If $p \equiv 1 \pmod 4$ then $p^2 \mid F_{(p-(\frac{5}{p}))/2}$ (by $p \mid K_p(2p)$ and Corollary 1) and hence

$$L_{p-(\frac{5}{p})} \equiv 5 \cdot 0 + 2(-1)^{(p-(\frac{5}{p}))/2} = 2\left(\frac{5}{p}\right) \pmod{p^4}.$$

If $p \equiv 3 \pmod 4$ then $p^2 \mid L_{(p-(\frac{5}{p}))/2}$ (by $p \mid K_p(2p)$ and Corollary 1) and thus

$$L_{p-(\frac{5}{p})} \equiv 0 - 2(-1)^{(p-(\frac{5}{p}))/2} = 2\left(\frac{5}{p}\right) \pmod{p^4}.$$

This proves part (ii).

Concerning part (iii) we have

$$\begin{aligned}
&1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{[p/10]} \\
&\quad = \sum_{k=1}^{[p/5]} \frac{1}{k} + \sum_{k=1}^{[p/5]} \frac{(-1)^k}{k} \equiv \sum_{k=1}^{[p/5]} \frac{(-1)^k}{k} \equiv -\sum_{k=1}^{[p/5]} \frac{(-1)^k}{p-k} \pmod p \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(by Lemma 4)} \\
&\quad = -\sum_{k=p-[p/5]}^{p-1} \frac{(-1)^{k-1}}{k} = -\Big(\sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k} + \sum_{k=1}^{p-1-[p/5]} \frac{(-1)^k}{k}\Big) \\
&\quad \equiv -\left(\frac{2^p-2}{p} + \frac{5}{2} \cdot \frac{F_{p-(\frac{5}{p})}}{p}\right) \pmod p \\
&\qquad\qquad\qquad\qquad\qquad\qquad \text{(by Eisenstein's and Williams' results)} \\
&\quad \equiv 0 \pmod p \quad \text{(by Wieferich's result and part (i))}.
\end{aligned}$$

This concludes the proof.

Remark 5. By Theorem 4, FLT1 is implied by the positive answer to Wall's question (see [13]). According to Williams [14], $p^2 \nmid F_{p-(\frac{5}{p})}$ for every odd prime p less than 10^9.

Let $d \in \mathbb{Z}^+$. By Remark 1, d is a divisor of some positive Fibonacci number. Let $n(d)$ denote the least positive integer n such that d divides F_n. From Theorem B we have

$$d \mid F_m \Leftrightarrow d \mid (F_m, F_{n(d)}) \Leftrightarrow d \mid F_{(m,n(d))} \Leftrightarrow (m, n(d)) = n(d) \Leftrightarrow n(d) \mid m$$

and

$$n(d) \mid m \Rightarrow F_{n(d)} \mid F_m \Rightarrow d \mid F_m \Rightarrow n(d) \mid m.$$

LEMMA 5. *Let $p \neq 2, 5$ be a prime. Suppose $p \mid F_m$ and $p \nmid m$. Then*

$$n(p) = n(p^2) \quad \text{iff} \quad p^2 \mid F_m .$$

In particular, $n(p) = n(p^2)$ *if and only if* $p^2 \mid F_{p-(\frac{5}{p})}$.

Proof. Since $p \mid F_m$ we have $n(p) \mid m$, $F_{n(p)} \mid F_m$. If $n(p) = n(p^2)$ then $p^2 \mid F_{n(p)}$ and hence $p^2 \mid F_m$.

Observe that $p \nmid \frac{m}{n(p)}$. If $n(p) \neq n(p^2)$ then $p \| F_{n(p)}$ and hence by Theorem C we have $p^2 \nmid F_{n(p)\cdot\frac{m}{n(p)}}$.

To end the proof we note that p divides $F_{p-(\frac{5}{p})}$.

LEMMA 6. *Let m and n be integers greater than one. Then $F_{mn} > F_m^2 F_n^2$.*

Proof. By Theorem B,

$$F_{mn} = \sum_{i=1}^{n} \binom{n}{i} F_{m-1}^{n-i} F_m^i F_i \quad \text{and} \quad F_{2n} = \sum_{i=1}^{n} \binom{n}{i} F_i .$$

From Theorem A it follows that

$$\sum_{i=2}^{n} \binom{n}{i} F_i = F_{2n} - \binom{n}{1} = F_n L_n - n = F_n(2F_{n+1} - F_n) - n$$
$$= F_n(F_n + 2F_{n-1}) - n \geq F_n^2 .$$

(Note that $F_2 < F_3 < F_4 < \ldots$ and that $2F_nF_{n-1} > F_n \geq F_2 + (n-2) = n-1$.) So we have

$$F_{mn} > \sum_{i=2}^{n} \binom{n}{i} F_{m-1}^{n-i} F_m^i F_i \geq \sum_{i=2}^{n} \binom{n}{i} F_i F_m^2 \geq F_n^2 F_m^2 .$$

Remark 6. Provided that $n_1, \ldots, n_k$ ($k \geq 2$) are integers greater than one (by Lemma 6), we have

$$F_{n_1\ldots n_k} > F_{n_1\ldots n_{k-1}}^2 F_{n_k}^2 \geq F_{n_1\ldots n_{k-1}} F_{n_k}^2$$
$$\geq F_{n_1\ldots n_{k-2}} F_{n_{k-1}}^2 F_{n_k}^2 \geq \ldots \geq F_{n_1}^2 \ldots F_{n_k}^2 .$$

Now we are able to give

THEOREM 5. FLT1 *holds for any odd prime of the form*

$$F_{mn_1\ldots n_k}/[F_{n_1}, \ldots, F_{n_k}] .$$

Proof. Suppose that $p = F_{mn_1\ldots n_k}/[F_{n_1}, \ldots, F_{n_k}]$ is an odd prime. Without loss of generality we may let $n_1 \geq n_2 \geq \ldots \geq n_k \geq 1$.

Now we claim that $p \| F_{mn_1\ldots n_k}$. In the case $n_1 = \ldots = n_k = 1$ this holds trivially (since $p = F_{mn_1\ldots n_k}$). For the other cases we will obtain the result by showing

$$F_{mn_1\ldots n_k} > F_{n_1}^2 \ldots F_{n_k}^2 \geq [F_{n_1}, \ldots, F_{n_k}]^2 \quad (\text{and hence } p^2 > F_{mn_1\ldots n_k}) .$$

In fact, if $n_1 > 1 = n_2 = \ldots = n_k$ then $m > 1$ (since $F_{mn_1} = pF_{n_1} > F_{n_1}$) and hence by Lemma 6

$$F_{mn_1\ldots n_k} = F_{mn_1} \geq F_{2n_1} > F_2^2 F_{n_1}^2 = F_{n_1}^2 = F_{n_1}^2 \ldots F_{n_k}^2 ;$$

if $n_1 \geq n_2 \geq \ldots \geq n_s > 1 = n_{s+1} = \ldots = n_k$ $(s \geq 2)$ then by Remark 6

$$F_{mn_1\ldots n_k} = F_{mn_1\ldots n_s} \geq F_{n_1\ldots n_s} > F_{n_1}^2 \ldots F_{n_s}^2 = F_{n_1}^2 \ldots F_{n_k}^2 .$$

This completes the proof of the claim.

Since FLT holds for the exponents 3, 5 we assume $p > 5$. By the claim $p \| F_{mn_1\ldots n_k}$. Since $n(p) \mid mn_1 \ldots n_k$ and $F_{n(p)} \mid F_{mn_1\ldots n_k}$ we have $p \| F_{n(p)}$ and hence $n(p) \neq n(p^2)$. Applying Lemma 5 we get $p^2 \nmid F_{p-(\frac{5}{p})}$. From this and Theorem 4 it follows that FLT1 holds for the exponent p.

EXAMPLES. Since $7 = 21/3 = F_8/F_4$, $61 = 610/(2 \cdot 5) = F_{15}/[F_3, F_5]$, by Theorem 5 FLT1 holds for the exponents 7 and 61.

COROLLARY 4. FLT1 *holds for all* (*odd*) *Fibonacci primes and Lucas primes.*

Proof. Observe that $F_n = F_{n\cdot 1}/F_1$ and that $L_n = F_{2n}/F_n$. Applying Theorem 5 we obtain the desired result.

Acknowledgement. The authors thank the referee for his valuable advice to make the paper readable.

Added in proof. Prof. A. Schinzel informs us that part (iii) of Theorem 4 has been claimed earlier by L. Skula, *Fermat's Last Theorem and the Fermat quatient* at the 9th Czechoslovak Conference on Number Theory (Računkova Dolina 1989).

References

[1] L. E. Dickson, *History of the Theory of Numbers*, Vol. I, Chelsea, New York 1952, 105, 393–396.

[2] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford Univ. Press, Oxford 1981, 148–150.

[3] E. Lehmer, *On the quartic character of quadratic units*, J. Reine Angew. Math. 268/269 (1974), 294–301.

[4] L. J. Mordell, *Diophantine Equations*, Academic Press, London and New York 1969, 60–61.

[5] P. Ribenboim, 13 *Lectures on Fermat's Last Theorem*, Springer, New York 1979, 139–159.

[6] Zhi-Hong Sun, *Combinatorial sum* $\sum_{\substack{k=0 \\ k\equiv r \pmod m}}^{n} \binom{n}{k}$ *and its applications in number theory (I)*, J. Nanjing Univ. Biquarterly, in press.

[7] —, *Combinatorial sum* $\sum_{\substack{k=0 \\ k\equiv r \pmod m}}^{n} \binom{n}{k}$ *and its applications in number theory (II)*, ibid., in press.

[8] Zhi-Wei Sun, *A congruence for primes*, preprint, 1991.

[9] —, *On the combinatorial sum* $\sum_{k\equiv r \pmod m} \binom{n}{k}$, submitted.

[10] —, *Combinatorial sum* $\sum_{k\equiv r \pmod{12}} \binom{n}{k}$ *and its number-theoretical applications*, to appear.

[11] —, *Reduction of unknowns in Diophantine representations*, Science in China (Ser. A) 35 (1992), 1–13.

[12] H. S. Vandiver, *Extension of the criteria of Wieferich and Mirimanoff in connection with Fermat's last theorem*, J. Reine Angew. Math. 144 (1914), 314–318.

[13] D. D. Wall, *Fibonacci series modulo m*, Amer. Math. Monthly 67 (1960), 525–532.

[14] H. C. Williams, *A note on the Fibonacci quotient* $F_{p-\varepsilon}/p$, Canad. Math. Bull. 25 (1982), 366–370.

DEPARTMENT OF MATHEMATICS
NANJING UNIVERSITY
NANJING 210008
PEOPLE'S REPUBLIC OF CHINA

Received on 27.11.1990
and in revised form on 16.5.1991 (2101)