A talk given at the Chinese Univ. of Hong Kong on April 7, 2000.

VARIOUS NUMBER-THEORETIC QUOTIENTS AND RELATED CONGRUENCES

Zhi-Wei Sun

Department of Mathematics
Nanjing University
Nanjing 210093
The People's Republic of China
E-mail: zwsun@nju.edu.cn

1. Lucas Quotients and Related Congruences

Let $A, B \in \mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$. The Lucas sequences $u_n = u_n(A,B)$ and $v_n = v_n(A,B)$ are defined as follows:

$$u_0 = 0,\ u_1 = 1,\quad \text{and } u_{n+1} = Au_n + Bu_{n-1} \text{ for } n = 1,2,3,\cdots,$$
$$v_0 = 2,\ v_1 = A,\quad \text{and } v_{n+1} = Av_n + Bv_{n-1} \text{ for } n = 1,2,3,\cdots.$$

The sequence $F_n = u_n(1,1)$ is called the Fibonacci sequence, its companion is the sequence $L_n = v_n(1,1)$. The sequence $P_n = u_n(2,1)$ is called the Pell sequence, its companion is the sequence $Q_n = v_n(2,1)$.

Suppose that $(A,B) = 1$ and p is a prime with $p \nmid B$. It is well known that

$$u_{p-(\frac{\Delta}{p})} \equiv 0 \pmod p \quad \text{where } \Delta = A^2 + 4B.$$

Thus we can define Lucas quotient

$$uq_p(A,B) = \frac{u_{p-(\frac{\Delta}{p})}(A,B)}{p}.$$

Let p be a prime different from 2 and 5. What can we say about the Fibonacci quotient $uq_p(1,1) = F_{p-(\frac{5}{p})}/p$? In 1982 H. C. Williams obtained the congruence:

$$\frac{F_{p-(\frac{5}{p})}}{p} \equiv \frac{2}{5}\sum_{k=1}^{[\frac{4}{5}p]} \frac{(-1)^k}{k} \pmod p.$$

In 1992 Z.-H. Sun and I [Acta Arith.] expressed the sum $\sum_{k\equiv r(\mathrm{mod}\ 10)}\binom{p}{k}$ in terms of Fibonacci numbers and Lucas numbers, as an application we determined $F_{(p\pm1)/2} \bmod p^2$. It follows that

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

In 1960 D.D. Wall asked whether $p^2\mid F_{p-(\frac{5}{p})}$ is always impossible. No counterexample has been found. In 1992 we showed that if $p^2\nmid F_{p-(\frac{5}{p})}$ then the first case of Fermat's Last Theorem is true for the exponent p. In 1997 R. Crandall, K. Dilcher and C. Pomerance [Math. Comput.] called p a *Wall-Sun-Sun prime* if $p^2\mid F_{p-(\frac{5}{p})}$.

Let p be an odd prime. Z.-H. Sun determined $\sum_{k\equiv r(\mathrm{mod}\ 8)}\binom{p}{k}$ in terms of the Pell sequence and its companion. He conjectured that

$$\sum_{k=1}^{\frac{p-1}{2}}\frac{1}{k2^k}\equiv\sum_{k=1}^{[3p/4]}\frac{(-1)^{k-1}}{k}\pmod p.$$

This is equivalent to the congruence

$$\frac{P_{p-(\frac{2}{p})}}{p}\equiv\frac{1}{2}\sum_{\frac{p}{4}<k<\frac{p}{2}}\frac{(-1)^k}{k}\pmod p.$$

I confirmed the conjecture in 1995 [Proc. Amer. Math. Soc.]. Later, in 1999 Z. Shan and Edward T.H. Wang [Proc. Amer. Math. Soc.] gave a new proof which avoids the sum $\sum_{k\equiv r(\mathrm{mod}\ 8)}\binom{p}{k}$. W. Kohnen [Monatsh. Math., 127(1999)] made a generalization by working with 2^nth roots of unity.

I have determined the sum $\sum_{k\equiv r(\mathrm{mod}\ 12)}\binom{p}{k}$ in terms of a special Lucas sequence $S_n=u_n(4,-1)$ and its companion $T_n=v_n(4,-1)$.

Theorem 1.1 [Israel J. Math., 128(2002), 135–156]**.** *Let $p\in\mathbb{Z}^+$, $2\nmid p$ and $r\in\mathbb{Z}$. Then*

$$12\sum_{\substack{0\leqslant k\leqslant p\\ 12\mid k-r}}\binom{p}{k}-2^p-1$$
$$=\begin{cases}3^{\frac{p+1}{2}}+(-1)^{\frac{r(p-r)}{2}}(\frac{2}{p})(2^{\frac{p+1}{2}}+T_{\frac{p+1}{2}}) & \text{if } r\equiv\frac{p\pm1}{2}\pmod 6,\\ -3+(-1)^{\frac{r(p-r)}{2}}(\frac{2}{p})(2^{\frac{p+1}{2}}-T_{\frac{p+1}{2}}+T_{\frac{p-1}{2}}) & \text{if } r\equiv\frac{p\pm3}{2}\pmod 6,\\ -3^{\frac{p+1}{2}}+(-1)^{\frac{r(p-r)}{2}}(\frac{2}{p})(2^{\frac{p+1}{2}}-T_{\frac{p-1}{2}}) & \text{if } r\equiv\frac{p\pm5}{2}\pmod 6.\end{cases}$$

Corollary 1.1. *Let $p > 3$ be a prime. Let $r \in \mathbb{Z}$,*

$$K_p(r,12) = \sum_{\substack{0<k<p\\ 12\mid k-rp}} \frac{1}{k} \quad \text{and} \quad \varepsilon_r = \begin{cases} 1 & \text{if } r \equiv 0,1 \pmod 6,\\ -1 & \text{if } 3 \mid r+1,\\ 0 & \text{otherwise.} \end{cases}$$

Then

$$\begin{aligned}(-1)^{r-1}K_p(r,12) \equiv & \frac{2+(-1)^{[r/2]}}{12} q_p(2) + [3 \nmid r+1](-1)^{[r/3]}\frac{q_p(3)}{8} \\ & + \varepsilon_r (-1)^{[r/2]} \left(\frac{2}{p}\right) \frac{S_{(p-(\frac{3}{p}))/2}}{2p} \pmod p\end{aligned}$$

where $[3 \nmid r+1]$ is 1 if $3 \nmid r+1$, and 0 otherwise; for $a \not\equiv 0 \pmod p$ we use $q_p(a)$ to denote the Fermat quotient $(a^{p-1}-1)/p$.

Corollary 1.2. *If p is a prime greater than 3, then*

$$q_p(2) \equiv 2(-1)^{\frac{p-1}{2}} \sum_{k=1}^{[\frac{p+1}{6}]} \frac{(-1)^k}{2k-1} \pmod p$$

and

$$\sum_{k=1}^{\frac{p-1}{2}} \frac{3^k}{k} \equiv \sum_{0<k<p/6} \frac{(-1)^k}{k} \equiv -6\left(\frac{2}{p}\right)\frac{S_{(p-(\frac{3}{p}))/2}}{p} - q_p(2) \pmod p.$$

The first congruence provides a quick way to compute $q_p(2) \bmod p$. The second one was announced by the author [Proc. Amer. Math. Soc.] in 1995.

2. Binomial Quotients and Bernoulli polynomials

Let p be a prime and $k \in \{1,\cdots,p-1\}$. It is easy to see that $\binom{p-1}{k} \equiv (-1)^k \pmod p$. Define the binomial quotient

$$bq_p(k) = \frac{(-1)^k\binom{p-1}{k}-1}{p}.$$

Clearly

$$bq_p(k) = \frac{\prod_{j=1}^{l}(1-\frac{p}{j})-1}{p} \equiv -\sum_{j=1}^{k}\frac{1}{j} \pmod p.$$

In general, it is difficult to determine $\sum_{j=1}^{k}\frac{1}{j} \bmod p$ and hence $bq_p(k) \bmod p$. However, if we choose the largest k such that $k/p \leqslant n/m$, then the problem becomes more interesting. It is easy to check the symmetry $bq_p([\frac{pn}{m}]) = bq_p([\frac{p(m-n)}{m}])$. Moreover, Granville and I [Pacific J. Math. 1996] observed the following result: If p is an odd prime, $0 \leqslant n < m$ and $p \nmid m$, then

$$bq_p\left(\left[\frac{pn}{m}\right]\right) \equiv B_{p-1}\left(\left\{\frac{pn}{m}\right\}\right) - B_{p-1} \pmod p.$$

It is well-known that $B_k(\frac{n}{m})$ $(1 \leqslant n < m)$ has simple closed form for $m = 1, 2, 3, 4, 6$. where k is an even integer. (For example, $B_k(1/6) = B_k(5/6) = (6^{1-k} - 3^{1-k} - 2^{1-k} + 1)B_k/2$.) In 1938 E. Lemma [Ann. Math.] deduced the following congruences from those close forms.

$$\begin{aligned}
&B_{p-1}\left(\frac{1}{2}\right) - B_{p-1} \equiv 2q_p(2) \pmod p;\\
&B_{p-1}\left(\frac{1}{3}\right) - B_{p-1} \equiv B_{p-1}\left(\frac{2}{3}\right) - B_{p-1} \equiv \frac{3}{2}q_p(3) \pmod p;\\
&B_{p-1}\left(\frac{1}{4}\right) - B_{p-1} \equiv B_{p-1}\left(\frac{3}{4}\right) - B_{p-1} \equiv 3q_p(2) \pmod p;\\
&B_{p-1}\left(\frac{1}{6}\right) - B_{p-1} \equiv B_{p-1}\left(\frac{5}{6}\right) - B_{p-1} \equiv \frac{3}{2}q_p(3) + 2q_p(2) \pmod p.
\end{aligned}$$

Thus, we have

$$bq_p\left(\left[\frac{p}{2}\right]\right) \equiv 2q_p(2) \pmod p,\ bq_p\left(\left[\frac{p}{4}\right]\right) = bq_p\left(\left[\frac{3p}{4}\right]\right) \equiv 3q_p(2) \pmod p,$$

$$bq_p\left(\left[\frac{p}{3}\right]\right) = bq_p\left(\left[\frac{2p}{3}\right]\right) \equiv 3q_p(2) \pmod p,$$

$$bq_p\left(\left[\frac{p}{6}\right]\right) = bq_p\left(\left[\frac{5p}{6}\right]\right) \equiv 2q_p(2) + \frac{3}{2}q_p(3) \pmod p.$$

In 1895 Morley found that if $p > 3$ then

$$(-1)^{\frac{p-1}{2}}\binom{p-1}{(p-1)/2} \equiv 4^{p-1} \pmod{p^2},\ \text{i.e. } bq_p\left(\left[\frac{p}{2}\right]\right) \equiv q_p(4) \pmod{p^2}.$$

Note the following two important things:
(i): We've evaluated $B_{p-1}(\frac{a}{m}) - B_{p-1} \pmod p$ where $\varphi(m) = 1$ or 2;
(ii): Each of the terms of the right hand side, like 2^p, 3^p, are numbers taken from a first-order linear recurrence sequence ($u_{n+1} = 2u_n$ and $u_{n+1} = 3u_n$ respectively).

In 1996 A. Granville and I [Pacific J. Math.] showed, for $m > 2$, that $B_{p-1}(\frac{a}{m}) - B_{p-1} \pmod p$ is congruent to a sum of multiples of terms, each of which are numbers taken from a kth-order linear recurrence sequence with

$$k \leq \varphi(m)/2.$$

Thus the next class of examples are those m for which $\varphi(m) = 4$, namely $m = 5, 8, 10, 12$. We showed that, for $1 \le a < m$ with $(a, m) = 1$ (there being four such integers a), we have, when odd prime p does not divide m,

$$B_{p-1}\left(\frac{a}{5}\right) - B_{p-1} \equiv \frac{5}{4}\left(\frac{ap}{5}\right)\frac{1}{p}F_{p-(\frac{5}{p})} + \frac{5}{4}q_p(5) \pmod p;$$
$$B_{p-1}\left(\frac{a}{8}\right) - B_{p-1} \equiv \left(\frac{2}{ap}\right)\frac{2}{p}P_{p-(\frac{2}{p})} + 4q_p(2) \pmod p;$$
$$B_{p-1}\left(\frac{a}{10}\right) - B_{p-1} \equiv \frac{15}{4}\left(\frac{ap}{5}\right)\frac{1}{p}F_{p-(\frac{5}{p})} + \frac{5}{4}q_p(5) + 2q_p(2) \pmod p;$$
$$B_{p-1}\left(\frac{a}{12}\right) - B_{p-1} \equiv \left(\frac{3}{a}\right)\frac{3}{p}S_{p-(\frac{3}{p})} + 3q_p(2) + \frac{3}{2}q_p(3). \pmod p$$

In general we showed that $B_{p-1}(a/m) - B_{p-1} \equiv m(U_p - 1)/(2p) \pmod p$, where U_n is a certain linear recurrence of order $[m/2]$ which depends only on a, m and the least positive residue of $p \pmod m$. This can be re-written as a sum of linear recurrence sequences of order $\le \varphi(m)/2$, and so we can recover the classical results where $\varphi(m) \le 2$ (for instance, $B_{p-1}(1/6) - B_{p-1} \equiv \frac{3}{2}q_p(3) + 2q_p(2) \pmod{p}$). Our results provided the first advance on the question of evaluating these polynomials when $\varphi(m) > 2$, a problem posed by Emma Lehmer in 1938.

A. Granville found that if an odd prime p does not divide a positive integer n then

$$\prod_{0<k<n} \binom{p-1}{[pk/n]} \equiv (-1)^{\frac{p-1}{2}(n-1)}(n^p - n + 1) \pmod{p^2}.$$

I strengthened this result as follows.

Theorem 2.1 [Acta Arith. 97(2001)]**.** *Let p be an odd prime, and n a positive integer not divisible by p. Then, for $\delta \in \{0, 1\}$ we have*

$$(-1)^{\frac{p-1}{2}[\frac{n-\delta}{2}]} \prod_{0<k\leqslant[(n-\delta)/2]} \binom{p-1}{[pk/n]}$$
$$\equiv \begin{cases} (\frac{n}{p}) + pn\mathrm{eq}_p(n) \pmod{p^2} & \text{if } 2 \nmid n, \\ (\frac{2n}{p}) + p((-1)^\delta(\frac{n}{p})2\mathrm{eq}_p(2) + (\frac{2}{p})n\mathrm{eq}_p(n)) \pmod{p^2} & \text{if } 2 \mid n, \end{cases}$$

where $\mathrm{eq}_p(a) = (a^{(p-1)/2} - (\frac{a}{p}))/p$ *for* $a \in \mathbb{Z}$.