Last revised: 30 December 2003

CONGRUENCES FOR FIBONACCI NUMBERS

Zhi-Hong Sun

Department of Mathematics, Huaiyin Teachers College,
Huaian, Jiangsu 223001, P.R. China
E-mail: hyzhsun@public.hy.js.cn
Homepage: http://www.hytc.cn/xsjl/szh

1. Basic properties of Fibonacci numbers.

The Fibonacci sequence $\{F_n\}$ was introduced by Italian mathematician Leonardo Fibonacci (1175-1250) in 1202. For integers n, $\{F_n\}$ is defined by

$$F_0 = 0,\ F_1 = 1,\ F_{n+1} = F_n + F_{n-1}\ (n = 0, \pm 1, \pm 2, \pm 3, \dots).$$

The first few Fibonacci numbers are shown below:

$n:$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$F_n:$	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610

The companion of Fibonacci numbers is the Lucas sequence $\{L_n\}$ given by

$$L_0 = 2,\ L_1 = 1,\ L_{n+1} = L_n + L_{n-1} \quad (n = 0, \pm 1, \pm 2, \pm 3, \dots).$$

It is easily seen that

$$F_{-n} = (-1)^{n-1}F_n, \quad L_{-n} = (-1)^n L_n \tag{1.1}$$

and

$$L_n = F_{n+1} + F_{n-1}, \quad F_n = \frac{1}{5}(L_{n+1} + L_{n-1}). \tag{1.2}$$

Using induction one can easily prove the following Binet's formulas (see [D],[R2]):

$$F_n = \frac{1}{\sqrt{5}}\left\{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right\}, \tag{1.3}$$

$$L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n. \tag{1.4}$$

In 2001 Z.H.Sun[S5] announced a general identity for Lucas sequences. Putting $a_1 = a_2 = -1$, $U_n = F_n$ and $U'_n = F_n$ or L_n in the identity (4.2) of [S5] we get the following two identities, which involve many known results.

Theorem 1.1. *Let k, m, n, s be integers with $m \geq 0$. Then*

$$F_s^m F_{km+n} = \sum_{j=0}^{m} \binom{m}{j} (-1)^{(s-1)(m-j)} F_k^j F_{k-s}^{m-j} F_{js+n} \tag{1.5}$$

and

$$F_s^m L_{km+n} = \sum_{j=0}^{m} \binom{m}{j} (-1)^{(s-1)(m-j)} F_k^j F_{k-s}^{m-j} L_{js+n}. \tag{1.6}$$

Proof. Let $x = (1+\sqrt{5})/2$ and $y = (1-\sqrt{5})/2$. Then $x+y=1$, $xy=-1$ and $F_r = (x^r - y^r)/(x-y)$. Thus applying the binomial theorem we obtain

$$\begin{aligned}
&\sum_{j=0}^{m} \binom{m}{j} (-1)^{(s-1)(m-j)} F_k^j F_{k-s}^{m-j} F_{js+n} \\
&= \sum_{j=0}^{m} \binom{m}{j} (-1)^{(s-1)(m-j)} \left(\frac{x^k - y^k}{x-y}\right)^j \left(\frac{x^{k-s} - y^{k-s}}{x-y}\right)^{m-j} \cdot \frac{x^{js+n} - y^{js+n}}{x-y} \\
&= \frac{1}{(x-y)^{m+1}} \sum_{j=0}^{m} \binom{m}{j} (x^{js+n} - y^{js+n})(x^k - y^k)^j (x^s y^k - x^k y^s)^{m-j} \\
&= \frac{1}{(x-y)^{m+1}} \Big\{ x^n \sum_{j=0}^{m} \binom{m}{j} (x^{k+s} - x^s y^k)^j (x^s y^k - x^k y^s)^{m-j} \\
&\qquad - y^n \sum_{j=0}^{m} \binom{m}{j} (x^k y^s - y^{k+s})^j (x^s y^k - x^k y^s)^{m-j} \Big\} \\
&= \frac{1}{(x-y)^{m+1}} \left\{ x^n (x^{k+s} - x^k y^s)^m - y^n (x^s y^k - y^{k+s})^m \right\} \\
&= \frac{1}{(x-y)^{m+1}} (x^n \cdot x^{km} - y^n \cdot y^{km})(x^s - y^s)^m = \left(\frac{x^s - y^s}{x-y}\right)^m \cdot \frac{x^{km+n} - y^{km+n}}{x-y} \\
&= F_s^m F_{km+n}.
\end{aligned}$$

This proves (1.5).

As for (1.6), noting that $L_r = F_r + 2F_{r-1}$ and then applying (1.5) we get

$$\begin{aligned}
&\sum_{j=0}^{m} \binom{m}{j} (-1)^{(s-1)(m-j)} F_k^j F_{k-s}^{m-j} L_{js+n} \\
&= \sum_{j=0}^{m} \binom{m}{j} (-1)^{(s-1)(m-j)} F_k^j F_{k-s}^{m-j} F_{js+n} + 2 \sum_{j=0}^{m} \binom{m}{j} (-1)^{(s-1)(m-j)} F_k^j F_{k-s}^{m-j} F_{js+n-1} \\
&= F_s^m F_{km+n} + 2F_s^m F_{km+n-1} = F_s^m L_{km+n}.
\end{aligned}$$

This completes the proof.

In the special case $s=1$ and $n=0$, (1.5) is due to H.Siebeck ([D,p.394]), and the general case $s=1$ of (1.5) is due to Z.W.Sun.

Taking $m=1$ in (1.5) and (1.6) we get

$$(1.7)\qquad F_sF_{k+n}=F_kF_{n+s}-(-1)^sF_{k-s}F_n,\quad F_sL_{k+n}=F_kL_{n+s}-(-1)^sF_{k-s}L_n.$$

From this we have the following well-known results (see [D],[R1] and [R2]):

$$(1.8)\qquad (Catalan)\qquad F_{k+n}F_{k-n}=F_k^2-(-1)^{k-n}F_n^2,$$

$$(1.9)\qquad F_{2n}=F_nL_n,\ F_{2n+1}=F_n^2+F_{n+1}^2,\ L_{2n}=L_n^2-2(-1)^n.$$

Putting $n=1$ in (1.8) we find $F_{k-1}F_{k+1}-F_k^2=(-1)^k$ and so F_{k-1} is prime to F_k.

For $m\ge 1$ it follows from (1.5) that

$$(1.10)\quad F_s^mF_{km+n}\equiv(-1)^{(s-1)m}F_{k-s}^mF_n+(-1)^{(s-1)(m-1)}mF_kF_{k-s}^{m-1}F_{n+s}\ (\mathrm{mod}\ F_k^2).$$

So

$$(1.11)\qquad F_{km+n}\equiv F_{k-1}^mF_n+mF_kF_{k-1}^{m-1}F_{n+1}\ (\mathrm{mod}\ F_k^2)$$

and hence

$$(1.12)\qquad F_{km}\equiv mF_kF_{k-1}^{m-1}\ (\mathrm{mod}\ F_k^2).$$

Let (a,b) be the greatest common divisor of a and b. From the above we see that

$$(F_{km+n},F_k)=(F_{k-1}^mF_n,F_k)=(F_k,F_n).$$

From this and Euclid's algorithm for finding the greatest common divisor of two given numbers, we have the following beautiful result due to E.Lucas (see [D] and [R1]).

Theorem 1.2 (Lucas' theorem). *Let m and n be positive integers. Then*

$$(F_m,F_n)=F_{(m,n)}.$$

Corollary 1.1. *If m and n are positive integers with $m\ne 2$, then*

$$F_m\mid F_n\iff m\mid n.$$

Proof. From Lucas' theorem we derive that

$$m\mid n\iff (m,n)=m\iff F_{(m,n)}=F_m\iff (F_m,F_n)=F_m\iff F_m\mid F_n.$$

2. Congruences for F_p and $F_{p\pm1}$ modulo p.

Let $(\frac{a}{p})$ be the Legendre symbol of a and p. For $p \neq 2,5$, using quadratic reciprocity law we see that

$$(\frac{5}{p}) = (\frac{p}{5}) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 5, \\ -1 & \text{if } p \equiv \pm 2 \pmod 5). \end{cases}$$

From [D] and [R1] we have the following well-known congruences.

Theorem 2.1(Legendre,Lagrange). *Let p be an odd prime. Then*

$$L_p \equiv 1 \pmod p \quad \textit{and} \quad F_p \equiv \left(\frac{p}{5}\right) \pmod p.$$

Proof. Since

$$\binom{p}{k} k! = p(p-1)\cdots(p-k+1) \equiv 0 \pmod p,$$

we see that $p \mid \binom{p}{k}$ for $k = 1, 2, \ldots, p-1$. From this and (1.4) we see that

$$\begin{aligned} L_p &= \left(\frac{1+\sqrt{5}}{2}\right)^p + \left(\frac{1-\sqrt{5}}{2}\right)^p \\ &= \frac{1}{2^p} \sum_{k=0}^{p} \binom{p}{k} \left((\sqrt{5})^k + (-\sqrt{5})^k\right) \\ &= \frac{1}{2^{p-1}} \sum_{\substack{k=0 \\ 2|k}}^{p} \binom{p}{k} 5^{\frac{k}{2}} \equiv \frac{1}{2^{p-1}} \equiv 1 \pmod p. \end{aligned}$$

Similarly, by using (1.3) and Euler's criterion we get

$$\begin{aligned} F_p &= \frac{1}{\sqrt{5}} \left\{ \left(\frac{1+\sqrt{5}}{2}\right)^p - \left(\frac{1-\sqrt{5}}{2}\right)^p \right\} \\ &= \frac{1}{\sqrt{5}\cdot 2^p} \sum_{k=0}^{p} \binom{p}{k} \left((\sqrt{5})^k - (-\sqrt{5})^k\right) \\ &= \frac{1}{2^{p-1}} \sum_{\substack{k=0 \\ 2\nmid k}}^{p} \binom{p}{k} 5^{\frac{k-1}{2}} \equiv 5^{\frac{p-1}{2}} \equiv (\frac{5}{p}) = (\frac{p}{5}) \pmod p. \end{aligned}$$

This proves the theorem.

Theorem 2.2(Legendre,Lagrange). *Let p be an odd prime. Then*

$$F_{p-1} \equiv \frac{1-(\frac{p}{5})}{2} \pmod p \quad \textit{and} \quad F_{p+1} \equiv \frac{1+(\frac{p}{5})}{2} \pmod p.$$

Proof. From (1.2) we see that

$$L_p = F_{p+1} + F_{p-1} = F_p + 2F_{p-1} = 2F_{p+1} - F_p.$$

Thus

$$F_{p-1} = \frac{L_p - F_p}{2} \quad \text{and} \quad F_{p+1} = \frac{L_p + F_p}{2}.$$

This together with Theorem 2.1 yields the result.

Corollary 2.1. *Let p be a prime. Then $p \mid F_{p-(\frac{p}{5})}$.*

Corollary 2.2. *Let $p > 3$ be a prime, and let q be a prime divisor of F_p. Then*

$$q \equiv \left(\frac{q}{5}\right) \pmod p \quad \textit{and} \quad q \equiv 1 \pmod 4.$$

Proof. From Corollary 2.1 we know that $q \mid F_{q-(\frac{q}{5})}$. Thus $q \mid (F_{q-(\frac{q}{5})}, F_p)$. Applying Lucas' theorem we get $q \mid F_{(p,q-(\frac{q}{5}))}$. Hence $(p, q-(\frac{q}{5})) = p$ and so $p \mid q-(\frac{q}{5})$.

Since $p > 3$ is a prime, by Corollary 1.1 we have $F_3 \nmid F_p$ and hence F_p and q are odd. By (1.9) we have $F^2_{\frac{p+1}{2}} + F^2_{\frac{p-1}{2}} = F_p \equiv 0 \pmod q$. Observing that $(F_{\frac{p+1}{2}}, F_{\frac{p-1}{2}}) = 1$ we get $q \nmid F_{\frac{p+1}{2}} F_{\frac{p-1}{2}}$. Hence $(F_{\frac{p+1}{2}}/F_{\frac{p-1}{2}})^2 \equiv -1 \pmod q$ and so $q \equiv 1 \pmod 4$. This finishes the proof.

3. Lucas' law of repetition.

For any integer k, using (1.3) and (1.4) one can easily prove the following well-known identity:

$$L_k^2 - 5F_k^2 = 4(-1)^k. \tag{3.1}$$

From (3.1) we see that $(L_k, F_k) = 1$ or 2.

Let $k, n \in \mathbb{Z}$ with $k \neq 0$. Putting $s = -k$ in (1.7) and then applying (1.1) we find

$$(-1)^{k-1} F_k F_{k+n} = F_k F_{n-k} - (-1)^k F_{2k} F_n.$$

Since $F_{2k} = F_k L_k$ and $F_k \neq 0$ we see that

$$F_{k+n} = L_k F_n + (-1)^{k-1} F_{n-k}. \tag{3.2}$$

This identity is due to E.Lucas ([D]).

Using (3.2) we can prove

Theorem 3.1. *Let k and n be integers with $k \neq 0$. Then*

$$\frac{F_{kn}}{F_k} \equiv \begin{cases} (-1)^{km}(2m+1) \pmod{5F_k^2} & \textit{if } n = 2m+1, \\ (-1)^{k(m-1)} m L_k \pmod{5F_k^2} & \textit{if } n = 2m. \end{cases}$$

Proof. By (1.1) we have $F_{-kn} = (-1)^{kn-1} F_{kn}$. From this we see that it suffices to prove the result for $n \geq 0$. Clearly the result is true for $n = 0, 1$. Now suppose $n \geq 2$ and the result is true for all positive integers less than n. From (3.2) we see that $F_{kn} = L_k F_{(n-1)k} + (-1)^{k-1} F_{(n-2)k}$. Since $L_k^2 = 5F_k^2 + 4(-1)^k \equiv 4(-1)^k \pmod{5F_k^2}$ by (3.1), using the inductive hypothesis we obtain

$$\begin{aligned} \frac{F_{kn}}{F_k} &= L_k \frac{F_{(n-1)k}}{F_k} + (-1)^{k-1} \frac{F_{(n-2)k}}{F_k} \\ &\equiv \begin{cases} L_k \cdot (-1)^{k(m-1)} m L_k + (-1)^{k-1} \cdot (-1)^{k(m-1)}(2m-1) \\ \qquad \equiv (-1)^{km}(2m+1) \pmod{5F_k^2} \qquad \text{if } n = 2m+1, \\ L_k \cdot (-1)^{k(m-1)}(2m-1) + (-1)^{k-1} \cdot (-1)^{km}(m-1)L_k \\ \qquad = (-1)^{k(m-1)} m L_k \pmod{5F_k^2} \qquad \text{if } n = 2m. \end{cases} \end{aligned}$$

This shows that the result is true for n. So the theorem is proved by induction.

Clearly Theorem 3.1 is much better than (1.12).

Corollary 3.1. *Let $k \neq 0$ be an integer, and let p be an odd prime divisor of F_k. Then*

$$\frac{F_{kp}}{F_k} \equiv p \pmod{5p^2}.$$

Proof. Since $p \mid F_k$ we see that $5p^2 \mid 5F_k^2$. So, by Theorem 3.1 we get

$$\frac{F_{kp}}{F_k} \equiv (-1)^{\frac{p-1}{2}k} p \pmod{5p^2}.$$

Since $L_k^2 = 5F_k^2 + 4(-1)^k \equiv 4(-1)^k \pmod{p}$ we see that $2 \mid k$ if $p \equiv 3 \pmod{4}$. So $\frac{p-1}{2}k \equiv 0 \pmod{2}$ and hence $F_{kp}/F_k \equiv p \pmod{5p^2}$.

For prime p and integer $n \neq 0$ let $\mathrm{ord}_p n$ be the order of n at p. That is, $p^{\mathrm{ord}_p n} \mid n$ but $p^{\mathrm{ord}_p n+1} \nmid n$. From Corollary 3.1 we have

Theorem 3.2 (Lucas' law of repetition ([D],[R2])). *Let k and m be nonzero integers. If p is an odd prime divisor of F_k, then*

$$\mathrm{ord}_p F_{km} = \mathrm{ord}_p F_k + \mathrm{ord}_p m.$$

Proof. Write $m = p^\alpha m_0$ with $p \nmid m_0$. Then $\mathrm{ord}_p m = \alpha$. Since $p \mid F_k$ we have $p \nmid L_k$ by (3.1). Thus using Theorem 3.1 we see that $F_{km_0}/F_k \not\equiv 0 \pmod{p}$. Observing that

$$\frac{F_{km}}{F_k} = \frac{F_{km_0}}{F_k} \cdot \prod_{s=1}^{\alpha} \frac{F_{p^s m_0 k}}{F_{p^{s-1} m_0 k}}$$

and $\mathrm{ord}_p(F_{p^s m_0 k}/F_{p^{s-1} m_0 k}) = p$ by Corollary 3.1, we then get $\mathrm{ord}_p(F_{km}/F_k) = \alpha$. This yields the result.

Definition 3.1. *For positive integer m let $r(m)$ denote the least positive integer n such that $m \mid F_n$. We call $r(m)$ the rank of appearance of m in the Fibonacci sequence.*

From Theorem 1.2 we have the following well-known result (see [D],[R1],[R2]).

Lemma 3.1. *Let m and n be positive integers. Then $m \mid F_n$ if and only if $r(m) \mid n$.*

Proof. From Theorem 1.2 and the definition of $r(m)$ we see that

$$\begin{aligned} m \mid F_n &\iff m \mid (F_n, F_{r(m)}) \iff m \mid F_{(n,r(m))} \\ &\iff (n, r(m)) = r(m) \iff r(m) \mid n. \end{aligned}$$

This proves the lemma.

If $p \neq 2, 5$ is a prime, $p^\beta \mid F_{r(p)}$ and $p^{\beta+1} \nmid F_{r(p)}$, then clearly $r(p^\alpha) = r(p)$ for $\alpha \leq \beta$. When $\alpha > \beta$, from Theorem 3.2 and Lemma 3.1 we see that $r(p^\alpha) = p^{\alpha-\beta} r(p)$. This is the original form of Lucas' law of repetition given by Lucas ([D]).

Theorem 3.3. *Let m be a positive integer. If $p \neq 2, 5$ is a prime such that $p \mid F_m$, then* $\mathrm{ord}_p F_m = \mathrm{ord}_p F_{p-(\frac{p}{5})} + \mathrm{ord}_p m$.

Proof. Since $p \mid F_{p-(\frac{p}{5})}$ by Corollary 2.1, using Lemma 3.1 we see that $r(p) \mid p - (\frac{p}{5})$ and $r(p) \mid m$. From Theorem 3.2 we know that

$$\mathrm{ord}_p F_{p-(\frac{p}{5})} = \mathrm{ord}_p F_{r(p)} + \mathrm{ord}_p \left(\frac{p-(\frac{p}{5})}{r(p)} \right) \quad \text{and} \quad \mathrm{ord}_p F_m = \mathrm{ord}_p F_{r(p)} + \mathrm{ord}_p \left(\frac{m}{r(p)} \right).$$

Since $p \nmid p - (\frac{p}{5})$ and so $p \nmid r(p)$ we obtain the desired result.

Corollary 3.2. *Let m be a positive integer. If $p \neq 2, 5$ is a prime such that $p \mid L_m$, then* $\mathrm{ord}_p L_m = \mathrm{ord}_p F_{p-(\frac{p}{5})} + \mathrm{ord}_p m$.

Proof. Since $F_{2m} = F_m L_m$ and $(F_m, L_m) \mid 2$ we see that $p \nmid F_m$ and $p \mid F_{2m}$. Thus applying Theorem 3.3 we have

$$\mathrm{ord}_p L_m = \mathrm{ord}_p F_{2m} = \mathrm{ord}_p F_{p-(\frac{p}{5})} + \mathrm{ord}_p (2m) = \mathrm{ord}_p F_{p-(\frac{p}{5})} + \mathrm{ord}_p m.$$

This is the result.

Theorem 3.4. *Let $\{S_n\}$ be given by $S_1 = 3$ and $S_{n+1} = S_n^2 - 2 (n \geq 1)$. If p is a prime divisor of S_n, then $p^\alpha \mid S_n$ if and only if $p^\alpha \mid F_{p-(\frac{p}{5})}$.*

Proof. Clearly $2 \nmid S_n$ and $5 \nmid S_n$. Thus $p \neq 2, 5$. From (1.9) we see that $S_n = L_{2^n}$. Thus by Corollary 3.2 we have

$$\mathrm{ord}_p S_n = \mathrm{ord}_p L_{2^n} = \mathrm{ord}_p F_{p-(\frac{p}{5})} + \mathrm{ord}_p 2^n = \mathrm{ord}_p F_{p-(\frac{p}{5})}.$$

This yields the result.

We note that if p is a prime divisor of S_n, then $p \equiv (\frac{p}{5}) \pmod{2^{n+1}}$. This is because $r(p) = 2^{n+1}$ and $r(p) \mid p - (\frac{p}{5})$.

4. Congruences for the Fibonacci quotient $F_{p-(\frac{p}{5})}/p \pmod p$.

From now on let $[x]$ be the greatest integer not exceeding x and $q_p(a) = (a^{p-1} - 1)/p$. For prime $p > 5$, it follows from Corollary 2.1 that $F_{p-(\frac{p}{5})}/p \in \mathbb{Z}$. So the next natural problem is to determine the so-called Fibonacci quotient $F_{p-(\frac{p}{5})}/p \pmod p$.

Theorem 4.1. *Let p be a prime greater than 5. Then*

(1) (Z.H.Sun and Z.W.Sun[SS],1992) $\frac{F_{p-(\frac{5}{p})}}{p} \equiv -2 \sum_{\substack{k=1 \\ k \equiv 2p \pmod 5}}^{p-1} \frac{1}{k} \pmod p$.

(2) (H.C.Williams[W2], 1991) $\frac{F_{p-(\frac{5}{p})}}{p} \equiv \frac{2}{5} \sum_{\frac{p}{5} < k < \frac{2p}{5}} \frac{1}{k} \pmod p$.

(3) (Z.H.Sun[S2],1995) $\frac{F_{p-(\frac{5}{p})}}{p} \equiv \frac{2}{5} \sum_{1 \leq k < \frac{2p}{5}} \frac{(-1)^{k-1}}{k} \pmod p$.

(4) (H.C.Williams[W1], 1982) $\frac{F_{p-(\frac{5}{p})}}{p} \equiv -\frac{2}{5} \sum_{1 \le k < \frac{4p}{5}} \frac{(-1)^{k-1}}{k} \pmod p$.

(5) (Z.H.Sun[S2],1995) $\frac{F_{p-(\frac{5}{p})}}{p} \equiv \frac{2}{5} \sum_{\frac{p}{5} < k < \frac{p}{3}} \frac{(-1)^k}{k} \pmod p$.

(6) (Z.H.Sun[S2],1995) $\frac{F_{p-(\frac{5}{p})}}{p} \equiv 6 \sum_{\substack{k=1 \\ k \equiv 4p \pmod{15}}}^{p-1} \frac{(-1)^{k-1}}{k} - 6 \sum_{\substack{k=1 \\ k \equiv 5p \pmod{15}}}^{p-1} \frac{(-1)^{k-1}}{k} \pmod p$.

(7) (Z.H.Sun[S2],1995) $\frac{F_{p-(\frac{5}{p})}}{p} \equiv -\frac{4}{3} \sum_{\substack{k=1 \\ k \equiv 2p, 3p \pmod{10}}}^{p-1} \frac{1}{k} \equiv \frac{2}{15} \sum_{\frac{p}{10} < k < \frac{3p}{10}} \frac{1}{k} \pmod p$.

(8) (Z.H.Sun[S1],1992) *If* $r \in \{1, 2, 3, 4\}$ *and* $r \equiv 3p \pmod 5$, *then*

$$\frac{F_{p-(\frac{5}{p})}}{p} \equiv \frac{2}{5} q_p(2) + 2 \sum_{k=0}^{\frac{p-5-2r}{10}} \frac{(-1)^{5k+r}}{5k+r} \pmod p.$$

(9) (Z.H.Sun[S2],1995) $\frac{F_{p-(\frac{5}{p})}}{p} \equiv \frac{4}{5}\big((-1)^{[p/5]}\binom{p-1}{[p/5]} - 1\big)/p - q_p(5) \pmod p$.

(10) (Z.H.Sun[S4],2001) $\frac{F_{p-(\frac{5}{p})}}{p} \equiv q_p(5) - 2q_p(2) - \sum_{k=1}^{(p-1)/2} \frac{1}{k \cdot 5^k} \pmod p$.

(11) (Z.H.Sun[S4],2001) $\frac{F_{p-(\frac{5}{p})}}{p} \equiv -\frac{1}{5}(2q_p(2) + \sum_{k=1}^{(p-1)/2} \frac{5^k}{k}) \pmod p$.

We remark that Theorem 4.1(11) can also be deduced from P.Bruckman's result ([B]).

Theorem 4.2 (A.Granville,Z.W.Sun[GS],1996). *Let* $\{B_n(x)\}$ *be the Bernoulli polynomials. If* p *is a prime greater than* 5, *then*

$$B_{p-1}(\frac{1}{5}) - B_{p-1} \equiv \frac{5}{4} q_p(5) + \frac{5}{4}(\frac{p}{5}) \frac{F_{p-(\frac{p}{5})}}{p} \pmod p,$$
$$B_{p-1}(\frac{2}{5}) - B_{p-1} \equiv \frac{5}{4} q_p(5) - \frac{5}{4}(\frac{p}{5}) \frac{F_{p-(\frac{p}{5})}}{p} \pmod p,$$
$$B_{p-1}(\frac{1}{10}) - B_{p-1} \equiv \frac{5}{4} q_p(5) + 2q_p(2) + \frac{15}{4}(\frac{p}{5}) \frac{F_{p-(\frac{p}{5})}}{p} \pmod p,$$
$$B_{p-1}(\frac{3}{10}) - B_{p-1} \equiv \frac{5}{4} q_p(5) + 2q_p(2) - \frac{15}{4}(\frac{p}{5}) \frac{F_{p-(\frac{p}{5})}}{p} \pmod p.$$

5. Wall-Sun-Sun prime.

Using Theorem 4.1(1) and H.S.Vandiver's result in 1914, Z.H.Sun and Z.W.Sun[SS] revealed the connection between Fibonacci numbers and Fermat's last theorem.

Theorem 5.1(Z.H.Sun, Z.W.Sun[SS],1992). *Let* $p > 5$ *be a prime. If there are integers* x, y, z *such that* $x^p + y^p = z^p$ *and* $p \nmid xyz$, *then* $p^2 \mid F_{p-(\frac{p}{5})}$.

On the basis of this result, mathematicians introduced the so-called Wall-Sun-Sun primes ([CDP]).

Definition 5.1. *If p is a prime such that $p^2 \mid F_{p-(\frac{p}{5})}$, then p is called a Wall-Sun-Sun prime.*

Up to now, no Wall-Sun-Sun primes are known. R. McIntosh showed that any Wall-Sun-Sun prime should be greater than 10^{14}. See the web pages:
$http://primes.utm.edu/glossary/page.php?sort=WallSunSunPrime$,
$http://en2.wikipedia.org/wiki/Wall-Sun-Sun\_prime$.

Theorem 5.2. *Let $p>5$ be a prime. Then p is a Wall-Sun-Sun prime if and only if $L_{p-(\frac{p}{5})} \equiv 2(\frac{p}{5}) \pmod{p^4}$.*

Proof. From (1.2), Theorems 2.1 and 2.2 we see that

$$L_{p-(\frac{p}{5})} = 2F_p - \left(\frac{p}{5}\right) F_{p-(\frac{p}{5})} \equiv 2\left(\frac{p}{5}\right) \pmod{p} \tag{5.1}$$

and so that $L_{p-(\frac{p}{5})} \not\equiv -2\left(\frac{p}{5}\right) \pmod{p}$. Since $L_n^2 - 5F_n^2 = 4(-1)^n$ by (3.1), we have

$$\begin{aligned} p^2 \mid F_{p-(\frac{p}{5})} &\iff p^4 \mid F^2_{p-(\frac{p}{5})} \iff L^2_{p-(\frac{p}{5})} \equiv 4 \pmod{p^4} \\ &\iff p^4 \mid \left(L_{p-(\frac{p}{5})} - 2\left(\frac{p}{5}\right)\right)\left(L_{p-(\frac{p}{5})} + 2\left(\frac{p}{5}\right)\right) \\ &\iff p^4 \mid L_{p-(\frac{p}{5})} - 2\left(\frac{p}{5}\right). \end{aligned}$$

This is the result.

From Theorem 3.3 we have

Theorem 5.3. *Let m be a positive integer. If $p \neq 2,5$ is a prime such that $p \mid F_m$, then p is a Wall-Sun-Sun prime if and only if $\mathrm{ord}_p F_m \geq \mathrm{ord}_p m + 2$.*

From Theorem 3.4 we have

Theorem 5.4. *Let $\{S_n\}$ be given by $S_1 = 3$ and $S_{n+1} = S_n^2 - 2 (n \geq 1)$. If p is a prime divisor of S_n, then $p^2 \mid S_n$ if and only if p is a Wall-Sun-Sun prime.*

According to Theorem 5.4 and R. McIntosh's search result we see that any square prime factor of S_n should be greater than 10^{14}.

6. Congruences for $F_{\frac{p-1}{2}}$ and $F_{\frac{p+1}{2}}$ modulo p.

For prime $p>5$, it looks very difficult to determine $F_{\frac{p-1}{2}}$ and $F_{\frac{p+1}{2}} \pmod{p}$. Anyway, the congruences were established by Z.H.Sun and Z.W.Sun[SS] in 1992. They deduced the desired congruences from the following interesting formulas.

Lemma 6.1 (Z.H.Sun and Z.W.Sun[SS],1992). *Let $p>0$ be odd, and $r \in \mathbb{Z}$.*

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

$$\sum_{\substack{k=0 \\ k\equiv r \pmod{10}}}^{p} \binom{p}{k} = \begin{cases} \frac{1}{10}(2^p + L_{p+1} + 5^{\frac{p+3}{4}} F_{\frac{p+1}{2}}) & \text{if } r \equiv \frac{p-1}{2} \pmod{10}, \\ \frac{1}{10}(2^p - L_{p-1} + 5^{\frac{p+3}{4}} F_{\frac{p-1}{2}}) & \text{if } r \equiv \frac{p-1}{2}+2 \pmod{10}, \\ \frac{1}{10}(2^p - L_{p-1} - 5^{\frac{p+3}{4}} F_{\frac{p-1}{2}}) & \text{if } r \equiv \frac{p-1}{2}+4 \pmod{10}, \\ \frac{1}{10}(2^p + L_{p+1} - 5^{\frac{p+3}{4}} F_{\frac{p+1}{2}}) & \text{if } r \equiv \frac{p-1}{2}+6 \pmod{10}. \end{cases}$$

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

$$\sum_{\substack{k=0\\ k\equiv r \pmod{10}}}^{p}\binom{p}{k}=\begin{cases}\frac{1}{10}(2^p+L_{p+1}+5^{\frac{p+1}{4}}L_{\frac{p+1}{2}}) & \text{if } r\equiv \frac{p-1}{2} \pmod{10},\\ \frac{1}{10}(2^p-L_{p-1}+5^{\frac{p+1}{4}}L_{\frac{p-1}{2}}) & r\equiv \frac{p-1}{2}+2 \pmod{10},\\ \frac{1}{10}(2^p-L_{p-1}-5^{\frac{p+1}{4}}L_{\frac{p-1}{2}}) & \text{if } r\equiv \frac{p-1}{2}+4 \pmod{10},\\ \frac{1}{10}(2^p+L_{p+1}-5^{\frac{p+1}{4}}L_{\frac{p+1}{2}}) & \text{if } r\equiv \frac{p-1}{2}+6 \pmod{10}.\end{cases}$$

(3) *If* $r\equiv \frac{p-1}{2}+8 \pmod{10}$, *then*

$$\sum_{\substack{k=0\\ k\equiv r \pmod{10}}}^{p}\binom{p}{k}=\frac{1}{10}(2^p-2L_p).$$

Lemma 6.1 was rediscovered by F.T.Howard and R.Witt[HW] in 1998.

If p is an odd prime, then $p\mid\binom{p}{k}$ for $k=1,2,\dots,p-1$. So, using Lemma 6.1 we can determine $F_{\frac{p-1}{2}}$ and $F_{\frac{p+1}{2}} \pmod p$.

Theorem 6.1(Z.H.Sun,Z.W.Sun[SS],1992). *Let* $p\neq 2,5$ *be a prime. Then*

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

and

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

In 2003, Z.H.Sun ([S6]) gave another proof of Theorem 6.1. Since $L_n=2F_{n+1}-F_n=2F_{n-1}+F_n$, by Theorem 6.1 one may deduce the congruences for $L_{\frac{p\pm1}{2}} \pmod p$.

Theorem 6.2(Z.H.Sun, 6 Jan. 1989). *Let* $p\equiv 3,7 \pmod{20}$ *be a prime and hence* $2p=x^2+5y^2$ *for some positive integers* x,y. *Then*

$$L_{\frac{p-1}{2}}\equiv(-1)^{\frac{x-y}{2}}\frac{x}{y} \pmod p.$$

7. Congruences for $F_{(p-(\frac{p}{3}))/3} \pmod p$.

Let $p>5$ be a prime. It is clear that

$$(\frac{-15}{p})=(\frac{-3}{p})(\frac{5}{p})=(\frac{p}{3})(\frac{p}{5})=\begin{cases}1 & \text{if } p\equiv 1,2,4,8 \pmod{15},\\ -1 & \text{if } p\equiv 7,11,13,14 \pmod{15}.\end{cases}$$

Using the theory of cubic residues, Z.H.Sun[S3] proved the following result.

Theorem 7.1 (Z.H.Sun[S3],1998). *Let p be an odd prime.*

(1) *If $p \equiv 1,4 \pmod{15}$ and so $p = x^2 + 15y^2$ for some integers x, y. Then*

$$F_{\frac{p-1}{3}} \equiv \begin{cases} 0 \pmod{p} & \text{if } y \equiv 0 \pmod{3}, \\ \mp \frac{x}{5y} \pmod{p} & \text{if } y \equiv \pm x \pmod{3} \end{cases}$$

and

$$L_{\frac{p-1}{3}} \equiv \begin{cases} 2 \pmod{p} & \text{if } y \equiv 0 \pmod{3}, \\ -1 \pmod{p} & \text{if } y \not\equiv 0 \pmod{3}. \end{cases}$$

(2) *If $p \equiv 2,8 \pmod{15}$ and so $p = 5x^2 + 3y^2$ for some integers x, y. Then*

$$F_{\frac{p+1}{3}} \equiv \begin{cases} 0 \pmod{p} & \text{if } y \equiv 0 \pmod{3}, \\ \pm \frac{x}{y} \pmod{p} & \text{if } y \equiv \pm x \pmod{3}. \end{cases}$$

and

$$L_{\frac{p+1}{3}} \equiv \begin{cases} -2 \pmod{p} & \text{if } y \equiv 0 \pmod{3}, \\ 1 \pmod{p} & \text{if } y \not\equiv 0 \pmod{3}. \end{cases}$$

Theorem 7.2. *Let p be an odd prime such that $p \equiv 7, 11, 13, 14 \pmod{15}$. Then $x \equiv F_{(p-(\frac{p}{3}))/3} \pmod{p}$ is the unique solution of the cubic congruence $5x^3 + 3x - 1 \equiv 0 \pmod{p}$, and $x \equiv L_{(p-(\frac{p}{3}))/3} \pmod{p}$ is the unique solution of the cubic congruence $x^3 - 3x + 3(\frac{p}{3}) \equiv 0 \pmod{p}$.*

Proof. Since $(\frac{-15}{p}) = 1$ and $(-1)^{(p-(\frac{p}{3}))/6} = (\frac{3}{p})$, by taking $a = -1$ and $b = 1$ in [S7, Corollary 2.1] we find

$$F_{(p-(\frac{p}{3}))/3} \equiv -\frac{t}{5} \pmod{p} \quad \text{and} \quad L_{(p-(\frac{p}{3}))/3} \equiv -(\frac{p}{3})y \pmod{p},$$

where t is the unique solution of the congruence $t^3 + 15t + 25 \equiv 0 \pmod{p}$, and y is the unique solution of the congruence $y^3 - 3y - 3 \equiv 0 \pmod{p}$. Now setting $t = -5x$ and $y = -(\frac{p}{3})x$ yields the result.

Using Theorem 7.1 Z.H.Sun proved

Theorem 7.3 (Z.H.Sun[S3],1998). *Let $p > 5$ be a prime.*

(1) *If $p \equiv 1 \pmod{3}$, then*

$$p \mid F_{\frac{p-1}{3}} \iff p = x^2 + 135y^2 (x, y \in \mathbb{Z}),$$
$$p \mid F_{\frac{p-1}{6}} \iff p = x^2 + 540y^2 (x, y \in \mathbb{Z}).$$

(2) *If $p \equiv 2 \pmod{3}$,*

$$p \mid F_{\frac{p+1}{3}} \iff p = 5x^2 + 27y^2 (x, y \in \mathbb{Z}),$$
$$p \mid F_{\frac{p+1}{6}} \iff p = 5x^2 + 108y^2 (x, y \in \mathbb{Z}).$$

In 1974, using cyclotomic numbers E.Lehmer[L2] proved that if $p \equiv 1 \pmod{12}$ is a prime, then $p \mid F_{\frac{p-1}{3}}$ if and only if p is represented by $x^2 + 135y^2$.

8. Congruences for $F_{(p-(\frac{-1}{p}))/4}$ modulo p.

Theorem 8.1 (E.Lehmer[L1],1966). *Let $p\equiv 1,9 \pmod{20}$ be a prime, and $p=a^2+b^2$ with $a,b\in\mathbb{Z}$ and $2\mid b$.*

(i) *If $p\equiv 1,29 \pmod{40}$, then $p\mid F_{\frac{p-1}{4}} \iff 5\mid b$;*

(ii) *If $p\equiv 9,21 \pmod{40}$, then $p\mid F_{\frac{p-1}{4}} \iff 5\mid a$.*

Theorem 8.2. *Let p be a prime greater than 5.*

(i) (E.Lehmer[L2], 1974) *If $p\equiv 1 \pmod 8$, then*

$$p\mid F_{\frac{p-1}{4}} \iff p=x^2+80y^2 \quad (x,y\in\mathbb{Z}).$$

(ii) (Z.H.Sun,Z.W.Sun[SS], 1992) *If $p\equiv 5 \pmod 8$, then*

$$p\mid F_{\frac{p-1}{4}} \iff p=16x^2+5y^2 \quad (x,y\in\mathbb{Z}).$$

In 1994, by computing some quartic Jacobi symbols Z.H.Sun established the following unpublished result.

Theorem 8.3 (Z.H.Sun, 1994). *Let $p\equiv 1,9 \pmod{20}$ be a prime with $p=a^2+b^2=x^2+5y^2 (a,b,x,y\in\mathbb{Z})$ and $a\equiv(-1)^{\frac{p-1}{4}} \pmod 4$. If $4\mid xy$, then*

$$L_{\frac{p-1}{4}}\equiv\begin{cases} 2\left(\frac{a-2b}{5}\right)_4\left(\frac{2ay+by+ax}{p}\right) \pmod p & \text{if } p\equiv 1 \pmod 8,\\ -\frac{2b}{a}\left(\frac{2a+b}{5}\right)_4\left(\frac{2ay+by+ax}{p}\right) \pmod p & \text{if } p\equiv 5 \pmod 8.\end{cases}$$

If $4\nmid xy$, then

$$F_{\frac{p-1}{4}}\equiv\begin{cases} \left(\frac{2a+b}{5}\right)_4\left(\frac{2ay+by+ax}{p}\right)\frac{2y}{x} \pmod p & \text{if } p\equiv 1 \pmod 8,\\ \left(\frac{2b-a}{5}\right)_4\left(\frac{2ay+by+ax}{p}\right)\frac{2by}{ax} \pmod p & \text{if } p\equiv 5 \pmod 8,\end{cases}$$

where $\left(\frac{m}{5}\right)_4=1$ or -1 according as $m\equiv 1 \pmod 5$ or not.

In the end we point out two interesting conjectures.

Conjecture 8.1 (Z.H.Sun[S6], 12 Feb.2003). *Let $p\equiv 3,7 \pmod{20}$ be a prime, and hence $2p=x^2+5y^2$ for some integers x and y. Then*

$$F_{\frac{p+1}{4}}\equiv\begin{cases} 2(-1)^{[\frac{p-5}{10}]}\cdot 10^{\frac{p-3}{4}} \pmod p & \text{if } y\equiv\pm\frac{p-1}{2} \pmod 8,\\ -2(-1)^{[\frac{p-5}{10}]}\cdot 10^{\frac{p-3}{4}} \pmod p & \text{if } y\not\equiv\pm\frac{p-1}{2} \pmod 8.\end{cases}$$

Since $F_{\frac{p+1}{4}}L_{\frac{p+1}{4}}=F_{\frac{p+1}{2}}$, from Theorem 6.1 we see that Conjecture 7.1 is equivalent to

$$(8.1)\qquad L_{\frac{p+1}{4}}\equiv\begin{cases} (-2)^{\frac{p+1}{4}} \pmod p & \text{if } y\equiv\pm\frac{p-1}{2} \pmod 8,\\ -(-2)^{\frac{p+1}{4}} \pmod p & \text{if } y\not\equiv\pm\frac{p-1}{2} \pmod 8.\end{cases}$$

Z.H.Sun has checked (8.1) for all primes $p<3000$.

Conjecture 8.2 (E.Lehmer[L2],1974). *Let $p\equiv 1 \pmod{16}$ be a prime, and $p=x^2+80y^2=a^2+16b^2$ for some integers x,y,a,b. Then*

$$p\mid F_{\frac{p-1}{8}} \iff y\equiv b \pmod 2.$$

References

[B] P. Bruckman, *Equivalent conditions for Fibonacci and Lucas pseudoprimes to contain a square factor*, Pi Mu Epsilon Journal **10** (1998), 634-642.

[CDP] R. Crandall, K. Dilcher and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. **66** (1997), 433-449, MR 97c:11004.

[D] L.E. Dickson, *History of the Theory of Numbers*, Vol.I, Chelsea, New York, 1952, pp. 393-407.

[GS] A.Granville and Z.W.Sun, *Values of Bernoulli polynomials*, Pacific J. Math. **172** (1996), 117-137.

[HW] F.T.Howard and R.Witt, *Lacunary sums of binomial coefficients*, Applications of Fibonacci Numbers (Vol 7) (1998), Kluwer Academic Publishers, 185-195.

[L1] E.Lehmer, *On the quadratic character of the Fibonacci root*, Fibonacci Quart. **4** (1966), 135-138, MR39#160.

[L2] E.Lehmer, *On the quartic character of quadratic units*, J. Reine Angew. Math. **268/269** (1974), 294-301.

[Le] D.H. Lehmer, *An extended theory of Lucas' functions*, Ann. Math. **31** (1930), 419-448.

[R1] P. Ribenboim, *The Book of Prime Number Records*, 2nd ed., Springer, Berlin, 1989, pp. 44-50.

[R2] P. Ribenboim, *My numbers, my friends*, Springer-Verlag New York, Inc., New York, Berlin, London, 2000, pp. 1-41.

[S1] Z.H. Sun, *Combinatorial sum* $\sum_{\substack{k=0\\ k\equiv r(\mathrm{mod}\ m)}}^{n}\binom{n}{k}$ *and its applications in number theory I*, J. Nanjing Univ. Math. Biquarterly **9** (1992), 227-240, MR94a:11026.

[S2] ____, *Combinatorial sum* $\sum_{k\equiv r(\mathrm{mod}\ m)}\binom{n}{k}$ *and its applications in number theory III*, J. Nanjing Univ. Math. Biquarterly **12** (1995), 90-102, MR96g:11017.

[S3] ____, *On the theory of cubic residues and nonresidues*, Acta Arith. **84** (1998), 291-335, MR99c:11005.

[S4] ____, *Five congruences for primes*, Fibonacci Quart. **40** (2001), 345-351.

[S5] ____, *Linear recursive sequences and powers of matrices*, Fibonacci Quart. **39** (2001), 339-351.

[S6] ____, *Values of Lucas sequences modulo primes*, Rocky Mountain J. Math. **33** (2003), 1123-1145.

[S7] ____, *Cubic and quartic congruences modulo a prime*, J. Number Theory **102** (2003), 41-89.

[SS] Z.H. Sun and Z.W. Sun, *Fibonacci numbers and Fermat's last theorem*, Acta Arith. **60** (1992), 371-388, MR93e:11025.

[W1] H.C.Williams, *A note on the Fibonacci quotient* $F_{p-\varepsilon}/p$, Canad. Math. Bull. **25** (1982), 366-370.

[W2] ____, *Some formulas concerning the fundamental unit of a real quadratic field*, Discrete Math. **92** (1991), 431-440.