南京大学学报数学半年刊
第12卷 第1期 JOURNAL OF NANJING UNIVERSITY Vol. 12, No. 1
1995年5月 MATHEMATICAL BIQUARTERLY May, 1995

组合和 $\sum_{k\equiv r(\mathrm{mod}\ m)}\binom{n}{k}$ 及其数论应用(Ⅲ)

孙智宏
(淮阴师范专科学校,223001)

摘 要 设 p 为大于 5 的素数,本文利用组合和给出 $F_{p-(\frac{5}{p})}/p$、$u_{p-(\frac{2}{p})}/p$ 与 $F(p)/p \bmod p$ 的基本结果. 这里 $\{F_n\}$、$\{u_n\}$、$\{F(n)\}$ 是如下定义的递推序列:

$F_0=0,\ F_1=1,\ F_{n+1}=F_n+F_{n-1}$

$u_0=0,\ u_1=1,\ u_{n+1}=2u_n+u_{n-1} \qquad (n=1,2,3,\cdots)$

$F(0)=1,\ F(1)=0,\ F(2)=2,\ F(n+2)=3F(n)-F(n-1).$

作为组合和理论的另一应用,我们还对 $4k+1$ 形素数 p 决定出 $5^{\frac{p-1}{4}} \bmod p$.

关键词 数论商,组合和,Lucas 序列.
分类号 O156.1

3.1 引言与基本引理

在[1]、[2]、[3]中我们讨论了如下的组合和

$$T^n_{r(m)}=\sum_{k\equiv r(\mathrm{mod}\ m)}\binom{n}{k}.$$

特别地,我们求出了 $m=3,4,5,6,8,10$ 时 $\Delta_m(k,n)=mT^n_{[\frac{n}{2}]+k(m)}-2^n$ 的明确表达式. 当 $m=12$ 时 $\Delta_m(k,n)$ 的公式已由孙智伟获得.

设 $\{u_n\}$、$\{F(n)\}$、$\{F_n\}$ 分别表示如下的递推序列:

$u_0=0,\ u_1=1,\ u_{n+1}=2u_n+u_{n-1},$

$F(0)=1,\ F(1)=0,\ F(2)=2,\ F(n+2)=3F(n)-F(n-1),$

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

则由[2]、[3]已知它们分别与 $m=8,9,10$ 时 $\Delta_m(k,n)$ 的公式相关联,并且当 p 为奇素数时

$$u_{p-(\frac{2}{p})}\equiv 0\ (\mathrm{mod}\ p),\ F(p)\equiv 0\ (\mathrm{mod}\ p)\ (p\neq 3),\ F_{p-(\frac{5}{p})}\equiv 0\ (\mathrm{mod}\ p)\ (p\neq 5).$$

* 收稿日期:1993-12-01.

这里$\left(\frac{d}{p}\right)$为 *Legendre* 符号．

在[2]、[3]中我们曾得到

$$u_{p-(\frac{2}{p})}/p\equiv(-1)^{\frac{p-1}{2}}\sum_{k=1}^{[\frac{p+1}{4}]}\frac{(-1)^k}{2k-1}\pmod p,$$

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

最近孙智伟和 *A. Granville* 在[4]中揭示了这两个 *Lucas* 商同 *Bernoulli* 多项式的联系，这给作者以极大的启发．作者特此致谢并向他们深表敬意．

本文是[1]、[2]、[3]的续篇，意在通过组合和导出$\frac{u_{p-(\frac{2}{p})}}{p}$、$\frac{F_{p-(\frac{5}{p})}}{p}$ *mod* p 的其它种种表达式，同时证明 F(p)/p *mod* p 的一个定理．作为组合和理论的重要应用，我们还将给出 p 为 4k+1 形素数时 $5^{\frac{p-1}{4}}$ *mod* p 的基本结果．

除了上面用到的记号，我们再作如下约定：$x\equiv r(m)$为$x\equiv r(\mathrm{mod}\ m)$的缩写，$q_p(a)=\frac{a^{p-1}-1}{p}$，[x]表示取整函数，$\{x\}=x-[x]$为 x 的小数部分，$\left(\frac{d}{m}\right)$为 d 对正奇数 m 的 *Jacobi* 符号．

在本文中，下面的同余式及其推论具有基本的重要性．

引理 3.1 设 p,m,k,s 为自然数，则

$$\sum_{\substack{a=0\\a\equiv sp(m)}}^{p-1}a^k\equiv(-m)^k\sum_{\frac{(s-1)p}{m}<a\leqslant\frac{sp}{m}}a^k\pmod p.$$

证 令 $a=sp-rm$，则由 $0\leqslant a<p$ 得$\frac{(s-1)p}{m}<r\leqslant\frac{sp}{m}$. 由此

$$\sum_{\substack{a=0\\a\equiv sp(m)}}^{p-1}a^k\equiv\sum_{\frac{(s-1)p}{m}<r\leqslant\frac{sp}{m}}(sp-rm)^k\equiv(-m)^k\sum_{\frac{(s-1)p}{m}<r\leqslant\frac{sp}{m}}r^k\pmod p.$$

推论 3.1 设 p 为奇素数，m、s∈Z^+，$p\nmid m$，则

$$m\sum_{\substack{k=1\\k\equiv sp(m)}}^{p-1}\frac{1}{k}\equiv-\sum_{\frac{(s-1)p}{m}<k<\frac{sp}{m}}\frac{1}{k}\pmod p.$$

证 在引理 3.1 中取 $k=p-2$ 利用 Fermat 小定理即知

$$\sum_{\substack{a=1\\a\equiv sp(m)}}^{p-1}\frac{1}{a}\equiv\sum_{\substack{a=0\\a\equiv sp(m)}}^{p-1}a^{p-2}\equiv(-m)^{p-2}\sum_{\frac{(s-1)p}{m}<a\leqslant\frac{sp}{m}}a^{p-2}\equiv-\frac{1}{m}\sum_{\frac{(s-1)p}{m}<a<\frac{sp}{m}}\frac{1}{a}\pmod p.$$

推论 3.2 设 p 为奇素数，$m\in Z^+$，$p\nmid m$，则

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

证 注意到

$$\sum_{k=1}^{[\frac{2p}{m}]}\frac{(-1)^k}{k}+\sum_{k=1}^{[\frac{2p}{m}]}\frac{1}{k}=\sum_{\substack{k=1\\2\mid k}}^{[\frac{2p}{m}]}\frac{2}{k}=\sum_{s=1}^{[\frac{p}{m}]}\frac{1}{s}$$

应用推论 3.1 即得

$$\sum_{k=1}^{\left[\frac{2p}{m}\right]} \frac{(-1)^k}{k} = -\sum_{\frac{p}{m}<k<\frac{2p}{m}} \frac{1}{k} \equiv m \sum_{\substack{k=1 \\ k\equiv 2p(m)}}^{p-1} \frac{1}{k} \pmod p.$$

推论 3.3 设 p 为奇素数，$k,m,s\in Z^{+}$，$p\nmid m$，$2\nmid m$，则

$$\sum_{\frac{(s-1)p}{m}<k<\frac{sp}{m}} \frac{(-1)^k}{k} \equiv (-1)^s m \sum_{\substack{k=1 \\ k\equiv sp(m)}}^{p-1} \frac{(-1)^{k-1}}{k} \pmod p.$$

证 因

$$\sum_{\frac{(s-1)p}{m}<k<\frac{sp}{m}} \frac{(-1)^k}{k} + \sum_{\frac{(s-1)p}{m}<k<\frac{sp}{m}} \frac{1}{k} = \sum_{\substack{\frac{(s-1)p}{m}<k<\frac{sp}{m} \\ 2\mid k}} \frac{2}{k} = \sum_{\frac{(s-1)p}{2m}<k<\frac{sp}{2m}} \frac{1}{k},$$

故由推论 3.1 有

$$\sum_{\frac{(s-1)p}{m}<k<\frac{sp}{m}} \frac{(-1)^k}{k} \equiv -2m \sum_{\substack{k=1 \\ k\equiv sp(2m)}}^{p-1} \frac{1}{k} + m \sum_{\substack{k=1 \\ k\equiv sp(m)}}^{p-1} \frac{(-1)^k}{k}$$

$$= m\left(\sum_{\substack{k=1 \\ k\equiv sp+m(2m)}}^{p-1} \frac{1}{k} - \sum_{\substack{k=1 \\ k\equiv sp(2m)}}^{p-1} \frac{1}{k}\right) = (-1)^s m \sum_{\substack{k=1 \\ k\equiv sp(m)}}^{p-1} \frac{(-1)^{k-1}}{k} \pmod p.$$

3.2 Lucas 商 $F_{p-\left(\frac{5}{p}\right)}/p$ 与 $u_{p-\left(\frac{2}{p}\right)}/p$

记 $K_m(s,p) = \sum\limits_{\substack{k=1 \\ k\equiv sp(m)}}^{p-1} \frac{1}{k}$，本节由 $\Delta_8(s,p)$和 $\Delta_{10}(s,p)$的计算公式得出 $K_8(s,p)$、$K_{10}(s,p)$ 模 p 的同余结果，进而获得 $u_{p-\left(\frac{2}{p}\right)}/p$ 和 $F_{p-\left(\frac{5}{p}\right)}/p$ 的多种表达式．

引理 3.2 设 p 为奇素数，$p\nmid m$，$s+t\equiv 1 \pmod m$，则

$$K_m(s,p) \equiv -K_m(t,p) \pmod p.$$

证

$$K_m(s,p) = \sum_{\substack{k=1 \\ p-k\equiv tp(m)}}^{p-1} \frac{1}{k} = \sum_{\substack{r=1 \\ r\equiv tp(m)}}^{p-1} \frac{1}{p-r} \equiv -K_m(t,p) \pmod p.$$

定理 3.1 设 $p\neq 2, 5$ 为素数，$q_p(a)=\frac{a^{p-1}-1}{p}$，则

(i) $10K_{10}(1,p)\equiv -10K_{10}(0,p)\equiv 2q_p(2)+\frac{5}{4}q_p(5)+\frac{15}{4}\cdot\frac{F_{p-\left(\frac{5}{p}\right)}}{p} \pmod p$,

(ii) $10K_{10}(2,p)\equiv -10K_{10}(9,p)\equiv -2q_p(2)-\frac{5}{2}\frac{F_{p-\left(\frac{5}{p}\right)}}{p} \pmod p$,

(iii) $10K_{10}(3,p)\equiv -10K_{10}(8,p)\equiv 2q_p(2)-5\,\frac{F_{p-\left(\frac{5}{p}\right)}}{p} \pmod p$,

(iv) $10K_{10}(4,p)\equiv -10K_{10}(7,p)\equiv -2q_p(2)+\frac{5}{2}\frac{F_{p-\left(\frac{5}{p}\right)}}{p} \pmod p$,

(v) $10K_{10}(5,p)\equiv -10K_{10}(6,p)\equiv 2q_p(2)-\frac{5}{4}q_p(5)+\frac{5}{4}\cdot\frac{F_{p-\left(\frac{5}{p}\right)}}{p} \pmod p$.

证　由[3]推论2(i)和推论3知

$$K_5(2,p)\equiv-\frac{1}{2}\frac{F_{p-(\frac{5}{p})}}{p}\pmod p,$$

$$K_5(0,p)\equiv-\frac{1}{4}q_p(5)-\frac{1}{4}\frac{F_{p-(\frac{5}{p})}}{p}\pmod p.$$

故

$$K_{10}(0,p)+K_{10}(5,p)=K_5(0,p)\equiv-\frac{1}{4}q_p(5)-\frac{1}{4}\frac{F_{p-(\frac{5}{p})}}{p}\pmod p,$$

$$K_{10}(2,p)+K_{10}(7,p)=K_5(2,p)\equiv-\frac{1}{2}\frac{F_{p-(\frac{5}{p})}}{p}\pmod p.$$

又由推论3.1和引理3.2知

$$-K_{10}(0,p)+K_{10}(2,p)=K_{10}(1,p)+K_{10}(2,p)\equiv-\frac{1}{10}\sum_{0<k<\frac{p}{5}}\frac{1}{k}$$

$$=-\frac{1}{2}K_5(0,p)\equiv\frac{1}{8}q_p(5)+\frac{1}{8}\frac{F_{p-(\frac{5}{p})}}{p}\pmod p,$$

故我们仅需再确定 $K_{10}(0,p)$ 和 $K_{10}(3,p) \bmod p$.

根据[1]定理1.7我们有

$$10K_{10}(0,p)=\sum_{k=1}^{[\frac{p}{10}]}\frac{1}{k}=\sum_{k=1}^{[\frac{p}{5}]}\frac{1}{k}+\sum_{k=1}^{[\frac{p}{5}]}\frac{(-1)^k}{k}=5K_5(0,p)-\sum_{k=1}^{[\frac{p}{5}]}\frac{(-1)^{k-1}}{k}$$

$$\equiv-\frac{5}{4}q_p(5)-\frac{5}{4}\frac{F_{p-(\frac{5}{p})}}{p}-2q_p(2)-\frac{5}{2}\frac{F_{p-(\frac{5}{p})}}{p}$$

$$\equiv-\left(2q_p(2)+\frac{5}{4}q_p(5)+\frac{15}{4}\frac{F_{p-(\frac{5}{p})}}{p}\right)\pmod p$$

和

$$10K_{10}(3,p)\equiv-10K_{10}(8,p)\equiv5(K_{10}(3,p)-K_{10}(8,p))=5\sum_{\substack{k=1\\k\equiv3p(5)}}^{p-1}\frac{(-1)^{k-1}}{k}$$

$$=5\sum_{0<k<\frac{p}{2}}\left(\frac{(-1)^{k-1}}{k}+\frac{(-1)^{p-k-1}}{p-k}\right)$$

$$\equiv10\sum_{\substack{0<k<\frac{p}{2}\\k\equiv3p(5)}}\frac{(-1)^{k-1}}{k}\equiv2q_p(2)-5\frac{F_{p-(\frac{5}{p})}}{p}\pmod p.$$

由此定理立即得证.

定理3.2　设 $p\neq2,5$ 为素数，则

(1)（孙智宏、孙智伟[3]）　$F_{p-(\frac{5}{p})}/p\equiv-2\sum_{\substack{k=1\\k\equiv2p(5)}}^{p-1}\frac{1}{k}\pmod p$;

(2) $F_{p-(\frac{5}{p})}/p \equiv \frac{2}{5}\sum_{\frac{p}{5}<k<\frac{2p}{5}} \frac{1}{k} \pmod p$;

(3) $F_{p-(\frac{5}{p})}/p \equiv \frac{2}{5}\sum_{1\leq k<\frac{2p}{5}} \frac{(-1)^{k-1}}{k} \pmod p$;

(4) (H. C. Williams[5]) $F_{p-(\frac{5}{p})}/p \equiv -\frac{2}{5}\sum_{1\leq k<\frac{4p}{5}} \frac{(-1)^{k-1}}{k} \pmod p$;

(5) $F_{p-(\frac{5}{p})}/p \equiv \frac{2}{5}\sum_{\frac{p}{5}<k<\frac{p}{3}} \frac{(-1)^{k}}{k} \pmod p \ (p\neq 3)$;

(6) $F_{p-(\frac{5}{p})}/p \equiv 6\Bigg(\sum_{\substack{k=1\\ k\equiv 4p(15)}}^{p-1} \frac{(-1)^{k-1}}{k} - \sum_{\substack{k=1\\ k\equiv 5p(15)}}^{p-1} \frac{(-1)^{k-1}}{k}\Bigg) \pmod p \ (p\neq 3)$;

(7) $F_{p-(\frac{5}{p})}/p \equiv -\frac{4}{3}\sum_{\substack{k=1\\ k\equiv 2p,3p(10)}}^{p-1} \frac{1}{k} \equiv \frac{2}{15}\sum_{\frac{p}{10}<k<\frac{3p}{10}} \frac{1}{k} \pmod p \ (p\neq 3)$;

(8) $F_{p-(\frac{5}{p})}/p \equiv \frac{4}{5}\,\frac{(-1)^{[\frac{p}{5}]}\binom{p-1}{[\frac{p}{5}]}-1}{p} - q_p(5) \pmod p$.

证 关于(1)和(4)参见[3]、[5]. 由推论 3.1 和推论 3.2 知

$$5\sum_{\substack{k=1\\ k\equiv 2p(5)}}^{p-1} \frac{1}{k} \equiv -\sum_{\frac{p}{5}<k<\frac{2p}{5}} \frac{1}{k} \equiv \sum_{k=1}^{[\frac{2p}{5}]} \frac{(-1)^k}{k} \quad (mod\ p).$$

故立得(2)、(3).

根据[1]推论 1.4 知 $p>3$ 时 $\sum_{1\leq k<\frac{2p}{3}} \frac{(-1)^{k-1}}{k} \equiv 0 \pmod p$,故由(4)有

$$F_{p-(\frac{5}{p})}/p \equiv -\frac{2}{5}\sum_{1\leq k<\frac{4p}{5}} \frac{(-1)^{k-1}}{k} \equiv -\frac{2}{5}\sum_{\frac{2p}{3}<k<\frac{4p}{5}} \frac{(-1)^{k-1}}{k}$$

$$\equiv -\frac{2}{5}\sum_{\frac{p}{5}<k<\frac{p}{3}} \frac{(-1)^{p-k-1}}{p-k} \equiv \frac{2}{5}\sum_{\frac{p}{5}<k<\frac{p}{3}} \frac{(-1)^{k}}{k} \pmod p.$$

这就证得(5). 而由推论 3.3 知

$$\sum_{\frac{p}{5}<k<\frac{p}{3}} \frac{(-1)^{k}}{k} = \sum_{\frac{p}{5}<k<\frac{4p}{15}} \frac{(-1)^{k}}{k} + \sum_{\frac{4p}{15}<k<\frac{p}{3}} \frac{(-1)^{k}}{k}$$

$$\equiv 15\sum_{\substack{k=1\\ k\equiv 4p(15)}}^{p-1} \frac{(-1)^{k-1}}{k} - 15\sum_{\substack{k=1\\ k\equiv 5p(15)}}^{p-1} \frac{(-1)^{k-1}}{k} \pmod p,$$

故由(5)立得(6).

依据定理 3.1(ii) (iii)和推论 3.1 我们知(7)成立.

对于(8),注意到

$$\sum_{k=1}^{[\frac{p}{5}]} \frac{1}{k} = 5K_5(0,p) \equiv -\frac{5}{4}q_p(5) - \frac{5}{4}\,\frac{F_{p-(\frac{5}{p})}}{p} \pmod p,$$

而由[1]引理 1.1

$$\sum_{k=1}^{[\frac{p}{5}]}\frac{1}{k}\equiv\left(1-(-1)^{[\frac{p}{5}]}\binom{p-1}{[\frac{p}{5}]}\right)\Big/p\pmod p,$$

故知

$$F_{p-(\frac{5}{p})}/p\equiv\frac{4}{5}\left((-1)^{[\frac{p}{5}]}\binom{p-1}{[\frac{p}{5}]}-1\right)\Big/p-q_p(5)\pmod p.$$

至此定理得证.

值得指出，利用定理的(5)和(6)来计算 Fibonacci 商是快速的，计算项数约为$\frac{2}{15}p$.

我们转而讨论 Lucas 商 $u_{p-(\frac{2}{p})}/p \bmod p$.

定理 3.3　设 p 为奇素数，$K_8(r,p)=\sum\limits_{\substack{k=1\\k\equiv rp(8)}}^{p-1}\frac{1}{k}$，则

(i) $8K_8(1,p)\equiv-8K_8(0,p)\equiv4q_p(2)+2u_{p-(\frac{2}{p})}/p\pmod p$;

(ii) $8K_8(2,p)\equiv-8K_8(7,p)\equiv-q_p(2)-2u_{p-(\frac{2}{p})}/p\pmod p$;

(iii) $8K_8(3,p)\equiv-8K_8(6,p)\equiv q_p(2)-2u_{p-(\frac{2}{p})}/p\pmod p$;

(iv) $8K_8(4,p)\equiv-8K_8(5,p)\equiv-2q_p(2)+2u_{p-(\frac{2}{p})}/p\pmod p$.

证　根据[1]推论 1.6 和推论 1.7，我们有

$$K_8(0,p)+K_8(4,p)=\frac{1}{4}\sum_{k=1}^{[\frac{p}{4}]}\frac{1}{k}\equiv-\frac{3}{4}q_p(2)\pmod p,$$

$$K_8(2,p)+K_8(6,p)=\sum_{\substack{k=1\\k\equiv2(4)}}^{p-1}\frac{1}{k}\equiv\frac{1}{2}\sum_{s=1}^{[\frac{p+1}{4}]}\frac{1}{2s-1}\equiv-\frac{1}{4}q_p(2)\pmod p.$$

又由推论 3.1 和[1]推论 1.6

$$K_8(2,p)-K_8(0,p)\equiv K_8(1,p)+K_8(2,p)\equiv-\frac{1}{8}\Big(\sum_{0<k<\frac{p}{8}}\frac{1}{k}+\sum_{\frac{p}{8}<k<\frac{2p}{8}}\frac{1}{k}\Big)$$

$$=-\frac{1}{8}\sum_{0<k<\frac{p}{4}}\frac{1}{k}\equiv\frac{3}{8}q_p(2)\pmod p,$$

故我们仅需对某一 s 确定 $K_8(s,p)\bmod p$.

由[1]推论 1.7 和[2]定理 2.5 知

$$\sum_{k=1}^{[\frac{p+1}{4}]}\frac{(-1)^k}{2k-1}\equiv(-1)^{\frac{p-1}{2}}u_{p-(\frac{2}{p})}/p\pmod p,$$

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

故

$$K_8((-1)^{\frac{p+1}{2}}2,p)=\sum_{k=1}^{[\frac{p+1}{8}]}\frac{1}{8k-2}=\frac{1}{4}\sum_{\substack{s=1\\2|s}}^{[\frac{p+1}{4}]}\frac{2}{2s-1}$$

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

由此不难导出全部关系式，从而定理获证．

定理 3.4 设 p 为奇素数，则

(i) $$u_{p-(\frac{2}{p})}/p\equiv-2q_p(2)+\frac{1}{2}\,\frac{(-1)^{[\frac{p}{8}]}\binom{p-1}{[\frac{p}{8}]}-1}{p}\pmod p;$$

(ii) $$u_{p-(\frac{2}{p})}/p\equiv-2\sum_{\substack{k=1\\k\equiv 2p,3p(8)}}^{p-1}\frac{1}{k}\equiv\frac{1}{4}\sum_{\frac{p}{8}<k<\frac{3p}{8}}\frac{1}{k}\pmod p;$$

(iii)（孙智伟）$$u_{p-(\frac{2}{p})}/p\equiv\frac{1}{2}\sum_{\frac{p}{4}<k<\frac{p}{2}}\frac{(-1)^k}{k}\pmod p;$$

(iv) $$u_{p-(\frac{2}{p})}/p\equiv\frac{1}{4}\left(\sum_{\frac{p}{8}<k<\frac{p}{4}}\frac{1}{k}+\sum_{\frac{p}{4}<k<\frac{p}{3}}\frac{(-1)^k}{k}\right)\pmod p\ (p\neq 3).$$

证 (i) 根据[1]引理 1.1 和定理 3.3(i) 知

$$u_{p-(\frac{2}{p})}/p\equiv-4K_8(0,p)-2q_p(2)\equiv-2q_p(2)-\frac{1}{2}\sum_{k=1}^{[\frac{p}{8}]}\frac{1}{k}$$

$$\equiv-2q_p(2)+\frac{1}{2}\left((-1)^{[\frac{p}{8}]}\binom{p-1}{[\frac{p}{8}]}-1\right)\Big/p\pmod p.$$

(ii) 由定理 3.3(ii)、(iii)和推论 3.1 立得．

(iii) 利用推论 3.2 和定理 3.3(ii)我们有

$$\sum_{\frac{p}{4}<k<\frac{p}{2}}\frac{(-1)^k}{k}=\sum_{1\leqslant k<\frac{p}{2}}\frac{(-1)^k}{k}-\sum_{1\leqslant k<\frac{p}{4}}\frac{(-1)^k}{k}\equiv 4K_4(2,p)-8K_8(2,p)$$

$$=2\sum_{k=1}^{[\frac{p+1}{4}]}\frac{1}{2k-1}-8K_8(2,p)\equiv-q_p(2)+q_p(2)+2\frac{u_{p-(\frac{2}{p})}}{p}$$

$$=2u_{p-(\frac{2}{p})}/p\pmod p.$$

(iv) 由推论 3.1 和推论 3.2 知

$$\sum_{\frac{p}{8}<k<\frac{p}{4}}\frac{1}{k}\equiv-8\sum_{\substack{k=1\\k\equiv 2p(8)}}^{p-1}\frac{1}{k}\equiv-\sum_{1\leqslant k<\frac{p}{4}}\frac{(-1)^k}{k}\pmod p,$$

又由[1]推论 1.3 得

$$\sum_{1\leqslant k<\frac{p}{3}}\frac{(-1)^k}{k}\equiv-2q_p(2)\qquad\pmod p.$$

故有

$$\sum_{\frac{p}{8}<k<\frac{p}{4}}\frac{1}{k}+\sum_{\frac{p}{4}<k<\frac{p}{3}}\frac{(-1)^k}{k}\equiv-8K_8(2,p)-2q_p(2)-8K_8(2,p)$$

$$\equiv -2q_p(2)+2\left(q_p(2)+2\frac{u_{p-(\frac{2}{p})}}{p}\right)=4\frac{u_{p-(\frac{2}{p})}}{p}\pmod p.$$

综上定理得证.

在实际计算 $u_{p-(\frac{2}{p})}/p \bmod p$ 时应用定理3.4(iv)甚为方便,其计算项数约为$\frac{5}{24}p<\frac{p}{4}$.

3.3 $F(p)/p \bmod p$

设$E_n(x)$表Euler多项式,即

$$E_n(x)+\sum_{r=0}^{n}\binom{n}{r}E_r(x)=2x^n\quad(n=0,1,2\cdots).$$

现已熟知(见[6])如下结果:

(i) $\sum_{k=1}^{m}(-1)^k k^n=\frac{1}{2}[(-1)^m E_n(m+1)-E_n(1)]$;

(ii) $E_n(1-x)=(-1)^n E_n(x)$;

(iii) $E_n(x)=\frac{2}{n+1}(B_{n+1}(x)-2^{n+1}B_{n+1}(\frac{x}{2}))$.

此处$B_n(x)$为Bernoulli多项式.

引理3.3 设p为奇素数,$x\equiv y \pmod p$, $0\leqslant n\leqslant p-2$, 则

$$E_n(x)\equiv E_n(y)\pmod p.$$

证 令$B_n=B_n(0)$为Bernoulli数,则 $B_n(x)=\sum_{k=0}^{n}\binom{n}{k}B_k x^{n-k}$. 据此有

$$E_n(x)=\frac{2}{n+1}(B_{n+1}(x)-2^{n+1}B_{n+1}(\frac{x}{2}))=\frac{2}{n+1}\sum_{k=0}^{n+1}\binom{n+1}{k}(1-2^k)B_k x^{n+1-k}$$

$$=\frac{2}{n+1}\sum_{r=0}^{n}\binom{n+1}{r+1}(1-2^{r+1})B_{r+1}x^{n-r}=\sum_{r=0}^{n}\binom{n}{r}\frac{2(1-2^{r+1})B_{r+1}}{r+1}x^{n-r}.$$

当$0\leqslant n\leqslant p-2$时$1\leqslant r+1\leqslant p-1$,故知$p\nmid r+1$. 又由Staudt定理和Fermat小定理知$2(1-2^{r+1})B_{r+1}$恒为整数(参看[7,p.247]),故当$x\equiv y\pmod p$时必有$E_n(x)\equiv E_n(y)\pmod p$.

现在我们能够给出如下的漂亮结果.

定理3.5 设$F(0)=1$, $F(1)=0$, $F(2)=2$, $F(n+2)=3F(n)-F(n-1)$ $(n=1,2,3,\cdots)$, 则当p为大于3的素数时 $p\mid F(p)$且有

$$\frac{F(p)}{p}\equiv(-1)^{[\frac{5p}{9}]}\frac{1}{6}E_{p-2}\left(\left\{\frac{5p}{9}\right\}\right)-\frac{1}{3}q_p(2)\pmod p.$$

证 由[2]定理2.7知$6F(p)=9T_{\frac{p}{2}(9)}-2^p+2$,而由[1]引理1.1

$$T_{\frac{p}{2}(9)}/p\equiv\sum_{\substack{k=1\\k\equiv\frac{p}{2}(9)}}^{p-1}\frac{(-1)^{k-1}}{k}=\sum_{\substack{k=1\\k\equiv 5p(9)}}^{p-1}\frac{(-1)^{k-1}}{k}\pmod p.$$

故

$$\frac{6F(p)}{p} \equiv 9 \sum_{\substack{k=1 \\ k \equiv 5p(9)}}^{p-1} \frac{(-1)^{k-1}}{k} - 2q_p(2) \pmod p.$$

根据推论 3.3、引理 3.3 和 $E_n(x)$ 的性质我们有

$$\sum_{\substack{k=1 \\ k \equiv 5p(9)}}^{p-1} \frac{(-1)^{k-1}}{k} \equiv -\frac{1}{9} \sum_{\frac{4p}{9}<k<\frac{5p}{9}} \frac{(-1)^k}{k} \equiv -\frac{1}{9}\left(\sum_{k=1}^{[\frac{5p}{9}]} (-1)^k k^{p-2} - \sum_{k=1}^{[\frac{4p}{9}]} (-1)^k k^{p-2} \right)$$

$$= -\frac{1}{18}\left((-1)^{[\frac{5p}{9}]} E_{p-2}(1+[\frac{5p}{9}]) - E_{p-2}(1) - (-1)^{[\frac{4p}{9}]} E_{p-2}(1+[\frac{4p}{9}]) + E_{p-2}(1) \right)$$

$$= -\frac{1}{18}\left((-1)^{[\frac{5p}{9}]} E_{p-2}(\frac{5p}{9}+1-\{\frac{5p}{9}\}) - (-1)^{[\frac{4p}{9}]} E_{p-2}(\frac{4p}{9}+1-\{\frac{4p}{9}\}) \right)$$

$$\equiv -\frac{1}{18}\left((-1)^{[\frac{5p}{9}]} E_{p-2}(1-\{\frac{5p}{9}\}) - (-1)^{[\frac{4p}{9}]} E_{p-2}(1-\{\frac{4p}{9}\}) \right)$$

$$= \frac{1}{18}\left((-1)^{[\frac{5p}{9}]} E_{p-2}(\{\frac{5p}{9}\}) + (-1)^{[\frac{4p}{9}]} E_{p-2}(\{\frac{5p}{9}\}) \right)$$

$$= \frac{1}{9}(-1)^{[\frac{5p}{9}]} E_{p-2}(\{\frac{5p}{9}\}) \pmod p,$$

因此

$$\frac{6F(p)}{p} \equiv (-1)^{[\frac{5p}{9}]} E_{p-2}(\{\frac{5p}{9}\}) - 2q_p(2) \pmod p.$$

证毕.

3.4 $5^{\frac{p-1}{4}} \bmod p$

设 p 为 $4k+1$ 形素数,则有整数 a、b 使得 $p=a^2+b^2$. 根据 $(1+\frac{b}{a})^2 \equiv 2\frac{b}{a} \pmod p$ 和 Euler 判别条件不难证明(参见[7, p. 64])如下的

命题 3.1 设 $p=a^2+b^2$ 为 $4k+1$ 形素数, $2|b$, 则

(i) (Gauss) 当 $p\equiv 1 \pmod 8$ 时 $2^{\frac{p-1}{4}} \equiv (-1)^{\frac{b}{4}} \pmod p$;

(ii) (Dirichlet) 当 $p\equiv 5 \pmod 8$ 时取 $a\equiv 1 \pmod 4$、$b\equiv 2 \pmod 8$, 则

$$2^{\frac{p-1}{4}} \equiv (\frac{b}{a})^{\frac{ab}{2}} \equiv \frac{b}{a} \pmod p.$$

本节将利用组合和理论和 Lucas 序列的知识给出 $5^{\frac{p-1}{4}} \bmod p$ 的完全结果. 值得注意的是,当 $(\frac{5}{p})=1$ 时这由四次互反律才能推出,而当 $(\frac{5}{p})=-1$ 时这属于四次剩余理论没有解决的问题.

令 $\{u_n(a,b)\}$ 表示如下定义的 Lucas 序列

$$u_0(a,b)=0,\ u_1(a,b)=1,\ u_{n+1}(a,b)=bu_n(a,b)-au_{n-1}(a,b)\ (n=1,2,3,\cdots).$$

如众周知,当 $b^2-4a\neq 0$ 时

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

由此不难验证 $a(b^2-4a)\neq 0$ 时

(*2) $u_n(a,b)=(\sqrt{a})^{n-1}u_n(1,\ \frac{b}{\sqrt{a}})$;

(*3) $u_{2n}(a,b)=bu_n(a^2,b^2-2a)$.

引理3.4　设 p 为奇素数，a,b 为 p—整数，$p\nmid a(b^2-4a)$，$(\frac{a}{p})=1$，$c^2\equiv a(\mathrm{mod}\ p)$，则

(i) 当 $\left(\frac{b^2-4a}{p}\right)=1$ 时 $u_{\frac{p+1}{2}}(a,b)\equiv\left(\frac{b-2c}{p}\right)$，$u_{\frac{p-1}{2}}(a,b)\equiv 0\ (\mathrm{mod}\ p)$;

(ii) 当 $\left(\frac{b^2-4a}{p}\right)=-1$ 时 $u_{\frac{p+1}{2}}(a,b)\equiv 0$，$u_{\frac{p-1}{2}}(a,b)\equiv\frac{1}{c}\left(\frac{b-2c}{p}\right)\ (\mathrm{mod}\ p)$.

证　由(*3)知 $u_n(1,x)=\frac{1}{\sqrt{x+2}}u_{2n}(1,\ \sqrt{x+2})=\frac{1}{\sqrt{x-2}}u_{2n}(-1,\sqrt{x-2})$，故

$$\begin{aligned}u_{2n+1}(1,\ \sqrt{x+2})&=\frac{1}{\sqrt{x+2}}(u_{2n+2}(1,\ \sqrt{x+2})+u_{2n}(1,\sqrt{x+2}))\\&=u_{n+1}(1,x)+u_n(1,x)\ ,\end{aligned}$$

$$\begin{aligned}u_{2n+1}(-1,\sqrt{x-2})&=\frac{1}{\sqrt{x-2}}(u_{2n+2}(-1,\sqrt{x-2})-u_{2n}(-1,\sqrt{x-2}))\\&=u_{n+1}(1,x)-u_n(1,x).\end{aligned}$$

由此知

$$u_{\frac{p+1}{2}}(1,x)=\frac{1}{2}(u_p(1,\sqrt{x+2})+u_p(-1,\sqrt{x-2})),$$

$$u_{\frac{p-1}{2}}(1,x)=\frac{1}{2}(u_p(1,\sqrt{x+2})-u_p(-1,\ \sqrt{x-2})).$$

当 α 和 β^2 为 p—整数时我们有($\beta^2-4\alpha\neq 0$)

$$\begin{aligned}u_p(\alpha,\beta)&=\frac{1}{\sqrt{\beta^2-4\alpha}}\left\{\left(\frac{\beta+\sqrt{\beta^2-4\alpha}}{2}\right)^p-\left(\frac{\beta-\sqrt{\beta^2-4\alpha}}{2}\right)^p\right\}\\&=\frac{1}{\sqrt{\beta^2-4\alpha}}\cdot\frac{1}{2^p}\cdot 2\sum_{\substack{k=0\\2\nmid k}}^{p}\binom{p}{k}\beta^{p-k}(\sqrt{\beta^2-4\alpha})^k\\&=\frac{1}{2^{p-1}}\left((\beta^2-4\alpha)^{\frac{p-1}{2}}+\sum_{\substack{k=1\\2\nmid k}}^{p-1}\binom{p}{k}(\beta^2)^{\frac{p-k}{2}}(\beta^2-4\alpha)^{\frac{k-1}{2}}\right)\\&\equiv(\beta^2-4\alpha)^{\frac{p-1}{2}}\equiv\left(\frac{\beta^2-4\alpha}{p}\right)\ (\mathrm{mod}\ p),\end{aligned}$$

故 $x\neq\pm 2$ 为 p-整数时

$$u_p(1,\sqrt{x+2})\equiv\left(\frac{x-2}{p}\right),\ u_p(-1,\ \sqrt{x-2})\equiv\left(\frac{x+2}{p}\right)\ (\mathrm{mod}\ p),$$

进而有

$$u_{\frac{p+1}{2}}(1,x)\equiv\frac{1}{2}\left[\left(\frac{x-2}{p}\right)+\left(\frac{x+2}{p}\right)\right]\ (\mathrm{mod}\ p),$$

$$u_{\frac{p-1}{2}}(1,x)\equiv\frac{1}{2}\left[\left(\frac{x-2}{p}\right)-\left(\frac{x+2}{p}\right)\right]\ (\mathrm{mod}\ p).$$

根据(*2)取 $x=\frac{b}{c}$ 我们得

$$u_{\frac{p+1}{2}}(a,b) \equiv c^{\frac{p-1}{2}} u_{\frac{p+1}{2}}(1,\frac{b}{c}) \equiv c^{\frac{p-1}{2}} \cdot \frac{1}{2}\left[\left(\frac{\frac{b}{c}-2}{p}\right)+\left(\frac{\frac{b}{c}+2}{p}\right)\right]$$

$$\equiv \frac{1}{2}\left[\left(\frac{b-2c}{p}\right)+\left(\frac{b+2c}{p}\right)\right] \pmod p$$

$$u_{\frac{p-1}{2}}(a,b) \equiv c^{\frac{p-1}{2}-1} u_{\frac{p-1}{2}}(1,\frac{b}{c}) \equiv c^{\frac{p-1}{2}} \cdot \frac{1}{c} \cdot \frac{1}{2}\left[\left(\frac{\frac{b}{c}-2}{p}\right)-\left(\frac{\frac{b}{c}+2}{p}\right)\right]$$

$$\equiv \frac{1}{2c}\left[\left(\frac{b-2c}{p}\right)-\left(\frac{b+2c}{p}\right)\right] \pmod p.$$

注意到$\left(\frac{b-2c}{p}\right)\left(\frac{b+2c}{p}\right)=\left(\frac{b^2-4a}{p}\right)$便知引理成立．

现在我们给出 $5^{\frac{p-1}{4}} \bmod p$ 的基本结果．

定理 3.6 设 $p\neq 5$ 为 $4k+1$ 形素数，$p=a^2+b^2$，$a,b\in Z$，$2|b$，则

(i) (Gauss) 当 $p\equiv 1, 9 \pmod{20}$ 时 $5^{\frac{p-1}{4}} \equiv \begin{cases} 1 \\ -1 \end{cases} \pmod p \quad \begin{matrix} \text{当 } 5|b \text{ 时,} \\ \text{当 } 5|a \text{ 时;} \end{matrix}$

(ii) 当 $p\equiv 13, 17 \pmod{20}$ 时必可选取上述的 a、b 使 $a\equiv b \pmod 5$，此时

$$5^{\frac{p-1}{4}} \equiv b/a \pmod p.$$

注：如众周知，$4k+1$ 形的素数 p 必可表成 $p=a^2+b^2$.

证 (i) 令 $F_n=u_n(-1,1)$ 为 Fibonacci 数列，则由[3]推论 1 知 $F_{\frac{p+1}{2}} \equiv (-1)^{[\frac{p+5}{10}]} 5^{\frac{p-1}{4}} \pmod p$. 注意到$(-\frac{b}{a})^2 \equiv -1 \pmod p$，由引理 3.4 知

$$F_{\frac{p+1}{2}} \equiv \left(\frac{1+2\frac{b}{a}}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a+2b}{p}\right) = \left(\frac{|a|}{p}\right)\left(\frac{|a+2b|}{p}\right)$$

$$= \left(\frac{p}{|a|}\right)\left(\frac{p}{|a+2b|}\right) = \left(\frac{a^2+b^2}{|a|}\right)\left(\frac{a^2-4b^2+5b^2}{|a+2b|}\right) = \left(\frac{5}{|a+2b|}\right)$$

$$= \left(\frac{a+2b}{5}\right) \pmod p.$$

故有

$$5^{\frac{p-1}{4}} \equiv (-1)^{[\frac{p+5}{10}]}\left(\frac{a+2b}{5}\right) = \begin{cases} 1\cdot 1 = 1 & \text{当 } p\equiv 1(20) \text{ 且 } 5|b \text{ 时} \\ 1\cdot(-1) = -1 & \text{当 } p\equiv 1(20) \text{ 且 } 5|a \text{ 时} \\ (-1)(-1) = 1 & \text{当 } p\equiv 9(20) \text{ 且 } 5|b \text{ 时} \\ (-1)\cdot 1 = -1 & \text{当 } p\equiv 9(20) \text{ 且 } 5|a \text{ 时} \end{cases}$$

$$= \begin{cases} 1 \\ -1 \end{cases} \pmod p \quad \begin{matrix} \text{当 } 5|b \text{ 时,} \\ \text{当 } 5|a \text{ 时.} \end{matrix}$$

(ii) 由设知 $p\equiv \pm 2 \pmod 5$，用 $a,b\equiv 0, \pm 1, \pm 2 \pmod 5$ 可验知，必可找到合乎要求的 a,b. 又根据引理 3.4 类似(i)的论证知

$$F_{\frac{p-1}{2}} \equiv -\frac{1}{b/a}\left(\frac{1+2\frac{b}{a}}{p}\right) \equiv \frac{b}{a}\left(\frac{a}{p}\right)\left(\frac{a+2b}{p}\right) = \frac{b}{a}\left(\frac{a+2b}{5}\right)$$

$$\equiv \frac{b}{a}\left(\frac{3a}{5}\right)=-\frac{b}{a}\left(\frac{a}{5}\right)=\begin{cases}\dfrac{b}{a} \pmod p & \text{当 } p\equiv 13 \pmod{20} \text{ 时},\\ -\dfrac{b}{a} & \text{当 } p\equiv 17 \pmod{20} \text{ 时}.\end{cases}$$

又据[3]推论1知 $F_{\frac{p-1}{2}}\equiv(-1)^{[\frac{p-5}{10}]}5^{\frac{p-1}{4}}\pmod p$，故

$$5^{\frac{p-1}{4}}\equiv(-1)^{[\frac{p-5}{10}]}F_{\frac{p-1}{2}}\equiv\frac{b}{a}\pmod p.$$

于是定理得证．

推论 3.4　设 p 为 $20k+1$ 或 $20k+9$ 形素数，$p=a^2+b^2$，$a,b\in\mathbb{Z}$，$2|b$，则

(i) 当 $p\equiv1$，$29\pmod{40}$ 时 $p|F_{\frac{p-1}{4}}\Leftrightarrow 5|b$；

(ii) 当 $p\equiv9,21\pmod{40}$ 时 $p|F_{\frac{p-1}{4}}\Leftrightarrow 5|a$.

证　由[3]引理3知 $p|F_{\frac{p-1}{4}}\Leftrightarrow 5^{\frac{p-1}{4}}\equiv(-1)^{[\frac{p+5}{10}]+\frac{p-1}{4}}\pmod p$. 此和定理3.6(i)结合即得推论．

作为文章的结束，我们指出如下猜想．

猜想 3.1　设 p 为 $12k+5$ 形素数，$p=a^2+b^2$，$a,b\in\mathbb{Z}$，$2|b$，$3|a+b$，则 $(-3)^{\frac{p-1}{4}}\equiv\frac{b}{a}$ $\pmod p$.

猜想 3.2　设 p 为 $8k+3$ 形素数，$p=x^2+2y^2$，x、$y\in\mathbb{Z}$，$x\equiv5,7\pmod 8$，$y\equiv3\pmod 4$，则

$$u_{\frac{p+1}{4}}\equiv\frac{1}{2}(-1)^{[\frac{x+y}{4}]}\pmod p.$$

补注　定理3.2(i)和定理3.4(ii)的一部分已由 H. C. Williams[8]获得，推论3.4早为 E. Lehmer[9]所知，猜想3.1及相应一般问题新近由作者解决．

参 考 文 献

1 孙智宏，组合和 $\sum\limits_{\substack{k=0\\k\equiv r(\mathrm{mod}\ m)}}^{n}\binom{n}{k}$ 及其数论应用(Ⅰ)，南京大学学报数学半年刊，9(1992)，No. 2，227～240.

2 孙智宏，组合和 $\sum\limits_{\substack{k=0\\k\equiv r(\mathrm{mod}\ m)}}^{n}\binom{n}{k}$ 及其数论应用(Ⅱ)，南京大学学报数学半年刊，10(1993)，No. 1，105～118.

3 Sun Zhihong and Sun Zhiwei (孙智宏、孙智伟)，Fibonacci numbers and Fermat's last theorem，Acta Arith.，60(1992)，No. 4，371～388.

4 Granville，A. and Zhiwei Sun，Values of Bernoulli polynomials，Pacific J. Math.，to appear.

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

6 王竹溪、郭敦仁，特殊函数概论，北京：科学出版社，1979.

7 Ireland，K. and Rosen，M.，A Classical Introduction to Modern Number Theory，Spring-Verlag，New York，1982.

8 Williams，H. C.，Some formulas concerning the fundamental unit of a real quadratic field，Discrete Mathematics，92(1991)，431～440.

9 Lehmer, E., On the quadratic character of the Fibonacci root, Fibonacci Quart., 4(1966), 135~138; MR39#160.

COMBINATORIAL SUM $\sum_{k\equiv r(\mathrm{mod}\ m)}\binom{n}{k}$ AND ITS APPLICATIONS IN NUMBER THEORY (Ⅲ)

Sun Zhihong

(Huaiyin Teachers' College)

Abstract This paper continues the disscussion of [1]、[2]、[3]. We obtain various expressions of $F_{p-(\frac{5}{p})}/p$、$u_{p-(\frac{2}{p})}/p$ and $F(p)/p$ mod p, where $p>5$ is a prime and

$F_0=0,\ F_1=1,\ F_{n+1}=F_n+F_{n-1}$

$u_0=0,\ u_1=1,\ u_{n+1}=2u_n+u_{n-1}$ $(n=1,2,3,\cdots)$

$F(0)=1,\ F(1)=0,\ F(2)=2,\ F(n+2)=3F(n)-F(n-1)$.

As another application, we completely determine $5^{\frac{p-1}{4}}$ mod p, where $p\neq5$ is a prime of the form $4k+1$.

Keywords Number theoretical quotients, combinatorial sum, Lucas sequences.