A talk given at the National Center for Theoretical Sciences (Hsinchu, Taiwan; July 20, 2011) and Shanghai Jiaotong University (Nov. 4, 2011)

Some sophisticated congruences involving Fibonacci numbers

Zhi-Wei Sun

Nanjing University
Nanjing 210093, P. R. China
zwsun@nju.edu.cn
http://math.nju.edu.cn/∼zwsun

Nov. 4, 2011

Abstract

The well-known Fibonacci numbers play important roles in many areas of mathematics and they have very nice number-theoretic properties. We will focus on some sophisticated congruences on Fibonacci numbers including the recent determination of $F_{p-(\frac{p}{5})}$ modulo p^3, where p is an odd prime. We will also mention some conjectures related to 5-adic valuations for further research.

Part A. On Fibonacci quotients and Wall-Sun-Sun primes

Fibonacci numbers and Lucas numbers

The Fibonacci sequence $\{F_n\}_{n\geqslant 0}$ is defined by

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

Thus

$$F_0 = 0,\ F_1 = F_2 = 1,\ F_3 = 2,\ F_4 = 3,\ F_5 = 5,\ F_6 = 8,$$
$$F_7 = 13,\ F_8 = 21,\ F_9 = 34,\ F_{10} = 55,\ F_{11} = 89,\ F_{12} = 144.$$

The Lucas numbers $L_0, L_1, L_2, \ldots$ are given by

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

Relations between Fibonacci numbers and Lucas numbers:

$$L_n = F_{n-1} + F_{n+1} \quad \text{and} \quad 5F_n = L_{n-1} + L_{n+1}.$$

More known results on Fibonacci numbers

An explicit expression.

$$F_n = \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} \binom{n-1-k}{k}.$$

Y. Bugeaud, M. Mignotte and S. Siksek [Ann. of Math. 163(2006)]: The only powers in the Fibonacci sequence are

$$F_0 = 0,\ F_1 = F_2 = 1,\ F_6 = 2^3,\ \text{and } F_{12} = 12^2.$$

Ke-Jian Wu and Z. W. Sun [Math. Comp. 78(2009)]: Let

$$a = 3120738688527450218817352213202366516736519\text{-}$$
$$36708237682341853548563549188738642 75$$

and

$$M = 3681285244392207118440249891307607050314622\text{-}$$
$$98208612115583470788713547837448507 78.$$

Then, for any $x \equiv a \pmod{M}$, the number x^2 cannot be written in the form $F_n/2 \pm p^m$ with p a prime and $m, n \in \mathbb{N} = \{0, 1, \ldots\}$.

Lucas sequences

Let $\mathbb{N} = \{0, 1, 2, \ldots\}$ and $\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$.

Fix $A, B \in \mathbb{Z}$. The Lucas sequence $u_n = u_n(A, B)$ ($n \in \mathbb{N}$) and its companion $v_n = v_n(A, B)$ ($n \in \mathbb{N}$) are defined as follows:

$$u_0 = 0,\ u_1 = 1,\ \text{and } u_{n+1} = Au_n - Bu_{n-1}\ (n = 1, 2, 3, \ldots);$$
$$v_0 = 2,\ v_1 = A,\ \text{and } v_{n+1} = Av_n - Bv_{n-1}\ (n = 1, 2, 3, \ldots).$$

Example : $F_n = u_n(1, -1),\ L_n = v_n(1, -1);\ u_n(2, 1) = n,\ v_n(2, 1) = 2.$

Universal Formulae: Let $\Delta = A^2 - 4B$, and let

$$\alpha = \frac{A + \sqrt{\Delta}}{2} \text{ and } \beta = \frac{A - \sqrt{\Delta}}{2}$$

be the two roots of the equation $x^2 - Ax + B = 0$. Then

$$u_n = \sum_{0 \leqslant k < n} \alpha^k \beta^{n-1-k} = \begin{cases} \frac{\alpha^n - \beta^n}{\alpha - \beta} & \text{if } \Delta \neq 0, \\ n(A/2)^{n-1} & \text{if } \Delta = 0. \end{cases}$$

And $$v_n = \alpha^n + \beta^n.$$

Basic properties of Lucas sequences

As $(\alpha^n - \beta^n)(\beta^n + \beta^n) = \alpha^{2n} - \beta^{2n}$, we have

$$u_{2n} = u_n v_n.$$

Note also that

$$\begin{aligned} v_n^2 - \Delta u_n^2 =& (\alpha^n + \beta^n)^2 - ((\alpha - \beta)u_n)^2 \\ =& (\alpha^n + \beta^n)^2 - (\alpha^n - \beta^n)^2 = 4(\alpha\beta)^n = 4B^n. \end{aligned}$$

Lucas' Theorem. Let $A, B \in \mathbb{Z}$ with $(A, B) = 1$. Then

$$(u_m, u_n) = |u_{(m,n)}|.$$

In particular,

$$m \mid n \Rightarrow u_m \mid u_n.$$

Example. $F_{2n} = F_n L_n,\ L_n^2 - 5F_n^2 = 4(-1)^n,\ (F_m, F_n) = F_{(m,n)}$.

Legendre symbols

Let p be an odd prime and $a \in \mathbb{Z}$. The Legendre symbol $(\frac{a}{p})$ is given by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } p \nmid a \text{ and } x^2 \equiv a \pmod{p} \text{ for some } x \in \mathbb{Z}, \\ -1 & \text{if } p \nmid a \text{ and } x^2 \equiv a \pmod{p} \text{ for no } x \in \mathbb{Z}. \end{cases}$$

It is well known that $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ for any $a, b \in \mathbb{Z}$. Also,

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv -1 \pmod{4}; \end{cases}$$

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}; \end{cases}$$

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

Congruence properties of Lucas sequences

Let p be an odd prime. Then

$$u_p \equiv \left(\frac{\Delta}{p}\right) \pmod{p} \text{ and } v_p \equiv A \pmod{p}.$$

In fact,

$$v_p = \alpha^p + \beta^p \equiv (\alpha + \beta)^p = A^p \equiv A \pmod{p};$$

also

$$\Delta u_p = (\alpha - \beta)(\alpha^p - \beta^p) \equiv (\alpha - \beta)^{p+1} = \Delta^{(p+1)/2} \pmod{p}$$

and hence $u_p \equiv (\frac{\Delta}{p}) \pmod{p}$ if $p \nmid \Delta$. When $\Delta = A^2 - 4B \equiv 0 \pmod{p}$, we have

$$u_p \equiv u_p\left(A, \frac{A^2}{4}\right) = p\left(\frac{A}{2}\right)^{p-1} \equiv \left(\frac{\Delta}{p}\right) \pmod{p}.$$

Congruence properties of Lucas sequences

Theorem. If p is an odd prime not dividing B, then

$$u_{p-(\frac{\Delta}{p})} \equiv 0 \pmod{p}. \qquad (*)$$

Proof. If $p \mid \Delta$, then $u_{p-(\frac{\Delta}{p})} = u_p \equiv (\frac{\Delta}{p}) = 0 \pmod{p}$.
If $(\frac{\Delta}{p}) = -1$, then

$$u_{p-(\frac{\Delta}{p})} = u_{p+1} = Au_p + v_p \equiv A\left(\frac{\Delta}{p}\right) + A = 0 \pmod{p}.$$

If $(\frac{\Delta}{p}) = 1$, then

$$u_{p-(\frac{\Delta}{p})} = u_{p-1}$$

and

$$2Bu_{p-1} = Au_p - v_p \equiv A\left(\frac{\Delta}{p}\right) - A = 0 \pmod{p}.$$

Congruence properties of Lucas sequences

The congruence $p \mid u_{p-(\frac{\Delta}{p})}$ is actually an extension of Fermat's little theorem. If $a \not\equiv 0, 1 \pmod{p}$, then

$$\frac{a^{p-1}-1}{a-1} = u_{p-1}(a+1, a) = u_{p-\left(\frac{(a+1)^2-4a}{p}\right)}(a+1, a) \equiv 0 \pmod{p}.$$

Example. If p is an odd prime, then

$$F_p \equiv \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) \pmod{p},\ L_p \equiv 1 \pmod{p},$$

and

$$F_{p-(\frac{p}{5})} \equiv 0 \pmod{p}.$$

For an odd prime p, we call the integer $F_{p-(\frac{p}{5})}/p$ a *Fibonacci quotient*.

D. D. Wall's question

In 1960 D. D. Wall [Amer. Math. Monthly] studied Fibonacci numbers modulo a positive integer systematically.

Let p be an odd prime and let $n(p)$ be the smallest positive integer n with $p \mid F_n$. Can $F_{n(p)}$ be a multiple of p^2? Wall found no such primes.

One can show that any positive integer d divides some positive Fibonacci numbers. Let $n(d)$ be the smallest positive integer such that $d \mid F_{n(d)}$. Then Wall's question is whether $n(p) \neq n(p^2)$ for any odd prime p.

Zhi-Hong Sun and Zhi-Wei Sun's contribution

Theorem (Zhi-Hong Sun and Zhi-Wei Sun [Acta Arith. 60(1992)]). Let $p \neq 2,5$ be a prime.

(i) We have $n(p) = n(p^2) \iff p^2 \mid F_{p-(\frac{p}{5})}$.

(ii) We have

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

(iii) If $p^2 \nmid F_{p-(\frac{p}{5})}$, then the first case of Fermat's last theorem holds for the exponent p, i.e., there are no positive integers x, y, z with $p \nmid xyz$ such that $x^p + y^p = z^p$.

(iv) If $p \equiv 1, 9 \pmod{20}$ and $p = x^2 + 5y^2$ with $x, y \in \mathbb{Z}$, then

$$p \mid F_{(p-1)/4} \iff 4 \mid xy.$$

Zhi-Hong Sun and Zhi-Wei Sun's contribution

(v) We can determine $F_{(p\pm1)/2}$ and $L_{(p\pm1)/2}$ mod p in the following way:

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

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

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

$$L_{(p+(\frac{p}{5}))/2} \equiv \begin{cases} (-1)^{\lfloor (p+5)/10 \rfloor}5^{(p-1)/4} \pmod p & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{\lfloor (p+5)/10 \rfloor}(\frac{5}{p})5^{(p+1)/4} \pmod p & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

The theorem was obtained via expressing the sum $\sum_{k\equiv r \pmod{10}} \binom{n}{k}$ in terms of Fibonacci and Lucas numbers.

Wall-Sun-Sun primes

R. Crandall, K. Dilcher and C. Pomerance [Math. Comp. 66(1997)] called those primes p satisfying $F_{p-(p/5)} \equiv 0 \pmod{p^2}$ *Wall-Sun-Sun primes*. Heuristically there should be infinitely many Wall-Sun-Sun primes though they are very rare.

Wall-Sun-Sun primes were also introduced in many papers and books including the famous book R. E. Cradall and C. Pomerance, *Prime Numbers: A Computational Perspective*, Springer, 2001.

Up to now no Wall-Sun-Sun primes have been found.

The current search record is due to F. G. Dorais and D. W. Klyve (2010): There are no Wall-Sun-Sun primes below 9.7×10^{14}.

Connection to cyclotomic fields

S. Jakubec [Math. Comp. 67(1998)]: Let $p = 2l + 1 \equiv 7 \pmod 8$ and q be odd primes with l a prime and $p \equiv -5 \pmod q$. Suppose that the order of q modulo l is $(l-1)/2$. If q divides the class number of the real cyclotomic field $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, then q must be a Wall-Sun-Sun prime.

Bernoulli polynomials and Fibonacci quotients

Bernoulli numbers $B_0, B_1, B_2, \ldots$ are given by

$$B_0 = 1, \quad \sum_{k=0}^{n} \binom{n+1}{k} B_k = 0 \quad (n = 1, 2, 3, \ldots).$$

Bernoulli polynomials are those

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k} \ (n = 0, 1, 2, \ldots).$$

Theorem (A. Granville and Z. W. Sun [Pacific J. Math. 1996]).
Let $p \neq 2, 5$ be a prime. Then

$$B_{p-1}\left(\frac{a}{5}\right) - B_{p-1} \equiv \left(\frac{ap}{5}\right) \frac{5}{4} \cdot \frac{F_{p-(\frac{p}{5})}}{p} + \frac{5}{4} q_p(5) \pmod{p}$$

for $a = 1, 2, 3, 4$, and for $a = 1, 3, 7, 9$ we have

$$B_{p-1}\left(\frac{a}{10}\right) - B_{p-1} \equiv \left(\frac{ap}{5}\right) \frac{15}{4} \cdot \frac{F_{p-(\frac{p}{5})}}{p} + \frac{5}{4} q_p(5) + 2q_p(2) \pmod{p},$$

where $q_p(m)$ denotes the Fermat quotient $(m^{p-1} - 1)/p$.

Part B. On $F_{p-(\frac{p}{5})}$ mod p^3 and some super congruences involving Fibonacci numbers

A curious identity and its consequence

H. Pan and Z. W. Sun [Discrete Math. 2006]. If $l, m, n \in \{0, 1, 2, \ldots\}$ then

$$\sum_{k=0}^{l}(-1)^{m-k}\binom{l}{k}\binom{m-k}{n}\binom{2k}{k-2l+m}$$
$$=\sum_{k=0}^{l}\binom{l}{k}\binom{2k}{n}\binom{n-l}{m+n-3k-l}.$$

On the basis of this identity, for $d, r \in \{0, 1, 2, \ldots\}$ the authors constructed explicit $F(d, r)$ and $G(d, r)$ such that for any prime $p > \max\{d, r\}$ we have

$$\sum_{k=1}^{p-1} k^r C_{k+d} \equiv \begin{cases} F(d, r) \pmod{p} & \text{if } p \equiv 1 \pmod{3}, \\ G(d, r) \pmod{p} & \text{if } p \equiv 2 \pmod{3}, \end{cases}$$

where C_n denotes the Catalan number $\frac{1}{n+1}\binom{2n}{n}$.

Some congruences involving central binomial coefficients

Let p be an odd prime.

H. Pan and Z. W. Sun [Discrete Math. 2006].

$$\sum_{k=0}^{p-1}\binom{2k}{k+d}\equiv\left(\frac{p-d}{3}\right)\pmod p\ \ (d=0,\ldots,p),$$

$$\sum_{k=1}^{p-1}\frac{\binom{2k}{k}}{k}\equiv 0 \pmod p\ \ \text{for } p>3.$$

Sun & R. Tauraso [AAM 45(2010); IJNT 7(2011)].

$$\sum_{k=0}^{p^a-1}\binom{2k}{k}\equiv\left(\frac{p^a}{3}\right)\pmod{p^2},$$

$$\sum_{k=1}^{p-1}\frac{\binom{2k}{k}}{k}\equiv\frac{8}{9}p^2B_{p-3}\pmod{p^3}\ \ \text{for } p>3,$$

$$\sum_{k=1}^{p-1}\frac{(-1)^k}{k}\binom{2k}{k}\equiv-5\frac{F_{p-(\frac{p}{5})}}{p}\ \ (\text{mod } p)\ \ (p\neq 5).$$

Some auxiliary identities

Sun and Tauraso [Adv. in Appl. Math. 2010]: Let $n \in \mathbb{Z}^+$ and $d \in \mathbb{N}$. Then

$$\sum_{0 \leqslant k < n} \binom{2k}{k+d} + \left(\frac{d}{3}\right) = \sum_{0 \leqslant k < n+d} \binom{2n}{k} \left(\frac{n+d-k}{3}\right),$$

$$\sum_{0 \leqslant k < n} (-1)^{k+d} \binom{2k}{k+d} + F_{2d} = \sum_{0 \leqslant k < n+d} (-1)^k \binom{2n}{k} F_{2(n+d-k)},$$

and

$$d \sum_{0 < k < n} \frac{(-1)^{k+d}}{k} \binom{2k}{k+d} + \sum_{0 \leqslant k < n+d} \binom{2n}{k} (-1)^k L_{2(n+d-k)}$$
$$= L_{2d} - (-1)^{n+d} 2 \binom{2n-1}{n+d-1} - \delta_{d,0}.$$

On $\sum_{k=0}^{p-1}\binom{2k}{k}/m^k \bmod p^2$

Z. W. Sun [Sci. China Math. 53(2010)]: Let p be an odd prime and let $m\in\mathbb{Z}$ with $p\nmid m$. Then

$$\sum_{k=0}^{p-1}\frac{\binom{2k}{k}}{m^k}\equiv\left(\frac{m^2-4m}{p}\right)+u_{p-(\frac{m^2-4m}{p})}(m-2,1)\pmod{p^2}.$$

In particular,

$$\sum_{k=0}^{p-1}\frac{\binom{2k}{k}}{2^k}\equiv(-1)^{(p-1)/2}\pmod{p^2},$$

$$\sum_{k=0}^{p-1}(-1)^k\binom{2k}{k}\equiv\left(\frac{p}{5}\right)\left(1-2F_{p-(\frac{p}{5})}\right)\pmod{p^2}\quad(p\neq 5).$$

(Note that $(-1)^{n-1}u_n(-3,1)=u_n(3,1)=F_{2n}=F_nL_n$.)

Two conjectures on Fibonacci and Lucas numbers

Conjecture (Sun and Tauraso [Adv. in Appl. Math. 2010]) Let $p \neq 2, 5$ be a prime and let $a \in \mathbb{Z}^+$. Then

$$\sum_{k=0}^{p^a-1} (-1)^k \binom{2k}{k} \equiv \left(\frac{p^a}{5}\right) \left(1 - 2F_{p^a - (\frac{p^a}{5})}\right) \pmod{p^3}.$$

Conjecture (Roberto Tauraso, Jan. 2010). For any prime $p > 5$ we have

$$\sum_{k=1}^{p-1} \frac{L_k}{k^2} \equiv 0 \pmod{p}.$$

These two conjectures are very sophisticated and difficult to prove.

Theorem (Hao Pan and Z. W. Sun, arXiv:1010.2489). The two conjectures are true!

Another congruence for $F_{p-(\frac{p}{5})}$ mod p^3

Theorem (Z. W. Sun, arXiv:0911.3060) Let $p \neq 2, 5$ be a prime and let $a \in \mathbb{Z}^+$. Then

$$\sum_{k=0}^{(p^a-1)/2} \frac{\binom{2k}{k}}{(-16)^k} \equiv \left(\frac{p^a}{5}\right)\left(1 + \frac{F_{p^a-(\frac{p^a}{5})}}{2}\right) \pmod{p^3}.$$

The proof is also very sophisticated and quite difficult. Below is a key lemma.

Lemma. Let $p \neq 2, 5$ be an odd prime. For any $a \in \mathbb{Z}^+$ we have

$$\frac{L_{p^a} - 1}{5} - \left(\frac{p^a}{5}\right) F_{p^a} + 1 \equiv -\frac{1}{2} F^2_{p^a-(\frac{p^a}{5})} \pmod{p^4}.$$

If we set $H_k^{(2)} = \sum_{0<j\leqslant k} 1/j^2$ for $k = 0, 1, 2, \ldots$, then

$$\sum_{k=0}^{p-1} (-1)^k \binom{2k}{k} H_k^{(2)} \equiv \left(\frac{p}{5}\right) \frac{5}{2} \left(\frac{F_{p-(\frac{p}{5})}}{p}\right)^2 \pmod{p}.$$

A further conjecture

Conjecture (Sun, 2010). Let p be an odd prime and let $a \in \mathbb{Z}^+$.
(i) If $p^a \equiv 1,2 \pmod 5$, or $a > 1$ and $p \not\equiv 3 \pmod 5$,

$$\sum_{k=0}^{\lfloor 4p^a/5 \rfloor} (-1)^k \binom{2k}{k} \equiv \left(\frac{5}{p^a}\right) \pmod{p^2}.$$

If $p^a \equiv 1,3 \pmod 5$, or $a > 1$ and $p \not\equiv 2 \pmod 5$, then

$$\sum_{k=0}^{\lfloor 3p^a/5 \rfloor} (-1)^k \binom{2k}{k} \equiv \left(\frac{5}{p^a}\right) \pmod{p^2}.$$

(ii) If $p \equiv 1,7 \pmod{10}$ or $a > 2$, then

$$\sum_{k=0}^{\lfloor 7p^a/10 \rfloor} \frac{\binom{2k}{k}}{(-16)^k} \equiv \left(\frac{5}{p^a}\right) \pmod{p^2}.$$

If $p \equiv 1,3 \pmod{10}$ or $a > 2$, then

$$\sum_{k=0}^{\lfloor 9p^a/10 \rfloor} \frac{\binom{2k}{k}}{(-16)^k} \equiv \left(\frac{5}{p^a}\right) \pmod{p^2}.$$

Some other congruences involving Fibonacci numbers

Theorem (Sun). For any prime $p > 5$, we have

$$\sum_{k=0}^{p-1} \frac{F_k}{12^k}\binom{2k}{k} \equiv \begin{cases} 0 \pmod{p} & \text{if } p \equiv \pm 1 \pmod{5}, \\ 1 \pmod{p} & \text{if } p \equiv \pm 13 \pmod{30}, \\ -1 \pmod{p} & \text{if } p \equiv \pm 7 \pmod{30}. \end{cases}$$

Theorem (Sun). Let $p \neq 2, 5$ be a prime. Then

$$\sum_{k=0}^{p-1} F_{2k}\binom{2k}{k} \equiv (-1)^{\lfloor p/5 \rfloor}\left(1 - \left(\frac{p}{5}\right)\right) \pmod{p^2},$$

$$\sum_{k=0}^{p-1} F_{2k+1}\binom{2k}{k} \equiv (-1)^{\lfloor p/5 \rfloor}\left(\frac{p}{5}\right) \pmod{p^2},$$

$$\sum_{k=0}^{(p-1)/2} \frac{F_{2k}}{16^k}\binom{2k}{k} \equiv (-1)^{(p-1)/2+\lfloor p/5 \rfloor} \pmod{p^2},$$

$$\sum_{k=0}^{(p-1)/2} \frac{F_{2k+1}}{16^k}\binom{2k}{k} \equiv (-1)^{(p-1)/2+\lfloor p/5 \rfloor}\frac{5+(\frac{p}{5})}{4} \pmod{p^2}.$$

A conjecture on 5-adic valuations

Conjecture (Sun). For any $n \in \mathbb{Z}^+$ the number

$$s_n := \frac{(-1)^{\lfloor n/5 \rfloor - 1}}{(2n+1)n^2\binom{2n}{n}} \sum_{k=0}^{n-1} F_{2k+1}\binom{2k}{k}$$

is a 5-adic integer and furthermore

$$s_n \equiv \begin{cases} 6 \pmod{25} & \text{if } n \equiv 0 \pmod 5, \\ 4 \pmod{25} & \text{if } n \equiv 1 \pmod 5, \\ 1 \pmod{25} & \text{if } n \equiv 2, 4 \pmod 5, \\ 9 \pmod{25} & \text{if } n \equiv 3 \pmod 5. \end{cases}$$

Also, if $a, b \in \mathbb{Z}^+$ and $a \geqslant b$ then the sum

$$\frac{1}{5^{2a}} \sum_{k=0}^{5^a-1} F_{2k+1}\binom{2k}{k}$$

modulo 5^b only depends on b.

A conjecture on q-Fibonacci numbers

Recall that the usual q-analogue of $n \in \mathbb{N}$ is given by

$$[n]_q = \frac{1-q^n}{1-q} = \sum_{0 \leqslant k < n} q^k$$

which tends to n as $q \to 1$. For any $n, k \in \mathbb{N}$ with $n \geqslant k$,

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{\prod_{0<r\leqslant n}[r]_q}{(\prod_{0<s\leqslant k}[s]_q)(\prod_{0<t\leqslant n-k}[t]_q)}$$

is a natural extension of the usual binomial coefficient $\binom{n}{k}$. A q-analogue of Fibonacci numbers introduced by I. Schur is defined as follows:

$$F_0(q) = 0,\ F_1(q) = 1, \text{and } F_{n+1}(q) = F_n(q) + q^n F_{n-1}(q)\ (n > 0).$$

Conjecture (Sun) Let a and m be positive integers. Then we have the following congruence in the ring $\mathbb{Z}[q]$:

$$\sum_{k=0}^{5^a m-1} q^{-2k(k+1)} \begin{bmatrix} 2k \\ k \end{bmatrix}_q F_{2k+1}(q) \equiv 0 \pmod{[5^a]_q^2}.$$

Four series involving Fibonacci and Lucas numbers

In Oct. 2010 Sun observed the following identities:

$$\sum_{k=1}^{\infty}\frac{F_{2k}}{k^2\binom{2k}{k}}=\frac{4\pi^2}{25\sqrt{5}},\quad \sum_{k=1}^{\infty}\frac{L_{2k}}{k^2\binom{2k}{k}}=\frac{\pi^2}{5},$$

$$\sum_{k=0}^{\infty}\frac{\binom{2k}{k}F_{2k+1}}{(2k+1)16^k}=\frac{2\pi}{5\sqrt{5}},\quad \sum_{k=0}^{\infty}\frac{\binom{2k}{k}L_{2k+1}}{(2k+1)16^k}=\frac{2\pi}{5}.$$

In fact, they can be obtained by putting $x=(\sqrt{5}\pm 1)/2$ in the known identities

$$\arcsin\frac{x}{2}=\sum_{k=0}^{\infty}\frac{\binom{2k}{k}}{(2k+1)4^k}\left(\frac{x}{2}\right)^{2k+1} \text{ and } \sum_{k=1}^{\infty}\frac{x^{2k}}{k^2\binom{2k}{k}}=2\arcsin^2\frac{x}{2}.$$

Note that

$$\sin\frac{\pi}{10}=\frac{\sqrt{5}-1}{4} \text{ and } \sin\frac{3\pi}{10}=\frac{\sqrt{5}+1}{4}.$$

Corresponding conjectural congruences

Conjecture (Sun, 2010). Let $p \neq 2, 5$ be a prime and set $q := F_{p-(\frac{p}{5})}/p$. Then

$$p\sum_{k=1}^{p-1}\frac{F_{2k}}{k^2\binom{2k}{k}} \equiv -\left(\frac{p}{5}\right)\left(\frac{3}{2}q+\frac{5}{4}p\,q^2\right) \pmod{p^2},$$

$$p\sum_{k=1}^{p-1}\frac{L_{2k}}{k^2\binom{2k}{k}} \equiv -\frac{5}{2}q-\frac{15}{4}p\,q^2 \pmod{p^2},$$

$$\sum_{k=0}^{(p-3)/2}\frac{\binom{2k}{k}F_{2k+1}}{(2k+1)16^k} \equiv (-1)^{(p+1)/2}\left(\frac{p}{5}\right)\left(\frac{1}{2}q+\frac{5}{8}p\,q^2\right) \pmod{p^2},$$

$$\sum_{k=0}^{(p-3)/2}\frac{\binom{2k}{k}L_{2k+1}}{(2k+1)16^k} \equiv (-1)^{(p+1)/2}\left(\frac{5}{2}q+\frac{5}{8}p\,q^2\right) \pmod{p^2}.$$

In Oct. 2011 K. Hessami Pilehrood and T. Hessami Pilehrood [arXiv:1110.5308] proved the last two congruences.

A conjecture related to $p = x^2 + 15y^2$ and $p = 3x^2 + 5y^2$

Conjecture (Z. W. Sun, Sept. 18, 2011). Let $p > 5$ be a prime.

(i) If $p \equiv 1, 4 \pmod{15}$ and $p = x^2 + 15y^2$ $(x, y \in \mathbb{Z})$ with $x \equiv 1 \pmod 3$, then

$$\sum_{k=0}^{p-1} \frac{k\binom{2k}{k}\binom{3k}{k}}{27^k} F_k \equiv \frac{2}{15}\left(\frac{p}{x} - 2x\right) \pmod{p^2},$$

$$\sum_{k=0}^{p-1} \frac{\binom{2k}{k}\binom{3k}{k}}{27^k} L_k \equiv 4x - \frac{p}{x} \pmod{p^2}$$

and

$$\sum_{k=0}^{p-1} (3k+2)\frac{\binom{2k}{k}\binom{3k}{k}}{27^k} L_k \equiv 4x \pmod{p^2}.$$

A conjecture related to $p = x^2 + 15y^2$ and $p = 3x^2 + 5y^2$

(ii) If $p \equiv 2, 8 \pmod{15}$ and $p = 3x^2 + 5y^2$ $(x, y \in \mathbb{Z})$ with $y \equiv 1 \pmod 3$, then

$$\sum_{k=0}^{p-1} \frac{\binom{2k}{k}\binom{3k}{k}}{27^k} F_k \equiv \frac{p}{5y} - 4y \pmod{p^2}$$

and

$$\sum_{k=0}^{p-1} \frac{k\binom{2k}{k}\binom{3k}{k}}{27^k} F_k \equiv \sum_{k=0}^{p-1} \frac{k\binom{2k}{k}\binom{3k}{k}}{27^k} L_k \equiv \frac{4}{3} y \pmod{p^2}.$$

Remark. Sun has many other similar conjectures.

Part C. Proof of $\sum_{k=1}^{p-1} \frac{L_k}{k^2} \equiv 0 \pmod{p}$ for any prime $p > 5$

Granville's work

Let p be an odd prime. Glaisher proved that

$$q_p(2) \equiv -\frac{1}{2}\sum_{k=1}^{p-1}\frac{2^k}{k} \pmod p.$$

A. Granville [Integers 4(2004)] confirmed the following conjecture of L. Skula:

$$q_p(2)^2 \equiv -\sum_{k=1}^{p-1}\frac{2^k}{k^2} \pmod p.$$

Define

$$q(x) = \frac{x^p + (1-x)^p - 1}{p} \text{ and } G(x) = \sum_{k=1}^{p-1}\frac{x^k}{k^2}.$$

Granville showed that if $p > 3$ then

$$\begin{aligned} G(x) \equiv& G(1-x) + x^p G(1-x^{-1}) \pmod p, \\ q(x)^2 \equiv& -2x^p G(x) - 2(1-x^p)G(1-x) \pmod p. \end{aligned}$$

A lemma and a proposition

Combining the last two congruences we obtain

Lemma. Let $p > 3$ be a prime. Then

$$\left(\frac{x^p + (1-x)^p - 1}{p}\right)^2 \equiv -2\sum_{k=1}^{p-1}\frac{(1-x)^k}{k^2} - 2x^{2p}\sum_{k=1}^{p-1}\frac{(1-x^{-1})^k}{k^2} \pmod p$$

Proposition. Let A and B be nonzero integers, and let α and β be the two roots of the equation $x^2 - Ax + B = 0$. Let p be an odd prime not dividing AB. Then

$$\left(\frac{v_p(A,B) - A^p}{p}\right)^2 \equiv -2A^2\sum_{k=1}^{p-1}\frac{\alpha^k}{A^k k^2} - 2\beta^{2p}\sum_{k=1}^{p-1}\frac{\alpha^{2k}}{(-B)^k k^2} \pmod p,$$

and

$$\left(\frac{v_p(A,B) - A^p}{p}\right)^2 \equiv -2A\alpha^p\sum_{k=1}^{p-1}\frac{\alpha^k}{A^k k^2} - 2\beta^{2p}\sum_{k=1}^{p-1}\frac{A^k\alpha^k}{B^k k^2} \pmod p.$$

Proof of the proposition

By the lemma and Fermat's little theorem,

$$\frac{1}{A^2}\left(\frac{x^p+(A-x)^p-A^p}{p}\right)^2$$

$$\equiv\left(\frac{(x/A)^p+(1-x/A)^p-1}{p}\right)^2$$

$$\equiv -2\sum_{k=1}^{p-1}\frac{(1-x/A)^k}{k^2}-2\left(\frac{x}{A}\right)^{2p}\sum_{k=1}^{p-1}\frac{(1-A/x)^k}{k^2} \pmod{p}.$$

Note that $v_p(A,B)=\beta^p+\alpha^p=\beta^p+(A-\beta)^p$ and $\alpha\beta=B$. So we have

$$\left(\frac{v_p(A,B)-A^p}{p}\right)^2\equiv -2A^2\sum_{k=1}^{p-1}\frac{(A-\beta)^k}{A^k k^2}$$

$$-2\beta^{2p}\sum_{k=1}^{p-1}\frac{(1-A\alpha/B)^k}{k^2} \pmod{p}$$

and hence the first desired congruence holds since $A\alpha-B=\alpha^2$.

Proof of the proposition (continued)

On the other hand,

$$\alpha^p(A^p - v_p(A,B)) = \alpha^p(A^p - \alpha^p - \beta^p) = (B+\alpha^2)^p + (-\alpha^2)^p - B^p$$

and hence

$$\begin{aligned}
&\alpha^{2p}\left(\frac{A^p - v_p(A,B)}{p}\right)^2 \\
=&\left(\frac{(-\alpha^2)^p + (B-(-\alpha^2))^p - B^p}{p}\right)^2 \\
\equiv&-2B^2\sum_{k=1}^{p-1}\frac{(1-(-\alpha^2)/B)^k}{k^2} - 2(-\alpha^2)^{2p}\sum_{k=1}^{p-1}\frac{(1-B/(-\alpha^2))^k}{k^2} \\
=&-2B^2\sum_{k=1}^{p-1}\frac{(A\alpha)^k}{B^k k^2} - 2\alpha^{4p}\sum_{k=1}^{p-1}\frac{(A\alpha)^k}{\alpha^{2k}k^2} \\
\equiv&-2(\alpha\beta)^{2p}\sum_{k=1}^{p-1}\frac{(A\alpha)^k}{B^k k^2} - 2A\alpha^{3p}\sum_{k=1}^{p-1}\frac{\alpha^{p-k}}{A^{p-k}(p-k)^2} \pmod{p}.
\end{aligned}$$

Therefore the second desired congruence follows.

Proof of $\sum_{k=1}^{p-1} L_k/k^2 \equiv 0 \pmod{p}$

Let $p > 5$ be a prime. We prove $\sum_{k=1}^{p-1} L_k/k^2 \equiv 0 \pmod{p}$.
Let α and β be the two roots of the equation $x^2 - x - 1 = 0$.
Applying the Proposition with $A = 1$ and $B = -1$, we get

$$\left(\frac{L_p - 1}{p}\right)^2 \equiv -2\sum_{k=1}^{p-1}\frac{\alpha^k}{k} - 2\beta^{2p}\sum_{k=1}^{p-1}\frac{\alpha^{2k}}{k^2} \pmod{p}, \tag{1}$$

$$\left(\frac{L_p - 1}{p}\right)^2 \equiv -2\alpha^p\sum_{k=1}^{p-1}\frac{\alpha^k}{k^2} - 2\beta^{2p}\sum_{k=1}^{p-1}\frac{(-\alpha)^k}{k^2} \pmod{p}. \tag{2}$$

$$\begin{aligned}\sum_{k=1}^{p-1}\frac{2\alpha^{2k}}{(2k)^2} &= \sum_{j=1}^{2p-1}(1+(-1)^j)\frac{\alpha^j}{j^2} \\ &= \sum_{k=1}^{p-1}\left(\frac{\alpha^k + (-\alpha)^k}{k^2} + \frac{\alpha^{p+k} + (-\alpha)^{p+k}}{(p+k)^2}\right) \\ &\equiv (1+\alpha^p)\sum_{k=1}^{p-1}\frac{\alpha^k}{k^2} + (1-\alpha^p)\sum_{k=1}^{p-1}\frac{(-\alpha)^k}{k^2} \pmod{p},\end{aligned}$$

Proof of $\sum_{k=1}^{p-1} L_k/k^2 \equiv 0 \pmod p$

so (1) can be rewritten as

$$\left(\frac{L_p-1}{p}\right)^2 \equiv -2(1+2(1+\alpha^p)\beta^{2p})\sum_{k=1}^{p-1}\frac{\alpha^k}{k^2} - 4(1-\alpha^p)\beta^{2p}\sum_{k=1}^{p-1}\frac{(-\alpha)^k}{k^2} \pmod p. \qquad (3)$$

Multiplying (2) by $2(1-\alpha^p)$ and then subtracting it from (3) we obtain

$$(2\alpha^p-1)\left(\frac{L_p-1}{p}\right)^2 \equiv \left(4\alpha^p(1-\alpha^p)-2-4(1+\alpha^p)\beta^{2p}\right)\sum_{k=1}^{p-1}\frac{\alpha^k}{k^2} = (4L_p-4L_{2p}-2)\sum_{k=1}^{p-1}\frac{\alpha^k}{k^2} \pmod p.$$

Proof of $\sum_{k=1}^{p-1} L_k/k^2 \equiv 0 \pmod{p}$

Now that $L_p \equiv 1 \pmod{p}$ and

$$L_{2p} = \alpha^{2p}+\beta^{2p} \equiv (\alpha^2+\beta^2)^p = \left((\alpha+\beta)^2 - 2\alpha\beta\right)^p = 3^p \equiv 3 \pmod{p},$$

we have

$$(2\alpha^p-1)\left(\frac{L_p-1}{p}\right)^2 \equiv (4-4\times3-2)\sum_{k=1}^{p-1}\frac{\alpha^k}{k^2} = -10\sum_{k=1}^{p-1}\frac{\alpha^k}{k^2} \pmod{p}.$$

Similarly,

$$(2\beta^p-1)\left(\frac{L_p-1}{p}\right)^2 \equiv -10\sum_{k=1}^{p-1}\frac{\beta^k}{k^2} \pmod{p}.$$

As $2\alpha^p - 1 + (2\beta^p-1) = 2L_p - 2 \equiv 0 \pmod{p}$, we finally obtain

$$\sum_{k=1}^{p-1}\frac{L_k}{k^2} = \sum_{k=1}^{p-1}\frac{\alpha^k+\beta^k}{k^2} \equiv 0 \pmod{p}.$$

More conjectures on congruences

For more conjectures of mine on congruences, see

Z. W. Sun, *Open Conjectures on Congruences*, `arXiv:0911.5665`

which contains **100 unsolved conjectures** raised by me.

You are welcome to solve my conjectures!

Thank you!