Sci. China Math. 57(2014), no. 10, 2091–2102.

PROOF OF THREE CONJECTURES ON CONGRUENCES

Hao Pan and Zhi-Wei Sun

Department of Mathematics, Nanjing University
Nanjing 210093, People's Republic of China
haopan1979@gmail.com, zwsun@nju.edu.cn

Abstract. In this paper we prove three conjectures on congruences involving central binomial coefficients or Lucas sequences. Let p be an odd prime and let a be a positive integer. We show that if $p \equiv 1 \pmod 4$ or $a > 1$ then

$$\sum_{k=0}^{\lfloor \frac{3}{4}p^a \rfloor} \binom{-1/2}{k} \equiv \left(\frac{2}{p^a}\right) \pmod{p^2},$$

where $(-)$ denotes the Jacobi symbol. This confirms a conjecture of the second author. We also confirm a conjecture of R. Tauraso by showing that

$$\sum_{k=1}^{p-1} \frac{L_k}{k^2} \equiv 0 \pmod p \quad \text{provided } p > 5,$$

where the Lucas numbers $L_0, L_1, L_2, \ldots$ are defined by $L_0 = 2,\ L_1 = 1$ and $L_{n+1} = L_n + L_{n-1}$ $(n = 1, 2, 3, \ldots)$. Our third theorem states that if $p \neq 5$ then we can determine $F_{p^a - (\frac{p^a}{5})} \bmod p^3$ in the following way:

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

which appeared as a conjecture in a paper of Sun and Tauraso in 2010.

1. Introduction

In this paper we aim to prove three conjectures on congruences.

Our first theorem confirms a conjecture raised by the second author [S11, Conjecture 1.2].

2010 *Mathematics Subject Classification.* Primary 11B65, 11A07; Secondary 05A10, 11B39.

The second author is the corresponding author.

Theorem 1.1. *Let p be an odd prime and let a be a positive integer. If $p\equiv 1 \pmod 4$ or $a>1$, then we have*

$$\sum_{k=0}^{\lfloor\frac34 p^a\rfloor}\binom{-1/2}{k}\equiv\left(\frac{2}{p^a}\right)\pmod{p^2},\tag{1.1}$$

where $(-)$ denotes the Jacobi symbol.

Our second theorem confirms a nice conjecture of R. Tauraso [T], and it presents a congruence involving Lucas numbers which is similar to the well-known Wolstenholme congruence $\sum_{k=1}^{p-1}1/k^2\equiv 0 \pmod p$ with $p>3$ prime (cf. [Wo]).

Theorem 1.2. *Let $p>5$ be a prime. Then*

$$\sum_{k=1}^{p-1}\frac{L_k}{k^2}\equiv 0 \pmod p,\tag{1.2}$$

where the Lucas numbers $L_0, L_1, L_2, \dots$ are defined by $L_0=2,\ L_1=1$ and $L_{n+1}=L_n+L_{n-1}$ $(n=1,2,3,\dots)$.

The Fibonacci sequence $\{F_n\}_{n\geqslant 0}$ is given by $F_0=0,\ F_1=1$ and $F_{n+1}=F_n+F_{n-1}$ $(n=1,2,3,\dots)$. It is well-known that $p\mid F_{p-(\frac{p}{5})}$ for any odd prime p, and the Fibonacci quotient $F_{p-(\frac{p}{5})}/p$ modulo p is closely related to fundamental units of real quadratic fields (cf. H. C. Williams [W]) and Vandiver's conjecture about class numbers of real cyclotomic fields (cf. S. Jakubec [J]). Our following theorem determines $F_{p^a-(\frac{p^a}{5})}$ mod p^3 for any $a=1,2,3,\dots$, and the result appeared as Conjecture 1.1 of Sun and Tauraso [ST].

Theorem 1.3. *Let $p\neq 2,5$ be a prime and let a be a positive integer. Then we have*

$$\sum_{k=0}^{p^a-1}(-1)^k\binom{2k}{k}\equiv\left(\frac{p^a}{5}\right)(1-2F_{p^a-(\frac{p^a}{5})})\pmod{p^3}.\tag{1.3}$$

Note that (1.3) modulo p is [ST, (1.7)] with $d=0$, and (1.3) modulo p^2 was given in [S10, Corollary 1.1].

Those primes $p>5$ satisfying the congruence $F_{p-(\frac{p}{5})}\equiv 0 \pmod{p^2}$ are called Wall-Sun-Sun primes (cf. [CP, p. 32] and [SS]). It is known that there are no Wall-Sun-Sun primes below 4.5×10^{16} (cf. [P]).

To understand our proofs of Theorems 1.1-1.3 one needs some basic knowledge of Lucas sequences.

Let A and B be two integers. The Lucas sequence $u_n = u_n(A,B)$ ($n \in \mathbb{N} = \{0,1,2,\dots\}$) and its companion $v_n = v_n(A,B)$ ($n \in \mathbb{N}$) are defined by

$$u_0 = 0,\ u_1 = 1,\ u_{n+1} = Au_n - Bu_{n-1} \quad \text{for } n = 1,2,3,\dots,$$

and

$$v_0 = 2,\ v_1 = A,\ v_{n+1} = Av_n - Bv_{n-1} \quad \text{for } n = 1,2,3,\dots.$$

Let $\Delta = A^2 - 4B$. The characteristic equation $x^2 - Ax + B = 0$ has two roots

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

which are both algebraic integers. It is well known that

$$(\alpha-\beta)u_n = \alpha^n - \beta^n \quad \text{and} \quad v_n = \alpha^n + \beta^n \quad \text{for all } n = 0,1,2,\dots.$$

For an odd prime p and a positive integer a, clearly

$$v_{p^a} \equiv (\alpha+\beta)^{p^a} = A^{p^a} \equiv A \pmod{p}$$

and

$$\Delta u_{p^a} = (\alpha-\beta)(\alpha^{p^a}-\beta^{p^a}) \equiv (\alpha-\beta)^{p^a+1} = \Delta^{(p^a+1)/2} \equiv \Delta\left(\frac{\Delta}{p^a}\right) \pmod{p}.$$

It is also known that $p^a \mid u_{p^a-(\frac{\Delta}{p^a})}$ provided that $p \nmid B$ (see, e.g., [S10, Lemma 2.3]).

Note that $F_n = u_n(1,-1)$ ($n \in \mathbb{N}$) and $L_n = v_n(1,-1)$ ($n \in \mathbb{N}$) are familiar Fibonacci numbers and Lucas numbers respectively. The Pell sequence and its companion are given by $P_n = u_n(2,-1)$ ($n \in \mathbb{N}$) and $Q_n = v_n(2,-1)$ ($n \in \mathbb{N}$) respectively.

We will show Theorems 1.1-1.3 in Sections 2-4 respectively. In the proofs of Theorems 1.2 and 1.3, we employ the useful technique of A. Granville [Gr] and deal with congruences in the ring of algebraic integers.

2. Proof of Theorem 1.1

Lemma 2.1. *Let p be an odd prime and let a be a positive integer. Then*

$$P_{p^a-(\frac{2}{p^a})}Q_{p^a-(\frac{2}{p^a})} \equiv \left(\frac{2}{p^a}\right)\frac{Q_{p^a}-2}{2} \pmod{p^2}. \tag{2.1}$$

Proof. Recall that $P_n = u_n(2,-1)$ and $Q_n = v_n(2,-1)$ for all $n \in \mathbb{N}$. So

$$P_{p^a} \equiv \left(\frac{2}{p^a}\right) \pmod p \quad \text{and} \quad Q_{p^a} \equiv 2 \pmod p.$$

Since $Q_{n-1} = 4P_n - Q_n$ and $Q_{n+1} = 4P_n + Q_n$ for $n = 1,2,3,\ldots$, we have

$$\left(\frac{2}{p^a}\right) Q_{p^a-(\frac{2}{p^a})} = 4\left(\frac{2}{p^a}\right) P_{p^a} - Q_{p^a} \equiv 2 \pmod p.$$

Similarly,

$$P_{p^a-(\frac{2}{p^a})} = \frac{Q_{p^a}}{2} - \left(\frac{2}{p^a}\right) P_{p^a} \equiv 0 \pmod p.$$

Clearly $\alpha = 1+\sqrt{2}$ and $\beta = 1-\sqrt{2}$ are the two roots of the equation $x^2 - 2x - 1 = 0$. Thus

$$Q_n^2 - 8P_n^2 = (\alpha^n + \beta^n)^2 - (\alpha^n - \beta^n)^2 = 4(\alpha\beta)^n = 4(-1)^n$$

for all $n \in \mathbb{N}$. Therefore

$$Q^2_{p^a-(\frac{2}{p^a})} - 4 = 8P^2_{p^a-(\frac{2}{p^a})} \equiv 0 \pmod{p^2}$$

and hence

$$4\left(\frac{2}{p^a}\right) P_{p^a} - Q_{p^a} = \left(\frac{2}{p^a}\right) Q_{p^a-(\frac{2}{p^a})} \equiv 2 \pmod{p^2}.$$

It follows that

$$\begin{aligned}&\left(\frac{2}{p^a}\right) P_{p^a-(\frac{2}{p^a})} Q_{p^a-(\frac{2}{p^a})}\\ \equiv& 2P_{p^a-(\frac{2}{p^a})} = Q_{p^a} - 2\left(\frac{2}{p^a}\right) P_{p^a} \equiv \frac{Q_{p^a}}{2} - 1 \pmod{p^2}.\end{aligned}$$

This proves (2.1). $\square$

Lemma 2.2. *Let p be an odd prime and let a be a positive integer. Suppose that $p \equiv 1 \pmod 4$ or $a > 1$. Then*

$$p^a \sum_{0 \leqslant k < \lfloor p^a/4 \rfloor} \frac{1}{\binom{(p^a-3)/2}{k}} \equiv \left(\frac{2}{p^a}\right) \frac{Q_{p^a} - 2}{4} \pmod{p^2}. \tag{2.2}$$

Proof. If $p^a \equiv 1 \pmod 4$, then $(p^a - 3)/2$ is odd and hence

$$\sum_{k=0}^{(p^a-1)/4-1} \frac{1}{\binom{(p^a-3)/2}{k}} = \frac{1}{2} \sum_{k=0}^{(p^a-3)/2} \frac{1}{\binom{(p^a-3)/2}{k}}.$$

If $p^a \equiv 3 \pmod 4$, then $a \in \{3, 5, \dots\}$ and

$$\sum_{k=0}^{(p^a-3)/4-1} \frac{1}{\binom{(p^a-3)/2}{k}} = \frac{1}{2}\sum_{k=0}^{(p^a-3)/2} \frac{1}{\binom{(p^a-3)/2}{k}} - \frac{1}{2}\cdot\frac{1}{\binom{(p^a-3)/2}{(p^a-3)/4}}.$$

In the case $p^a \equiv 3 \pmod 4$, as the fractional parts of $(p^a-3)/(2p)$ and $(p^a-3)/(4p)$ are $(p-3)/(2p)$ and $(p-3)/(4p)$ respectively, we have

$$\left\lfloor \frac{(p^a-3)/2}{p} \right\rfloor = 2\left\lfloor \frac{(p^a-3)/4}{p} \right\rfloor$$

and hence

$$\nu_p\left(\binom{(p^a-3)/2}{(p^a-3)/4}\right) = \sum_{j=1}^{a-1}\left(\left\lfloor \frac{(p^a-3)/2}{p^j} \right\rfloor - 2\left\lfloor \frac{(p^a-3)/4}{p^j} \right\rfloor\right) < a-1,$$

where $\nu_p(x)$ denotes the p-adic valuation of an integer x. (It is well known that $\nu_p(n!) = \sum_{j=1}^{\infty}\lfloor n/p^j \rfloor$ for any $n \in \mathbb{N}$.) Therefore,

$$p^a \sum_{0\leqslant k<\lfloor p^a/4\rfloor} \frac{1}{\binom{(p^a-3)/2}{k}} \equiv \frac{p^a}{2}\sum_{k=0}^{(p^a-3)/2} \frac{1}{\binom{(p^a-3)/2}{k}} \pmod{p^2}.$$

Applying the known identity

$$\sum_{k=0}^{n} \frac{x^k}{\binom{n}{k}} = (n+1)\left(\frac{x}{1+x}\right)^{n+1}\sum_{k=1}^{n+1}\frac{1+x^k}{k(1+x)}\left(\frac{1+x}{x}\right)^k$$

(cf. [G, (2.4)]) with $x=1$ and $n=(p^a-3)/2$, we get

$$\begin{aligned}\frac{p^a}{2}\sum_{k=0}^{(p^a-3)/2} \frac{1}{\binom{(p^a-3)/2}{k}} &= \frac{p^a(p^a-1)}{2^{(p^a+3)/2}}\sum_{k=1}^{(p^a-1)/2}\frac{2^k}{k} \\ &\equiv -\left(\frac{2}{p^a}\right)\frac{p^a}{4}\sum_{k=1}^{(p^a-1)/2}\frac{2^k}{k} \pmod{p^2}.\end{aligned}$$

Since

$$\binom{p^a}{j} = \frac{p^a}{j}\prod_{0<i<j}\frac{p^a-i}{i} \equiv \frac{p^a}{j}(-1)^{j-1} \pmod{p^2}$$

for all $j=1,\dots,p^a-1$, we have

$$\begin{aligned}p^a\sum_{k=1}^{(p^a-1)/2}\frac{2^k}{k} &\equiv -2\sum_{k=1}^{(p^a-1)/2}\binom{p^a}{2k}2^k = -\sum_{k=1}^{p^a}\binom{p^a}{k}(\sqrt{2}^k + (-\sqrt{2})^k) \\ &= -(1+\sqrt{2})^{p^a} - (1-\sqrt{2})^{p^a} + 2 = -Q_{p^a} + 2 \pmod{p^2}.\end{aligned}$$

Combining the above we immediately get (2.2). □

Proof of Theorem 1.1. Clearly,

$$\binom{-1/2}{k} = \frac{\binom{2k}{k}}{(-4)^k} \qquad \text{for all } k = 0, 1, 2, \ldots .$$

Choose $\delta \in \{1, 3\}$ such that $p^a \equiv \delta \pmod 4$. Then

$$\sum_{k=0}^{\lfloor \frac{3}{4}p^a \rfloor} \binom{-1/2}{k} = \sum_{k=0}^{p^a-1} \frac{\binom{2k}{k}}{(-4)^k} - \sum_{k=(3p^a+\delta)/4}^{p^a-1} \frac{\binom{2k}{k}}{(-4)^k}.$$

By Sun [S10, Theorem 1.1 and Lemma 2.3],

$$\sum_{k=0}^{p^a-1} \frac{\binom{2k}{k}}{(-4)^k} \equiv \left(\frac{2}{p^a}\right) + u_{p^a-(\frac{2}{p^a})}(-6, 1) \pmod{p^2}.$$

Hence we only need to prove the following congruence:

$$\sum_{k=(3p^a+\delta)/4}^{p^a-1} \frac{\binom{2k}{k}}{(-4)^k} \equiv u_{p^a-(\frac{2}{p^a})}(-6, 1) \pmod{p^2} \tag{2.3}$$

provided that $p \equiv 1 \pmod 4$ or $a > 1$.

Let k and l be positive integers with $k + l = p^a$ and $0 < l < p^a/2$. Then

$$\frac{\binom{2k}{k}}{\binom{2p^a-2}{p^a-1}} = \frac{(2p^a - 2l)!}{(2p^a - 2)!} \left(\frac{(p^a - 1)!}{(p^a - l)!}\right)^2 = \frac{\prod_{0<i<l}(p^a - i)^2}{\prod_{1<j<2l}(2p^a - j)}$$

and hence

$$\frac{\binom{2k}{k}}{\binom{2p^a-2}{p^a-1}} \cdot \frac{(2l-1)!}{(l-1)!^2} = \frac{\prod_{0<i<l}(1 - p^a/i)^2}{\prod_{1<j<2l}(1 - 2p^a/j)} \equiv 1 \pmod p.$$

Note that

$$\binom{2p^a - 2}{p^a - 1} = p^a \prod_{j=2}^{p^a-1} \frac{2p^a - j}{j} \equiv -p^a \pmod{p^{a+1}}$$

and

$$\binom{2k}{k} = \binom{p^a + (2k - p^a)}{0p^a + k} \equiv \binom{2k - p^a}{k} = 0 \pmod p$$

by Lucas' theorem. So we have

$$\frac{l}{2}\binom{2l}{l}=\frac{(2l-1)!}{(l-1)!^2}\not\equiv 0 \pmod{p^a}$$

and

$$\binom{2k}{k}\equiv -p^a\frac{(l-1)!^2}{(2l-1)!}=-\frac{2p^a}{l\binom{2l}{l}} \pmod{p^2}.$$

In view of the above,

$$\sum_{k=(3p^a+\delta)/4}^{p^a-1}\frac{\binom{2k}{k}}{(-4)^k}\equiv\frac{-2p^a}{(-4)^{p^a}}\sum_{l=1}^{(p^a-\delta)/4}\frac{(-4)^l}{l\binom{2l}{l}}\equiv\frac{p^a}{2}\sum_{k=1}^{(p^a-\delta)/4}\frac{(-4)^k}{k\binom{2k}{k}} \pmod{p^2}.$$

For $k=1,\dots,(p^a-1)/2$, clearly

$$\begin{aligned}\frac{\binom{(p^a-1)/2}{k}}{\binom{2k}{k}/(-4)^k}=&\frac{\binom{(p^a-1)/2}{k}}{\binom{-1/2}{k}}=\prod_{j=0}^{k-1}\frac{(p^a-1)/2-j}{-1/2-j}\\ =&\prod_{j=0}^{k-1}\left(1-\frac{p^a}{2j+1}\right)\equiv 1 \pmod{p}\end{aligned}$$

and hence

$$\frac{\binom{(p^a-3)/2}{k-1}}{k\binom{2k}{k}/(-4)^k}\equiv\frac{2}{p^a-1}\equiv -2 \pmod{p}.$$

Therefore

$$\frac{p^a}{2}\sum_{k=1}^{(p^a-\delta)/4}\frac{(-4)^k}{k\binom{2k}{k}}\equiv -p^a\sum_{k=0}^{(p^a-\delta)/4-1}\frac{1}{\binom{(p^a-3)/2}{k}} \pmod{p^2}.$$

So far we have reduced (2.3) to the following congruence:

$$p^a\sum_{k=0}^{(p^a-\delta)/4-1}\frac{1}{\binom{(p^a-3)/2}{k}}\equiv -u_{p^a-(\frac{2}{p^a})}(-6,1) \pmod{p^2}. \tag{2.4}$$

In view of (2.4) and Lemma 2.2, it suffices to show that

$$u_{p^a-(\frac{2}{p^a})}(-6,1)\equiv-\left(\frac{2}{p^a}\right)\frac{Q_{p^a}-2}{4} \pmod{p^2}.$$

As $-3+2\sqrt{2}$ and $-3-2\sqrt{2}$ are the two roots of the equation $x^2+6x+1=0$, for any $n\in\mathbb{N}$ we have

$$\begin{aligned}u_n(-6,1)=&\frac{(-3+2\sqrt{2})^n-(-3-2\sqrt{2})^n}{4\sqrt{2}}\\=&\frac{(-1)^{n-1}}{2}\cdot\frac{(1+\sqrt{2})^{2n}-(1-\sqrt{2})^{2n}}{2\sqrt{2}}=\frac{(-1)^{n-1}}{2}P_nQ_n\end{aligned}$$

Therefore, with the help of Lemma 2.1 we finally obtain

$$u_{p^a-(\frac{2}{p^a})}(-6,1)=-\frac{1}{2}P_{p^a-(\frac{2}{p^a})}Q_{p^a-(\frac{2}{p^a})}\equiv-\left(\frac{2}{p^a}\right)\frac{Q_{p^a}-2}{4}\pmod{p^2}$$

as desired.

The proof of Theorem 1.1 is now complete. □

3. Proof of Theorem 1.2

Lemma 3.1. *Let $p>3$ be a prime. Then we have the following congruence:*

$$\left(\frac{x^p+(1-x)^p-1}{p}\right)^2\equiv-2\sum_{k=1}^{p-1}\frac{(1-x)^k}{k^2}-2x^{2p}\sum_{k=1}^{p-1}\frac{(1-x^{-1})^k}{k^2}\pmod{p}. \tag{3.1}$$

Proof. (3.1) follows immediately if we combine (4) and (5) of Granville [Gr]. □

Proposition 3.2. *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*

$$\left(\frac{v_p(A,B)-A^p}{p}\right)^2\equiv-2A^2\sum_{k=1}^{p-1}\frac{\alpha^k}{A^kk^2}-2\beta^{2p}\sum_{k=1}^{p-1}\frac{\alpha^{2k}}{(-B)^kk^2}\pmod{p}, \tag{3.2}$$

and

$$\left(\frac{v_p(A,B)-A^p}{p}\right)^2\equiv-2A\alpha^p\sum_{k=1}^{p-1}\frac{\alpha^k}{A^kk^2}-2\beta^{2p}\sum_{k=1}^{p-1}\frac{A^k\alpha^k}{B^kk^2}\pmod{p}. \tag{3.3}$$

Proof. By (3.1) and Fermat's little theorem,

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

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

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

and hence (3.2) holds since $A\alpha - B = \alpha^2$.

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 (3.3) follows. □

Proof of Theorem 1.2. Let α and β be the two roots of the equation $x^2 - x - 1 = 0$. Applying Proposition 3.2 with $A = 1$ and $B = -1$, we get

$$\left(\frac{L_p - 1}{p}\right)^2 \equiv -2\sum_{k=1}^{p-1}\frac{\alpha^k}{k^2} - 2\beta^{2p}\sum_{k=1}^{p-1}\frac{\alpha^{2k}}{k^2} \pmod p \tag{3.4}$$

and

$$\left(\frac{L_p - 1}{p}\right)^2 \equiv -2\alpha^p\sum_{k=1}^{p-1}\frac{\alpha^k}{k^2} - 2\beta^{2p}\sum_{k=1}^{p-1}\frac{(-\alpha)^k}{k^2} \pmod p. \tag{3.5}$$

Since

$$\sum_{k=1}^{p-1}\frac{2\alpha^{2k}}{(2k)^2}=\sum_{j=1}^{2p-1}(1+(-1)^j)\frac{\alpha^j}{j^2}=\sum_{k=1}^{p-1}\left(\frac{\alpha^k+(-\alpha)^k}{k^2}+\frac{\alpha^{p+k}+(-\alpha)^{p+k}}{(p+k)^2}\right)$$

$$\equiv(1+\alpha^p)\sum_{k=1}^{p-1}\frac{\alpha^k}{k^2}+(1-\alpha^p)\sum_{k=1}^{p-1}\frac{(-\alpha)^k}{k^2}\pmod p,$$

(3.4) can be rewritten as

$$\begin{aligned}\left(\frac{L_p-1}{p}\right)^2\equiv&-2(1+2(1+\alpha^p)\beta^{2p})\sum_{k=1}^{p-1}\frac{\alpha^k}{k^2}\\&-4(1-\alpha^p)\beta^{2p}\sum_{k=1}^{p-1}\frac{(-\alpha)^k}{k^2}\pmod p.\end{aligned}\tag{3.6}$$

Multiplying (3.5) by $2(1-\alpha^p)$ and then subtracting it from (3.6) we obtain

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

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

$$(2\alpha^p-1)\left(\frac{L_p-1}{p}\right)^2\equiv(4-4\times 3-2)\sum_{k=1}^{p-1}\frac{\alpha^k}{k^2}=-10\sum_{k=1}^{p-1}\frac{\alpha^k}{k^2}\pmod p.$$

Similarly,

$$(2\beta^p-1)\left(\frac{L_p-1}{p}\right)^2\equiv-10\sum_{k=1}^{p-1}\frac{\beta^k}{k^2}\pmod p.\tag{3.7}$$

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

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

So far we have completed the proof of Theorem 1.2. □

Remark 3.3. Let $p>5$ be a prime. In view of (3.7), we also have

$$\sum_{k=1}^{p-1}\frac{F_k}{k^2}\equiv-\frac{2F_p}{10}\left(\frac{L_p-1}{p}\right)^2\equiv-\frac{1}{5}\left(\frac{p}{5}\right)\left(\frac{L_p-1}{p}\right)^2\pmod p.\tag{3.8}$$

4. Proof of Theorem 1.3

We need a lemma which extends a congruence due to Granville [Gr, (6)].

Lemma 4.1. *Let p be an odd prime and let a be a positive integer. Then*

$$\begin{aligned}&p\delta_{p,3}+p^{a-1}\sum_{k=1}^{p^a-1}\frac{(1-x)^k}{k}\\ \equiv&\frac{1-x^{p^a}-(1-x)^{p^a}}{p}-p\bigg(\sum_{k=1}^{p-1}\frac{x^k}{k^2}\bigg)^{p^{a-1}}\pmod{p^2},\end{aligned}\tag{4.1}$$

where the Kronecker symbol $\delta_{p,3}$ is 1 or 0 according as $p=3$ or not.

Proof. As observed by Granville [Gr], for any integer $n>1$ we have

$$\begin{aligned}\sum_{k=1}^{n-1}\frac{(1-x)^k-1}{k}=&\sum_{k=1}^{n-1}\frac{1}{k}\sum_{j=1}^{k}\binom{k}{j}(-x)^j=\sum_{j=1}^{n-1}\frac{(-x)^j}{j}\sum_{k=j}^{n-1}\binom{k-1}{j-1}\\ =&\sum_{j=1}^{n-1}\frac{(-x)^j}{j}\binom{n-1}{j}\quad\text{(by [G, (1.52)])}\\ =&\sum_{j=1}^{n-1}\frac{(-x)^j}{j}\bigg(\frac{n}{j}\binom{n-1}{j-1}-\frac{j}{n}\binom{n}{j}\bigg)\\ =&n\sum_{j=1}^{n-1}\binom{n-1}{j-1}\frac{(-x)^j}{j^2}-\frac{(1-x)^n-(-x)^n-1}{n}.\end{aligned}$$

Note that

$$\begin{aligned}2p^{a-1}\sum_{k=1}^{p^a-1}\frac{1}{k}=&p^{a-1}\sum_{k=1}^{p^a-1}\bigg(\frac{1}{k}+\frac{1}{p^a-k}\bigg)=\sum_{k=1}^{p^a-1}\frac{p^a}{k}\cdot\frac{p^{a-1}}{p^a-k}\\ \equiv&\sum_{j=1}^{p-1}\frac{p^a}{p^{a-1}j}\cdot\frac{p^{a-1}}{p^a-p^{a-1}j}\equiv-p\sum_{j=1}^{p-1}\frac{1}{j^2}\equiv p\delta_{p,3}\pmod{p^2}.\end{aligned}$$

(As $\sum_{j=1}^{p-1}1/j^2\equiv\sum_{k=1}^{p-1}1/(2k)^2 \pmod p$, we have $\sum_{j=1}^{p-1}1/j^2\equiv 0\pmod p$ if $p>3$.) Hence

$$p^{a-1}\sum_{k=1}^{p^a-1}\frac{1}{k}\equiv-p\delta_{p,3}\pmod{p^2}.$$

Note also that

$$\binom{p^a-1}{j-1}=\prod_{0<i<j}\frac{p^a-i}{i}\equiv(-1)^{j-1}\pmod p.$$

Therefore

$$\begin{aligned} &p^{a-1}\sum_{k=1}^{p^a-1}\frac{(1-x)^k}{k}+p\delta_{p,3}\\ \equiv&p^{a-1}\sum_{k=1}^{p^a-1}\frac{(1-x)^k-1}{k}\\ \equiv&-p^{2a-1}\sum_{j=1}^{p^a-1}\frac{x^j}{j^2}-\frac{x^{p^a}+(1-x)^{p^a}-1}{p} \pmod{p^2} \end{aligned}$$

To complete the proof, it suffices to note that

$$p^{2a-1}\sum_{j=1}^{p^a-1}\frac{x^j}{j^2}\equiv p^{2a-1}\sum_{k=1}^{p-1}\frac{x^{p^{a-1}k}}{(p^{a-1}k)^2}=p\sum_{k=1}^{p-1}\frac{x^{p^{a-1}k}}{k^2} \pmod{p^2}$$

and

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

This concludes the proof. □

Proposition 4.2. *Let $p\neq 2,5$ be a prime and let a be a positive integer. Then*

$$p^{a-1}\sum_{k=1}^{p^a-1}\frac{F_{2(p^a-k)}}{k}\equiv\frac{F_{2p^a}-F_{p^a}}{p}+\frac{p}{10}\left(\frac{p^a}{5}\right)\left(\frac{L_p-1}{p}\right)^2 \pmod{p^2}. \tag{4.2}$$

Proof. Let α and β be the two roots of the equation $x^2-x-1=0$. Clearly $\alpha+\beta=1$ and $\alpha\beta=-1$. Set

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

By Lemma 4.1 we have

$$p\delta_{p,3}+g(1-x)\equiv -q(x)-pG(x)^{p^{a-1}} \pmod{p^2}.$$

In view of (3.7),

$$G(\beta)\equiv\frac{1-2\beta^p}{10}\left(\frac{L_p-1}{p}\right)^2-\delta_{p,3} \pmod{p}$$

(this can be checked directly when $p=3$). Hence

$$\begin{aligned}G(-\alpha)=&G(\beta^{-1})=\frac{1}{\beta^p}\sum_{k=1}^{p-1}\frac{\beta^{p-k}}{k^2}\\&\equiv-\alpha^pG(\beta)\equiv\delta_{p,3}\alpha^p-\frac{2+\alpha^p}{10}\left(\frac{L_p-1}{p}\right)^2\pmod p.\end{aligned}$$

Note that

$$q(-\alpha)=\frac{(-\alpha)^{p^a}+(1+\alpha)^{p^a}-1}{p}=\frac{\alpha^{p^a}(\alpha^{p^a}+\beta^{p^a}-1)}{p}=\alpha^{p^a}\frac{L_{p^a}-1}{p}.$$

Applying Lemma 4.1 we get

$$\begin{aligned}&g(\alpha^2)=g(1-(-\alpha))\\&\equiv-p\delta_{p,3}-pG(-\alpha)^{p^{a-1}}-q(-\alpha)\\&\equiv-p\delta_{p,3}-p\delta_{p,3}\alpha^{p^a}+p\left(\frac{\alpha^p+2}{10}\right)^{p^{a-1}}\left(\frac{L_p-1}{p}\right)^{2p^{a-1}}-\alpha^{p^a}\frac{L_{p^a}-1}{p}\\&\equiv-p\delta_{p,3}(1+\alpha)^{p^a}+p\frac{\alpha^{p^a}+2}{10}\left(\frac{L_p-1}{p}\right)^2-\alpha^{p^a}\frac{L_{p^a}-1}{p}\pmod{p^2}\end{aligned}$$

and hence

$$\begin{aligned}&\beta^{2p^a}g(\alpha^2)+p\delta_{p,3}(\alpha\beta)^{2p^a}\\\equiv&p\frac{2\beta^{2p^a}-\beta^{p^a}}{10}\left(\frac{L_p-1}{p}\right)^2+\beta^{p^a}\frac{L_{p^a}-1}{p}\pmod{p^2}.\end{aligned}$$

As $\beta^{2p^a}=(1+\beta)^{p^a}\equiv1+\beta^{p^a}\pmod p$, we have

$$\beta^{2p^a}g(\alpha^2)\equiv-p\delta_{p,3}+p\frac{2+\beta^{p^a}}{10}\left(\frac{L_p-1}{p}\right)^2+\beta^{p^a}\frac{L_{p^a}-1}{p}\pmod{p^2}.$$

Similarly,

$$\alpha^{2p^a}g(\beta^2)\equiv-p\delta_{p,3}+p\frac{2+\alpha^{p^a}}{10}\left(\frac{L_p-1}{p}\right)^2+\alpha^{p^a}\frac{L_{p^a}-1}{p}\pmod{p^2}.$$

Observe that

$$\begin{aligned}\sum_{k=1}^{p^a-1}\frac{F_{2(p^a-k)}}{k}&=\sum_{k=1}^{p^a-1}\frac{\alpha^{2p^a-2k}-\beta^{2p^a-2k}}{(\alpha-\beta)k}\\&=\frac{1}{\alpha-\beta}\left(\alpha^{2p^a}\sum_{k=1}^{p^a-1}\frac{\beta^{2k}}{k}-\beta^{2p^a}\sum_{k=1}^{p^a-1}\frac{\alpha^{2k}}{k}\right).\end{aligned}$$

So, by the above, we have

$$
\begin{aligned}
p^{a-1}\sum_{k=1}^{p^a-1}\frac{F_{2(p^a-k)}}{k} =&\frac{\alpha^{2p^a}g(\beta^2)-\beta^{2p^a}g(\alpha^2)}{\alpha-\beta}\\
\equiv&p\frac{F_{p^a}}{10}\left(\frac{L_p-1}{p}\right)^2+F_{p^a}\frac{L_{p^a}-1}{p}\\
\equiv&\frac{p}{10}\left(\frac{p^a}{5}\right)\left(\frac{L_p-1}{p}\right)^2+\frac{F_{2p^a}-F_{p^a}}{p} \pmod{p^2}.
\end{aligned}
$$

This concludes the proof. □

Lemma 4.3. *Let $p\neq 2,5$ be a prime and let a be a positive integer. Then*

$$
\left(\frac{p^a}{5}\right)(2F_{p^a}-F_{2p^a})+\frac{(L_p-1)^2}{5}\equiv 1-2F_{p^a-(\frac{p^a}{5})} \pmod{p^3}. \tag{4.3}
$$

Proof. Note that

$$
(L_{p^a}-1)^2=p^2\left(\frac{L_{p^a}-1}{p}\right)^2\equiv p^2\left(\frac{L_p-1}{p}\right)^2=(L_p-1)^2 \pmod{p^3}
$$

since $L_{p^a}\equiv L_p \pmod{p^2}$ by [S10, (2.4)]. Also,

$$
L_{p^a}=F_{p^a}+2F_{p^a-1}=2F_{p^a+1}-F_{p^a}=2F_{p^a-(\frac{p^a}{5})}+\left(\frac{p^a}{5}\right)F_{p^a}.
$$

Thus

$$
\begin{aligned}
&1-2F_{p^a-(\frac{p^a}{5})}-\left(\frac{p^a}{5}\right)(2F_{p^a}-F_{2p^a})\\
=&1-L_{p^a}+\left(\frac{p^a}{5}\right)F_{p^a}-\left(\frac{p^a}{5}\right)(2F_{p^a}-F_{p^a}L_{p^a})\\
=&(L_{p^a}-1)\left(\left(\frac{p^a}{5}\right)F_{p^a}-1\right)
\end{aligned}
$$

and hence it suffices to show that

$$
\left(\frac{p^a}{5}\right)F_{p^a}-1\equiv\frac{L_{p^a}-1}{5} \pmod{p^2} \tag{4.4}
$$

as $L_{p^a}\equiv 1 \pmod{p}$. Since $L_{p^a}\equiv L_p \pmod{p^2}$, and

$$
F_{p^a}\equiv\left(\frac{p}{5}\right)^{a-1}F_p \pmod{p^2}
$$

by [S10, (2.5)], (4.4) is reduced to the case $a=1$. Note that

$$\left(\frac{p}{5}\right)F_p-1=L_p-2F_{p-(\frac{p}{5})}-1\equiv\frac{L_p-1}{5}\pmod{p^2}$$

since $L_p\equiv 1+\frac{5}{2}F_{p-(\frac{p}{5})}\pmod{p^2}$ by the proof of [ST, Corollary 1.3]. The proof is now complete. □

Proof of Theorem 1.3. Applying [ST, (2.4)] with $d=0$ and $n=p^a$, we get

$$\sum_{k=0}^{p^a-1}(-1)^k\binom{2k}{k}=\sum_{k=0}^{p^a-1}(-1)^k\binom{2p^a}{k}F_{2(p^a-k)}. \tag{4.5}$$

For each $k=1,\ldots,p^a-1$, clearly

$$\begin{aligned}(-1)^k\binom{2p^a}{k}=&(-1)^k\frac{2p^a}{k}\binom{2p^a-1}{k-1}=-\frac{2p^a}{k}\prod_{0<j<k}\left(1-\frac{2p^a}{j}\right)\\ \equiv&-\frac{2p^a}{k}\left(1-2p^a\sum_{0<j<k}\frac{1}{j}\right)\pmod{p^3}\end{aligned}$$

and similarly

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

hence

$$(-1)^k\binom{2p^a}{k}\equiv 4(-1)^k\binom{p^a}{k}+\frac{2p^a}{k}\pmod{p^3}.$$

So, (4.5) yields that

$$\begin{aligned}&\sum_{k=0}^{p^a-1}(-1)^k\binom{2k}{k}-F_{2p^a}\\ \equiv&4\sum_{k=1}^{p^a-1}\binom{p^a}{k}(-1)^kF_{2(p^a-k)}+2\sum_{k=1}^{p^a-1}\frac{p^a}{k}F_{2(p^a-k)}\\ =&4\sum_{k=1}^{p^a-1}\binom{p^a}{k}(-1)^{p^a-k}F_{2k}+2\sum_{k=1}^{p^a-1}\frac{p^a}{k}F_{2(p^a-k)}\pmod{p^3}.\end{aligned}$$

Let α and β be the two roots of the equation $x^2-x-1=0$. Then

$$\begin{aligned}\sum_{k=1}^{p^a-1}\binom{p^a}{k}(-1)^{p^a-k}F_{2k}=&-F_{2p^a}+\sum_{k=0}^{p^a}\binom{p^a}{k}(-1)^{p^a-k}\frac{\alpha^{2k}-\beta^{2k}}{\alpha-\beta}\\ =&\frac{(\alpha^2-1)^{p^a}-(\beta^2-1)^{p^a}}{\alpha-\beta}-F_{2p^a}=F_{p^a}-F_{2p^a}.\end{aligned}$$

Thus, by the above and Proposition 4.2 we have

$$\begin{aligned}\sum_{k=0}^{p^a-1}(-1)^k\binom{2k}{k} \equiv& F_{2p^a}+4(F_{p^a}-F_{2p^a})+2p^a\sum_{k=1}^{p^a-1}\frac{F_{2(p^a-k)}}{k}\\ \equiv& 4F_{p^a}-3F_{2p^a}+2(F_{2p^a}-F_{p^a})+\left(\frac{p^a}{5}\right)\frac{(L_p-1)^2}{5}\\ =& 2F_{p^a}-F_{2p^a}+\left(\frac{p^a}{5}\right)\frac{(L_p-1)^2}{5} \pmod{p^3}.\end{aligned}$$

Combining this with (4.3) we immediately get the desired (1.3). This completes the proof of Theorem 1.3. □

Acknowledgments. The work was supported by the National Natural Science Foundation of China (Grant Nos. 10901078 and 11171140). After we established Theorem 1.2, we got Roberto Tauraso's generous permission (on Oct. 1, 2010) to cite his conjecture (1.2) (cf. [T]). Thus we would like to express our sincere thanks to Prof. R. Tauraso. We are also grateful to the two referees for their helpful comments.

References

[CP] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective*, Second Edition, Springer, New York, 2005.

[G] H. W. Gould, *Combinatorial Identities*, Morgantown Printing and Binding Co., 1972.

[Gr] A. Granville, *The square of the Fermat quotient*, Integers **4** (2004), #A22, 3pp (electronic).

[J] S. Jakubec, *On divisibility of the class number h^+ of the real cyclotomic fields of prime degree l*, Math. Comp. **67** (1998), 369–398.

[P] PrimeGrid, *Wall-Sun-Sun Prime Search Statistics*, June 2014. http://prpnet.primegrid.com:13001.

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

[S10] Z.-W. Sun, *Binomial coefficients, Catalan numbers and Lucas quotients*, Sci. China Math. **53** (2010), 2473–2488. http://arxiv.org/abs/0909.5648.

[S11] Z.-W. Sun, *Super congruences and Euler numbers*, Sci. China Math. **54** (2011), 2509–2535.

[ST] Z.-W. Sun and R. Tauraso, *New congruences for central binomial coefficients*, Adv. in Appl. Math. **45** (2010), 125–148.

[T] R. Tauraso, *A personal communication via e-mail*, Jan. 29, 2010.

[W] H. C. Williams, *Some formulae concerning the fundamental unit of a real quadratic field*, Discrete Math. **92** (1991), 431–440.

[Wo] J. Wolstenholme, *On certain properties of primes numbers*, Quart. J. Pure Appl. Math. **5** (1862), 35–39.