FIVE CONGRUENCES FOR PRIMES

Zhi-Hong Sun

Dept. of Mathematics, Huaiyin Teachers College, Huaian, Jiangsu 223001, P.R. China

E-mail: hyzhsun@public.hy.js.cn

(Submitted July 2000-Final Revision March 2001)

1. INTRODUCTION

Let p be an odd prime. In 1988, using the formula for the sum

$$\sum_{k\equiv r \pmod 8} \binom{n}{k},$$

the author proved that (cf. [7], Theorem 2.6)

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

and

$$\sum_{1\le k<\frac{p}{2}} \frac{1}{k\cdot 2^k} \equiv -4 \sum_{\frac{1+(-1)^{\frac{p-1}{2}}}{2}\le k<\frac{p}{8}} \frac{1}{4k-(-1)^{\frac{p-1}{2}}} \pmod p.$$

In 1995, using a similar method, Zhi-Wei Sun [9] proved the author's conjecture,

$$\sum_{1\le k<\frac{p}{2}} \frac{1}{k\cdot 2^k} \equiv \sum_{1\le k<\frac{3p}{4}} \frac{(-1)^{k-1}}{k} \pmod p.$$

Later, Zun Shan and Edward T. H. Wang [5] gave a simple proof of the above congruence. In [9] and [10], Zhi-Wei Sun also pointed out another congruence,

$$\sum_{1\le k<\frac{p}{2}} \frac{3^k}{k} \equiv \sum_{1\le k<\frac{p}{6}} \frac{(-1)^k}{k} \pmod p.$$

In this paper, by using the formulas for Fibonacci quotient and Pell quotient, we obtain the following five congruences:

$$\sum_{1\le k<\frac{p}{2}} \frac{2^k}{k} \equiv 2 \sum_{\frac{p}{4}<k<\frac{p}{2}} \frac{(-1)^{k-1}}{k} \pmod p, \tag{1.1}$$

$$\sum_{1\le k<\frac{p}{2}} \frac{5^k}{k} \equiv 2 \sum_{\frac{p}{5}<k<\frac{p}{2}} \frac{(-1)^{k-1}}{k} \pmod p, \tag{1.2}$$

$$\sum_{1\le k<\frac{p}{2}} \frac{2^k}{k} \equiv -\sum_{\frac{p}{8}<k<\frac{3p}{8}} \frac{1}{k} \pmod p, \tag{1.3}$$

$$\sum_{1\le k<\frac{p}{2}} \frac{1}{k\cdot 2^k} \equiv -\sum_{\frac{p}{4}<k<\frac{3p}{8}} \frac{1}{k} \pmod p, \tag{1.4}$$

$$\sum_{1\le k<\frac{p}{2}} \frac{3^k}{k} \equiv -\sum_{\frac{p}{12}<k<\frac{p}{6}} \frac{1}{k} \pmod p, \tag{1.5}$$

where $p>5$ is a prime.

2. BASIC LEMMAS

The Lucas sequences $\{u_n(a,b)\}$ and $\{v_n(a,b)\}$ are defined as follows:

$$u_0(a,b)=0,\ u_1(a,b)=1,\ u_{n+1}(a,b)=bu_n(a,b)-au_{n-1}(a,b)\ \ (n\ge 1),$$
$$v_0(a,b)=2,\ v_1(a,b)=b,\ v_{n+1}(a,b)=bv_n(a,b)-av_{n-1}(a,b)\ \ (n\ge 1).$$

It is well known that

$$u_n(a,b)=\frac{1}{\sqrt{b^2-4a}}\left\{\left(\frac{b+\sqrt{b^2-4a}}{2}\right)^n-\left(\frac{b-\sqrt{b^2-4a}}{2}\right)^n\right\}\ \ (b^2-4a\neq 0)$$

and

$$v_n(a,b)=\left(\frac{b+\sqrt{b^2-4a}}{2}\right)^n+\left(\frac{b-\sqrt{b^2-4a}}{2}\right)^n.$$

Let p be an odd prime, and let m be an integer with $m\not\equiv 0 \pmod p$. It is evident that

$$2\sum_{\substack{k=1\\ 2\mid k}}^{p-1}\binom{p}{k}(\sqrt{m})^k=(1+\sqrt{m})^p-(1-\sqrt{m})^p-2(\sqrt{m})^p$$

and

$$2\sum_{\substack{k=1\\ 2\nmid k}}^{p-1}\binom{p}{k}(\sqrt{m})^k=(1+\sqrt{m})^p+(1-\sqrt{m})^p-2.$$

Since

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

by the above one can easily prove

Lemma 1 ([7], Lemma 2.4): Suppose that p is an odd prime and that m is an integer such that $p\nmid m$. Then

(a) $$\sum_{k=1}^{(p-1)/2}\frac{1}{k\cdot m^k}\equiv\frac{m^{p-1}-1}{p}-2\cdot\frac{\left(\frac{m}{p}\right)u_p(1-m,2)-1}{p} \pmod p,$$

(b) $$\sum_{k=1}^{(p-1)/2}\frac{m^k}{k}\equiv\frac{2-v_p(1-m,2)}{p} \pmod p,$$

where $\left(\frac{m}{p}\right)$ is the Legendre symbol.

For any odd prime p and integer m, set $q_p(m)=\frac{m^{p-1}-1}{p}$. Using Lemma 1, we can prove

Proposition 1: Let m be an integer and let p be an odd prime such that $p\nmid m(m-1)$. Then

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

Proof: Set $u_n = u_n(1-m,2)$ and $v_n = v_n(1-m,2)$. From [1], [4], and Lemma 1.7 of [6], we know that

$$v_n^2 - 4mu_n^2 = 4(1-m)^n,\ v_n = 2u_{n+1} - 2u_n,\ u_n = \frac{1}{2m}(v_{n+1} - v_n)$$

and

$$u_{p-(\frac{m}{p})} \equiv u_p - \left(\frac{m}{p}\right) \equiv 0 \pmod p.$$

Thus,

$$v^2_{p-(\frac{m}{p})} \equiv 4(1-m)^{p-(\frac{m}{p})} \pmod{p^2},$$

and hence,

$$v_{p-(\frac{m}{p})} \equiv \pm 2\left(\frac{1-m}{p}\right)(1-m)^{(p-(\frac{m}{p}))/2} \pmod{p^2}.$$

If $(\frac{m}{p}) = 1$, then $v_{p-1} = 2u_p - 2u_{p-1} \equiv 2 \pmod p$. Hence, by the above, we get

$$v_{p-1} \equiv 2(1-m)^{(p-1)/2}\left(\frac{1-m}{p}\right) \equiv 2 + q_p(m-1)p \pmod{p^2}. \tag{2.1}$$

Now, applying Lemma 1 we find

$$\begin{aligned}\frac{u_{p-1}}{p} &= \frac{1}{2m}\cdot\frac{v_p - v_{p-1}}{p} = \frac{1}{2m}\left(\frac{v_p - 2}{p} - \frac{v_{p-1} - 2}{p}\right)\\ &\equiv \frac{1}{2m}\left(-\sum_{k=1}^{(p-1)/2}\frac{m^k}{k} - q_p(m-1)\right) \pmod p\end{aligned}$$

and

$$\begin{aligned}\frac{u_{p-1}}{p} &= \frac{2u_p - v_{p-1}}{2p} = \frac{u_p - 1}{p} + \frac{1}{2}\cdot\frac{2 - v_{p-1}}{p}\\ &\equiv \frac{1}{2}\left(q_p(m) - \sum_{k=1}^{(p-1)/2}\frac{1}{k\cdot m^k} - q_p(m-1)\right) \pmod p.\end{aligned}$$

This proves the result in the case $(\frac{m}{p}) = 1$.

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

$$v_{p+1} = 2u_{p+1} - 2(1-m)u_p \equiv 2(1-m) \pmod p.$$

So

$$v_{p+1} \equiv 2(1-m)\left(\frac{1-m}{p}\right)(1-m)^{(p-1)/2} \equiv (1-m)(2 + q_p(m-1)p) \pmod{p^2}. \tag{2.2}$$

Note that

$$u_{p+1} = \frac{1}{2m}(v_{p+1} + (m-1)v_p) = \frac{1}{2}v_{p+1} + (1-m)u_p.$$

Applying (2.2) and Lemma 1, one can easily deduce the desired result. Therefore, the proof is complete.

Corollary 1: Let p be an odd prime and let $\{P_n\}$ denote the Pell sequence given by $P_0 = 0,\ P_1 = 1$, and $P_{n+1} = 2P_n + P_{n-1}\ (n \geq 1)$. Then *(a)* $\sum_{k=1}^{(p-1)/2} \frac{2^k}{k} \equiv -4\frac{P_{p-(\frac{2}{p})}}{p} \pmod{p}$.

(b) $\sum_{k=1}^{(p-1)/2} \frac{1}{k\cdot 2^k} \equiv -2\frac{P_{p-(\frac{2}{p})}}{p} + q_p(2) \pmod{p}$.

Proof: Taking $m = 2$ in Proposition 1 gives the result.

Corollary 2: Let $p > 3$ be a prime, $S_0 = 0$, $S_1 = 1$, and $S_{n+1} = 4S_n - S_{n-1}$ $(n \geq 1)$. Then

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

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

Proof: Suppose a and b are integers. From [4] we know that $u_{2n}(a,b) = u_n(a,b)v_n(a,b)$ and

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

Thus,

$$v_{p-(\frac{3}{p})}(-2,2) = \begin{cases} 2u_p(-2,2) - 2u_{p-1}(-2,2) \equiv 2 \pmod{p} & \text{if } \left(\frac{3}{p}\right) = 1, \\ 2u_{p+1}(-2,2) + 4u_p(-2,2) \equiv -4 \pmod{p} & \text{if } \left(\frac{3}{p}\right) = -1, \end{cases}$$
$$\equiv 3\left(\frac{3}{p}\right) - 1 \pmod{p}.$$

Observing that $S_n = u_n(1,4) = 2^{-n}u_{2n}(-2,2)$, we get

$$\begin{aligned} S_{p-(\frac{3}{p})}/p &= 2^{(\frac{3}{p})-p} v_{p-(\frac{3}{p})}(-2,2)u_{p-(\frac{3}{p})}(-2,2)/p \\ &\equiv 2^{(\frac{3}{p})-1}\left(3\left(\frac{3}{p}\right)-1\right)u_{p-(\frac{3}{p})}(-2,2)/p \\ &= \frac{1}{2}\left(1+3\left(\frac{3}{p}\right)\right)u_{p-(\frac{3}{p})}(-2,2)/p \pmod{p}. \end{aligned}$$

This, together with the case $m = 3$ of Proposition 1 gives the result.

Remark 1: The sequence $\{S_n\}$ was first introduced by my brother Zhi-Wei Sun, who gave the formula for the sum $\sum_{k\equiv r \pmod{12}} \binom{n}{k}$ in terms of $\{S_n\}$ (cf. [10]).

Corollary 3: Let $p > 5$ be a prime and let $\{F_n\}$ denote the Fibonacci sequence. Then

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

(b) $\sum_{k=1}^{(p-1)/2} \frac{1}{k\cdot 5^k} \equiv -\frac{F_{p-(\frac{5}{p})}}{p} + q_p(5) - 2q_p(2) \pmod{p}$.

Proof: It is easily seen that $u_n(-4,2)=2^{n-1}F_n$. So we have

$$\frac{F_{p-(\frac{5}{p})}}{p}=2^{1-p+(\frac{5}{p})}\frac{u_{p-(\frac{5}{p})}(-4,2)}{p}\equiv 2^{(\frac{5}{p})}\frac{u_{p-(\frac{5}{p})}(-4,2)}{p} \pmod p.$$

Combining this with the case $m=5$ of Proposition 1 yields the result.

Let $\{B_n\}$ and $\{B_n(x)\}$ be the Bernoulli numbers and Bernoulli polynomials given by

$$B_0=1,\ \sum_{k=0}^{n-1}\binom{n}{k}B_k=0\ (n\ge 2)$$

and

$$B_n(x)=\sum_{k=0}^{n}\binom{n}{k}B_kx^{n-k}.$$

It is well known that (cf. [3])

$$\sum_{x=0}^{n-1}x^m=\frac{1}{m+1}(B_{m+1}(n)-B_{m+1})$$

Lemma 2: Let p be an odd prime and let m be a positive integer such that $p\nmid m$. If $s\in\{1,2,\dots,m-1\}$, then

$$\sum_{1\le k\le[\frac{sp}{m}]}\frac{1}{k}\equiv-\left(B_{p-1}\left(\left\{\frac{sp}{m}\right\}\right)-B_{p-1}\right)\pmod p,$$

where $[x]$ is the greatest integer not exceeding x and $\{x\}=x-[x]$.

Proof: Clearly,

$$\sum_{1\le k\le[\frac{sp}{m}]}\frac{1}{k}\equiv\sum_{1\le k\le[\frac{sp}{m}]}k^{p-2}=\frac{1}{p-1}\left(B_{p-1}\left(\left[\frac{sp}{m}\right]+1\right)-B_{p-1}\right)$$

$$=\frac{1}{p-1}\left(B_{p-1}\left(\frac{sp}{m}+1-\left\{\frac{sp}{m}\right\}\right)-B_{p-1}\right)\pmod p.$$

For any rational p-integers x and y, it is evident that (cf. [3])

$$pB_k(x)=\sum_{r=0}^{k}\binom{k}{r}pB_rx^{k-r}\equiv 0\pmod p\ \text{ for } k=0,1,\dots,p-2,$$

and so

$$B_{p-1}(x+py)-B_{p-1}(x)=\sum_{k=0}^{p-2}\binom{p-1}{k}B_k(x)(py)^{p-1-k}\equiv 0\pmod p.$$

Hence, by the above and the relation $B_n(1-x)=(-1)^nB_n(x)$ (cf. [3]), we get

$$\sum_{1\le k\le[\frac{sp}{m}]}\frac{1}{k}\equiv\frac{1}{p-1}\left(B_{p-1}\left(1-\left\{\frac{sp}{m}\right\}\right)-B_{p-1}\right)$$

$$\equiv-\left(B_{p-1}\left(\left\{\frac{sp}{m}\right\}\right)-B_{p-1}\right)\pmod p.$$

This proves the lemma.

3. PROOF OF (1.1)-(1.5)

In [8], using the formula for the sum $\sum_{k\equiv r \pmod 8}\binom{n}{k}$, the author proved that

$$\frac{P_{p-(\frac{2}{p})}}{p} \equiv \frac{1}{2}\sum_{\frac{p}{4}<k<\frac{p}{2}} \frac{(-1)^k}{k} \pmod p \tag{3.1}$$

and

$$\frac{P_{p-(\frac{2}{p})}}{p} \equiv \frac{1}{4}\sum_{\frac{p}{8}<k<\frac{3p}{8}} \frac{1}{k} \pmod p. \tag{3.2}$$

Here, (3.1) was found by Z. W. Sun [10], and (3.2) was also given by Williams [12].

Now, putting (3.1) and (3.2) together with Corollary 1(a) proves (1.1) and (1.3).

To prove (1.2), we note that Williams (see [11]) has shown that

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

Since Eisenstein, it is well known that (cf. [6])

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

Thus, by Williams' result,

$$\frac{F_{p-(\frac{5}{p})}}{p} \equiv -\frac{2}{5}\left(2q_p(2) - \sum_{k=1}^{[p/5]} \frac{(-1)^{k-1}}{k}\right) \equiv -\frac{2}{5}\left(q_p(2) + \sum_{\frac{p}{5}<k<\frac{p}{2}} \frac{(-1)^{k-1}}{k}\right) \pmod p.$$

Hence, by Corollary 3(a), we have

$$\sum_{1\le k<\frac{p}{2}} \frac{5^k}{k} \equiv -5\frac{F_{p-(\frac{5}{p})}}{p} - 2q_p(2) \equiv 2\sum_{\frac{p}{5}<k<\frac{p}{2}} \frac{(-1)^{k-1}}{k} \pmod p.$$

This proves (1.2).

Now, consider (1.4). From [2], we know that

$$B_{p-1}\left(\left\{\frac{p}{4}\right\}\right) - B_{p-1} \equiv 3q_p(2) \pmod p$$

and

$$B_{p-1}\left(\left\{\frac{3p}{8}\right\}\right) - B_{p-1} \equiv -2\frac{P_{p-(\frac{2}{p})}}{p} + 4q_p(2) \pmod p.$$

Thus, by using Lemma 2, we obtain

$$-\sum_{\frac{p}{4}<k<\frac{3p}{8}} \frac{1}{k} = \sum_{1\le k<\frac{p}{4}} \frac{1}{k} - \sum_{1\le k<\frac{3p}{8}} \frac{1}{k} \equiv -\left(B_{p-1}\left(\left\{\frac{p}{4}\right\}\right) - B_{p-1}\right) + B_{p-1}\left(\left\{\frac{3p}{8}\right\}\right) - B_{p-1}$$

$$\equiv -3q_p(2) + 4q_p(2) - 2\frac{P_{p-(\frac{2}{p})}}{p} \pmod p.$$

This, together with Corollary 1(b) proves (1.4).

Finally, we consider (1.5). By [2],

$$B_{p-1}\left(\left\{\frac{p}{6}\right\}\right)-B_{p-1}\equiv 2q_p(2)+\frac{3}{2}q_p(3) \pmod p$$

and

$$B_{p-1}\left(\left\{\frac{p}{12}\right\}\right)-B_{p-1}\equiv 3\left(\frac{3}{p}\right)\frac{S_{p-(\frac{3}{p})}}{p}+3q_p(2)+\frac{3}{2}q_p(3) \pmod p.$$

Thus, by Lemma 2 and Corollary 2(a),

$$-\sum_{\frac{p}{12}<k<\frac{p}{6}}\frac{1}{k}\equiv\left(B_{p-1}\left(\left\{\frac{p}{6}\right\}\right)-B_{p-1}\right)-\left(B_{p-1}\left(\left\{\frac{p}{12}\right\}\right)-B_{p-1}\right)$$

$$\equiv 2q_p(2)+\frac{3}{2}q_p(3)-3q_p(2)-\frac{3}{2}q_p(3)-3\left(\frac{3}{p}\right)\frac{S_{p-(\frac{3}{p})}}{p}\equiv\sum_{1\le k<\frac{p}{2}}\frac{3^k}{k} \pmod p.$$

This proves (1.5) and the proof is complete.

Remark 2: The congruences (1.1)-(1.3) can also be proved by using the method in the proof of (1.4) or (1.5).

REFERENCES

1. L. E. Dickson. *History of the Theory of Numbers*, Vol. I, pp. 393-407. New York: Chelsea, 1952.
2. A. Granville & Zhi-Wei Sun. "Values of Bernoulli Polynomials." *Pacific J. Math.* **172** (1996):117-37.
3. K. Ireland & M. Rosen. *A Classical Introduction to Modern Number Theory*, pp. 228-48. New York: Springer, 1982.
4. P. Ribenboim. *The Book of Prime Number Records*, 2nd. ed., pp. 44-50. Berlin: Springer, 1989.
5. Z. Shan & E. T. H. Wang. "A Simple Proof of a Curious Congruence by Sun." *Proc. Amer. Math. Soc.* **127.5** (1999):1289-91.
6. Z. H. Sun. "Combinatorial Sum $\sum_{k=0;\,k\equiv r \pmod m}^{n}\binom{n}{k}$ and Its Applications in Number Theory I." *J. Nanjing Univ. Math. Biquarterly* **9** (1992):227-40. MR94a:11026.
7. Z. H. Sun. "Combinatorial Sum $\sum_{k=0;\,k\equiv r \pmod m}^{n}\binom{n}{k}$ and Its Applications in Number Theory II." *J. Nanjing Univ. Math. Biquarterly* **10** (1993):105-18. MR94j:11021.
8. Z. H. Sun. "Combinatorial Sum $\sum_{k\equiv r \pmod m}^{n}\binom{n}{k}$ and Its Applications in Number Theory III." *J. Nanjing Univ. Math. Biquarterly* **12** (1995):90-102. MR96g:11017.
9. Z. W. Sun. "A Congruence for Primes." *Proc. Amer. Math. Soc.* **123** (1995):1341-46.
10. Z. W. Sun. "On the sum $\sum_{k\equiv r \pmod m}^{n}\binom{n}{k}$ and Related Congruences." *Israel J. Math.* **128** (2002):135-56.
11. H. C. Williams. "A Note on the Fibonacci Quotient $F_{p-\varepsilon}/p$." *Canad. Math. Bull.* **25** (1982): 366-70.
12. H. C. Williams. "Some Formulas Concerning the Fundamental Unit of a Real Quadratic Field." *Discrete Math.* **92** (1991):431-40.

AMS Classification Numbers: 11A07, 11B39, 11B68

❖❖❖