组合和 $\sum_{\substack{k=0\\k\equiv r(\mathrm{mod}\ m)}}^{n}\binom{n}{k}$ 及其数论应用(Ⅰ)*

孙智宏
(淮阴师范专科学校)

COMBINATORIAL SUM $\sum_{\substack{k=0\\k\equiv r(\mathrm{mod}\ m)}}^{n}\binom{n}{k}$ AND ITS APPLICATIONS IN NUMBER THEORY (Ⅰ)

Sun Zhihong
(Huaiyin Normal College)

Abstract

This paper studies the sum $T^{n}_{r(m)}=\sum_{\substack{k=0\\k\equiv r(\mathrm{mod}\,m)}}^{n}\binom{n}{k}$ in the cases $m=3,4,5,6$, and shows that it can be used to obtain congruences concerning Fermat quotients $q_p(2)=\frac{2^{p-1}-1}{p}$ and $q_p(3)=\frac{3^{p-1}-1}{p}$. Furthermore, we establish the following recursive relations:

$$\sum_{s=0}^{m}(-1)^{[\frac{m-s}{2}]}\binom{[\frac{m+s}{2}]}{s}\Delta_{2m+1}(k,n+s)=0\quad(n=0,1,2,\cdots)$$

$$\sum_{s=0}^{m}(-1)^{m-s}\binom{m+1+s}{m-s}\Delta_{2m+2}(k,n+2s)=0\quad(n=1,2,3,\cdots)$$

* 1989年10月30日收到初稿;1992年元月23日收到修改稿.

where

$$\Delta_m(k,n)=\begin{cases} mT^n_{\frac{n}{2}+k(m)}-2^n & \text{if} \quad 2\nmid m; \\ mT^n_{\left[\frac{n}{2}\right]+k(m)}-2^n & \text{if} \quad 2|m. \end{cases}$$

引 言

本文(Ⅰ、Ⅱ、Ⅲ)主要讨论组合和

$$T^n_{r(m)}=\sum_{\substack{k=0\\ k\equiv r(\mathrm{mod}\, m)}}^{n}\binom{n}{k} \tag{1.0}$$

与它的数论应用.

$T^n_{r(m)}$ 的组合意义是 n 个元素的集合其基数模 m 余 r 的子集个数.

熟知

$$T^n_{0(1)}=2^n,\quad T^n_{0(2)}=T^n_{1(2)}=2^{n-1}\qquad (n\geqslant 1) \tag{1.1}$$

对于正整数 m, 确定 $T^n_{r(m)}$ 对于数论很有意义. 这表现为本文用它来处理数论商 (Fermat 商和 Lucas 商) 和获得同余式. 事实上, H.C.Williams[1] 已经应用对 $T^n_{r(5)}$ 的讨论 (并未确定其值) 求得了 Fibonacci 商, [5] 中更有一些深刻结果.

我们在全文中通用以下的记号与约定:

$x\equiv r(m)$为$x\equiv r(\mathrm{mod}\ m)$的缩写,

$T^n_{r(m)}$表示(1.0)式给出的组合和,

$[x]$表示不超过实数x的最大整数,

$\left(\frac{a}{m}\right)$为a对正整数m的Jacobi符号,

$q_p(a)=\frac{a^{p-1}-1}{p}$为$a$对奇素数$p$的Fermat商,

(m,n)表示整数m和n的最大公因子,

$$ct(k\equiv r(m))=\begin{cases}1 & \text{当}k\equiv r(\mathrm{mod}m)\text{时}\\ 0 & \text{当}k\not\equiv r(\mathrm{mod}m)\text{时},\end{cases}$$

$$\Delta_m(k,n)=\begin{cases} mT^n_{\frac{n}{2}+k(m)}-2^n & \text{当}2\nmid m\text{时} \\ mT^n_{\left[\frac{n}{2}\right]+k(m)}-2^n & \text{当}2|m\text{时}, \end{cases}$$

$\frac{1}{k}\mathrm{mod}p$为同余式$kx\equiv 1(\mathrm{mod}p)$的解.

$u_n(a,b)$、$v_n(a,b)$ 表示如下的 Lucas 序列 u_n、v_n:

$$u_0=0,\ u_1=1,\ u_{n+1}=bu_n-au_{n-1}$$

$$(n=1,2,\cdots)$$

$$v_0=2,\ v_1=b,\ v_{n+1}=bv_n-av_{n-1}$$

$F_n=u_n(-1,1)$ 表 Fibonacci 数列，$L_n=v_n(-1,1)$ 为 Lucas 序列，m 表正整数，n、p 表非负整数，k、r 表整数，求和号上标小于下标时和为零.

孙智伟曾与作者一起研究和 $T^n_{r(m)}$，本文推论 1.8 是他首先明确指出的，$\Delta_m(k,n)$ 递推关系的研究也是他提出的课题. 作者特此致谢.

1.1　$T^n_{r(3)}$ 与 $T^n_{r(4)}$ 的值及其推论

引理 1.1　设 p 为奇素数，则

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

(2)　若 0 和 p 中恰有 ε 个 $(\varepsilon=0,1,2)$ 模 m 余 r，则

$$\sum_{\substack{k=1\\k\equiv r(m)}}^{p-1}\frac{(-1)^{k-1}}{k}\equiv\frac{T^p_{r(m)}-\varepsilon}{p}\pmod p$$

证　(1)　当 $1\leqslant k\leqslant p-1$ 时，$\binom{p-1}{k}=\frac{1}{k!}(p-1)(p-2)\cdots(p-k)$

$$=\frac{1}{k!}\left[p^k+\sum_{s=1}^{k}(-s)p^{k-1}+\cdots+\sum_{s=1}^{k}\frac{(-1)(-2)\cdots(-k)}{(-s)}p+(-1)(-2)\cdots(-k)\right]$$

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

当 $k=0$ 时 $\binom{p-1}{0}=1\equiv(-1)^0\times1\pmod p$

(2)　$$\frac{T^p_{r(m)}-\varepsilon}{p}=\frac{1}{p}\sum_{\substack{k=1\\k\equiv r(m)}}^{p-1}\binom{p}{k}=\sum_{\substack{k=1\\k\equiv r(m)}}^{p-1}\frac{1}{k}\binom{p-1}{k-1}\equiv\sum_{\substack{k=1\\k\equiv r(m)}}^{p-1}\frac{(-1)^{k-1}}{k}\pmod p$$

推论 1.1　设 p 为奇素数，$m\neq1,p$，则

(1)　当 $2\nmid m$ 时，$$\sum_{k=1}^{\left[\frac{p-1}{m}\right]}\frac{(-1)^{k-1}}{k}\equiv\frac{mT^p_{o(m)}-m}{p}\pmod p$$

(2)　当 $2\mid m$ 时，$$\sum_{k=1}^{\left[\frac{p-1}{m}\right]}\frac{1}{k}\equiv\frac{m-mT^p_{o(m)}}{p}\pmod p$$

证　在引理 1.1 中取 $r=0$ 即得.

推论 1.2　(Eisenstein[2])　设 p 为奇素数，则

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

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

定理 1.1 $T^n_{\frac{n}{2}(3)}=\frac{2^n+2(-1)^n}{3}$，$T^n_{\frac{n}{2}\pm 1(3)}=\frac{2^n-(-1)^n}{3}$

证 令 $\omega=\frac{-1+\sqrt{3}i}{2}$ 为三次本原单位根，则

$$(-1)^n\omega^{2n}=(-\omega^2)^n=(1+\omega)^n=\sum_{k=0}^{n}\binom{n}{k}\omega^k=T^n_{0(3)}+T^n_{1(3)}\omega+T^n_{2(3)}\omega^2$$

$$=T^n_{0(3)}-T^n_{2(3)}+(T^n_{1(3)}-T^n_{2(3)})\omega$$

当 $n\equiv 0 \pmod 3$ 时，$\omega^{2n}=1$，故比较上式两端得

$$T^n_{0(3)}-T^n_{2(3)}=(-1)^n,\quad T^n_{1(3)}-T^n_{2(3)}=0$$

再由 $T^n_{0(3)}+T^n_{1(3)}+T^n_{2(3)}=T^n_{0(1)}=2^n$ 即可解得

$$T^n_{1(3)}=T^n_{2(3)}=\frac{2^n-(-1)^n}{3},\quad T^n_{0(3)}=\frac{2^n+2(-1)^n}{3}$$

当 $n\equiv 1(3)$、$n\equiv 2(3)$ 时公式类似可证．

推论 1.3 设 p 为大于 3 的素数，则

$$\frac{1}{3}\sum_{k=1}^{[\frac{p}{3}]}\frac{(-1)^{k-1}}{k}\equiv\sum_{k=1}^{[\frac{p}{3}]}\frac{(-1)^k}{3k-1}\equiv\sum_{k=1}^{[\frac{p+1}{3}]}\frac{(-1)^{k-1}}{3k-2}\equiv\frac{1}{3}\cdot\frac{2^p-2}{p}\pmod p$$

此由引理 1.1 和定理 1.1 直接计算可得．

推论 1.4 设 p 为大于 3 的素数，则

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

证： $\sum_{k=1}^{[\frac{2p}{3}]}\frac{(-1)^{k-1}}{k}=\sum_{k=1}^{p-1}\frac{(-1)^{k-1}}{k}-\sum_{k=[\frac{2}{3}p]+1}^{p-1}\frac{(-1)^{k-1}}{k}=\sum_{k=1}^{p-1}\frac{(-1)^{k-1}}{k}$

$-\sum_{s=1}^{[\frac{p}{3}]}\frac{(-1)^{p-1-s}}{p-s}$

$$\equiv\sum_{k=1}^{p-1}\frac{(-1)^{k-1}}{k}-\sum_{s=1}^{[\frac{p}{3}]}\frac{(-1)^{s-1}}{s}\equiv\frac{2^p-2}{p}-\frac{2^p-2}{p}\equiv 0\pmod p$$

定理 1.2 设 $n\geqslant 1$，$A_n=\frac{1}{2}(2^{n-1}+(-1)^{[\frac{n}{4}]}2^{[\frac{n}{2}]})$，$B_n=\frac{1}{2}(2^{n-1}-(-1)^{[\frac{n}{4}]}2^{[\frac{n}{2}]})$，

则 (1) 当 $n\equiv 0 \pmod 4$ 时，$T^n_0(4)=A_n$，$T^n_{2(4)}=B_n$，$T^n_{1(4)}=T^n_{3(4)}=2^{n-2}$；

(2) 当 $n\equiv 1 \pmod 4$ 时，$T^n_{0(4)}=T^n_{1(4)}=A_n$，$T^n_{2(4)}=T^n_{3(4)}=B_n$；

(3)　当$n\equiv 2\pmod 4$时，$T^n_{1(4)}=A_n$，$T^n_{3(4)}=B_n$，$T^n_{0(4)}=T^n_{2(4)}=2^{n-2}$;

(4)　当$n\equiv 3\pmod 4$时，$T^n_{1(4)}=T^n_{2(4)}=A_n$，$T^n_{0(4)}=T^n_{3(4)}=B_n$.

证　因为 $(1+i)^n=\sum\limits_{k=0}^{n}\binom{n}{k}i^k=T^n_{0(4)}-T^n_{2(4)}+(T^n_{1(4)}-T^n_{3(4)})i$, 而当 $n\equiv 0\pmod 4$ 时 $(1+i)^n=(2i)^{\frac{n}{2}}=(-1)^{\frac{n}{4}}2^{\frac{n}{2}}$, 故 $4|n$ 时

$$T^n_{0(4)}-T^n_{2(4)}=(-1)^{\frac{n}{4}}2^{\frac{n}{2}},\ T^n_{1(4)}-T^n_{3(4)}=0$$

再由 (1.1) 式即知 $T^n_{0(4)}=A_n$，$T^n_{2(4)}=B_n$，$T^n_{1(4)}=T^n_{3(4)}=2^{n-2}$.

当 $n\equiv 1\pmod 4$ 时，$(1+i)^n=(1+i)(2i)^{\frac{n-1}{2}}=(-1)^{\frac{n-1}{4}}2^{\frac{n-1}{2}}(1+i)$, 故

$$T^n_{0(4)}-T^n_{2(4)}=(-1)^{\frac{n-1}{4}}2^{\frac{n-1}{2}},\ T^n_{1(4)}-T^n_{3(4)}=(-1)^{\frac{n-1}{4}}2^{\frac{n-1}{2}}$$

再据 (1.1) 式即得 $T^n_{0(4)}=T^n_{1(4)}=A_n$, $T^n_{2(4)}=T^n_{3(4)}=B_n$.

$n\equiv 2\pmod 4$ 与 $n\equiv 3\pmod 4$ 之情形同理可证.

推论 1.5 (Euler)　设 p 为奇素数，则$\left(\frac{2}{p}\right)=(-1)^{\frac{p-1}{2}+[\frac{p}{4}]}$.

证　当 $p\equiv 1\pmod 4$ 时，$\frac{1}{2}(1-(-1)^{[\frac{p}{4}]}2^{\frac{p-1}{2}})\equiv B_p=T^p_{2(4)}\equiv 0\pmod p$. 当 $p\equiv 3\pmod 4$ 时，$\frac{1}{2}(1+(-1)^{[\frac{p}{4}]}2^{\frac{p-1}{2}})\equiv A_p=T^p_{1(4)}\equiv 0\pmod p$. 故

$$\left(\frac{2}{p}\right)\equiv 2^{\frac{p-1}{2}}\equiv(-1)^{\frac{p-1}{2}+[\frac{p}{4}]}\pmod p$$

即　$\left(\frac{2}{p}\right)=(-1)^{\frac{p-1}{2}+[\frac{p}{4}]}$.

引理 1.2.　设 p 为奇素数，$p\nmid a$, 则

$$\left(\frac{a}{p}\right)a^{\frac{p-1}{2}}\equiv 1+\frac{1}{2}q_p(a)p\pmod{p^2}$$

证　设 $a^{\frac{p-1}{2}}=\left(\frac{a}{p}\right)+kp$, 则 $a^{p-1}=\left[\left(\frac{a}{p}\right)+kp\right]^2\equiv 1+2\left(\frac{a}{p}\right)kp\pmod{p^2}$. 由 $q_p(a)$ 定义，$q_p(a)=\frac{a^{p-1}-1}{p}\equiv 2\left(\frac{a}{p}\right)k\pmod p$, 故立知引理成立.

推论 1.6 (Lerch[2])　设 p 为大于 4 的素数，则

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

证:　由推论 1.1、引理 1.2 和定理 1.2 得

$$\sum_{k=1}^{[\frac{p}{4}]}\frac{1}{k}\equiv-4\cdot\frac{T^p_{0(4)}-1}{p}=-2\cdot\frac{2^{p-1}-1+\left(\frac{2}{p}\right)2^{\frac{p-1}{2}}-1}{p}\equiv-3q_p(2)\pmod p$$

推论 1.7 设 p 为奇素数，则

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

证： 由于 $\sum_{\substack{k=1\\k\equiv 2(4)}}^{p-1}\frac{(-1)^{k-1}}{k}\equiv\frac{T^p_{2(4)}}{p}=\frac{1}{2}\cdot\frac{2^{p-1}-\left(\frac{2}{p}\right)2^{\frac{p-1}{2}}}{p}\equiv\frac{1}{4}q_p(2)\pmod p$，故

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

1.2 $\Delta_m(k,n)$的递推公式

引理 1.3 $T^n_{r(m)}=\frac{2^n}{m}\sum_{l=0}^{m-1}\cos^n\frac{\pi l}{m}\cos\frac{\pi l(n-2r)}{m}$

证： 熟知 $ct(k\equiv r(m))=\frac{1}{m}\sum_{l=0}^{m-1}e^{2\pi i\frac{k-r}{m}l}$，故

$$T^n_{r(m)}=\sum_{k=0}^{n}\binom{n}{k}ct(k\equiv r(m))=\frac{1}{m}\sum_{l=0}^{m-1}\sum_{k=0}^{n}\binom{n}{k}e^{2\pi i\frac{k-r}{m}l}$$

$$=\frac{1}{m}\sum_{l=0}^{m-1}e^{-2\pi i\frac{rl}{m}}\left(1+e^{2\pi i\frac{l}{m}}\right)^n$$

$$=\frac{1}{m}\sum_{l=0}^{m-1}e^{-2\pi i\frac{rl}{m}}\left(2\cos\frac{\pi l}{m}e^{i\frac{\pi l}{m}}\right)^n$$

$$=\frac{1}{m}\sum_{l=0}^{m-1}2^n\cos^n\frac{\pi l}{m}e^{\pi i\frac{n-2r}{m}l}$$

由于 $T^n_{r(m)}$ 为实数，故由 Euler 公式即得引理．

此引理是已知的（见 [3]P.58），由它立刻导出

推论 1.8 $T^n_{r(m)}=T^n_{n-r(m)}$，$T^{n+1}_{r(m)}=T^n_{r(m)}+T^n_{r-1(m)}$

该结果表明 $T^n_{r(m)}$ 类似于组合数 $\binom{n}{r}$．

取代 $T^n_{r(m)}$，以后我们讨论下述函数

$$\Delta_m(k,n)=\begin{cases}mT^n_{\frac{n}{2}+k(m)}-2^n & 若 2\nmid m\\ mT^n_{[\frac{n}{2}]+k(m)}-2^n & 若 2\mid m\end{cases}$$

由推论 1.8 知 $\Delta_m(k,n)$ 具有如下性质：

当 $2\nmid m$ 或 $2\mid n$ 时，$\Delta_m(k,n)=\Delta_m(-k,n)$

当 $2|m$ 且 $2\nmid n$ 时，　$\Delta_m(k,n)=\Delta_m(1-k,n)$　　(1.2)

若 $2\nmid m$, 则 $\Delta_m(k,n)=\Delta_m(\frac{m+1}{2}+k,n-1)+\Delta_m\left(\frac{m-1}{2}+k,n-1\right)$　　(1.3_1)

若$2|m$,则$\Delta_m(k,n)=\Delta_m(k,n-1)+\Delta_m(k+(-1)^n,n-1)$　　(1.3_2)

两次运用 (1.3) 式可得

推论 1.9　$\Delta_m(k,n)=\Delta_m(k+1,n-2)+2\Delta_m(k,n-2)+\Delta_m(k-1,n-2)$

由此推论可以递推计算 $\Delta_m(k,m)$, 但我们有使 k 保持不变的更有用的递推公式 .

定理 1.3　设 $2\nmid m$, $G_{\frac{m-1}{2}}(x)=\prod_{l=1}^{\frac{m-1}{2}}(x+2\cos\frac{2l-1}{m}\pi)=\sum_{s=0}^{\frac{m-1}{2}}a_sx^s$,

则
$$\sum_{s=0}^{\frac{m-1}{2}}a_s\Delta_m(k,n+s)=0\quad(n=0,1,\cdots)$$

证　令 $r\equiv\frac{n}{2}(\mathrm{mod}\ m)$, $sm=n-2r$, 则 n、s 奇偶性相同 . 故由引理 1.3 得

$$T^n_{\frac{n}{2}+k(m)}=T^n_{r+k(m)}=\frac{2^n}{m}\sum_{l=0}^{m-1}\cos^n\frac{\pi l}{m}\cos\frac{\pi l(n-2r-2k)}{m}$$

$$=\frac{2^n}{m}\sum_{l=0}^{m-1}\cos^n\frac{\pi l}{m}\cos(\pi ls-\frac{2\pi lk}{m})$$

$$=\frac{2^n}{m}\sum_{l=0}^{m-1}\cos^n\frac{\pi l}{m}(-1)^{ls}\cos\frac{2\pi lk}{m}$$

$$=\frac{1}{m}\sum_{l=0}^{m-1}\cos\frac{2\pi lk}{m}[2(-1)^l\cos\frac{\pi l}{m}]^n$$

$$\Delta_m(k,n)=mT^n_{\frac{n}{2}+k(m)}-2^n=\sum_{l=1}^{m-1}\cos\frac{2\pi lk}{m}[2(-1)^l\cos\frac{\pi l}{m}]^n$$

$$=\sum_{\substack{l=1\\2\nmid l}}^{m-1}\cos\frac{2\pi lk}{m}(-2\cos\frac{\pi l}{m})^n+\sum_{\substack{l=1\\2|l}}^{m-1}\cos\frac{2\pi(m-l)k}{m}[2(-1)^{m-l}\cos\frac{\pi(m-l)}{m}]^n$$

$$=2\sum_{\substack{l=1\\2\nmid l}}^{m-1}\cos\frac{2\pi lk}{m}(-2\cos\frac{\pi l}{m})^n\qquad(1.4)$$

于是

$$\sum_{s=0}^{\frac{m-1}{2}}a_s\Delta_m(k,n+s)=2\sum_{\substack{l=1\\2\nmid l}}^{m-1}\cos\frac{2\pi lk}{m}\sum_{s=0}^{\frac{m-1}{2}}a_s(-2\cos\frac{\pi l}{m})^{n+s}$$

$$=2\sum_{\substack{l=1\\2\nmid l}}^{m-1}\cos\frac{2\pi lk}{m}(-2\cos\frac{\pi l}{m})^nG_{\frac{m-1}{2}}(-2\cos\frac{\pi l}{m})=0$$

定理证完 .

定理 1.4 设 $2|m$，$Q_{\frac{m}{2}-1}(x)=\prod_{l=1}^{\frac{m}{2}-1}(x-2-2\cos\frac{2\pi l}{m})=\sum_{s=0}^{\frac{m}{2}-1}a_s x^s$，则

$$\sum_{s=0}^{\frac{m}{2}-1}a_s\Delta_m(k,n+2s)=0\quad(n=1,2,\cdots)$$

证 当 $2|n$ 时由引理 1.3 知

$$\Delta_m(k,n)=mT^n_{\frac{n}{2}+k(m)}-2^n=\sum_{l=1}^{m-1}\cos\frac{2\pi lk}{m}(2\cos\frac{\pi l}{m})^n$$

$$=\sum_{l=1}^{\frac{m}{2}-1}\cos\frac{2\pi lk}{m}(2\cos\frac{\pi l}{m})^n+\sum_{l=1}^{\frac{m}{2}-1}\cos\frac{2\pi(m-l)k}{m}(2\cos\frac{m-l}{m}\pi)^n$$

$$+\cos\frac{2\pi\cdot\frac{m}{2}k}{m}(2\cos\frac{\frac{m}{2}\pi}{m})^n$$

故 n 为正偶数时

$$\Delta_m(k,n)=2\sum_{l=1}^{\frac{m}{2}-1}\cos\frac{2\pi lk}{m}(2\cos\frac{\pi l}{m})^n\tag{1.5}$$

$$\sum_{s=0}^{\frac{m}{2}-1}a_s\Delta_m(k,n+2s)=2\sum_{l=1}^{\frac{m}{2}-1}\cos\frac{2\pi lk}{m}\sum_{s=0}^{\frac{m}{2}-1}a_s(2\cos\frac{\pi l}{m})^{n+2s}$$

$$=2\sum_{l=1}^{\frac{m}{2}-1}\cos\frac{2\pi lk}{m}(2\cos\frac{\pi l}{m})^nQ_{\frac{m}{2}-1}(2+2\cos\frac{2\pi l}{m})=0.$$

当 $2\nmid n$ 时由引理 1.3 得

$$\Delta_m(k,n)=mT^n_{\frac{n-1}{2}+k(m)}-2^n=\sum_{l=1}^{m-1}\cos\frac{(2k-1)\pi l}{m}(2\cos\frac{\pi l}{m})^n$$

$$=\sum_{l=1}^{\frac{m}{2}-1}\cos\frac{(2k-1)\pi l}{m}(2\cos\frac{\pi l}{m})^n+\sum_{l=1}^{\frac{m}{2}-1}\cos\frac{(2k-1)\pi(m-l)}{m}(2\cos\frac{m-l}{m}\pi)^n$$

$$+\cos\frac{(2k-1)\pi\frac{m}{2}}{m}(2\cos\frac{\frac{m}{2}\pi}{m})^n$$

$$=2\sum_{l=1}^{\frac{m}{2}-1}\cos\frac{(2k-1)\pi l}{m}(2\cos\frac{\pi l}{m})^n\tag{1.6}$$

同上可知

$$\sum_{s=0}^{\frac{m}{2}-1}a_s\Delta_m(k,n+2s)=0\quad(n=1,3,5,\cdots)$$ 证完.

1.3 $G_n(x)$、$\Delta_5(r,n)$与Fibonacci商

在 § 1.2 中我们导出了 $2\nmid m$ 时 $\Delta_m(k,n)$ 所满足的递推公式，本节就来确定其中的递推系数 .

为此，我们先讨论 Lucas 序列 .

Lucas 序列 $u_n(a,b)$、$v_n(a,b)$ 定义为如下的 u_n、v_n:

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

$$v_0=2,\ v_1=b,\ v_{n+1}=bv_n-av_{n-1}$$

引理 1.4 $u_n(a,b)=\sum_{r=0}^{[\frac{n-1}{2}]}\binom{n-1-r}{r}(-a)^r b^{n-1-2r}$

引理 1.5 设 $b^2-4a\neq 0$，则

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

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

直接验证初值与递推关系便知二引理成立 .

现在能够证明

定理 1.5 设 $G_n(x)=\prod_{l=1}^{n}(x+2\cos\frac{2l-1}{2n+1}\pi)$，则

$$G_n(x)=u_n(1,x)+u_{n+1}(1,x)=\sum_{k=0}^{n}(-1)^{[\frac{n-k}{2}]}\binom{[\frac{n+k}{2}]}{k}x^k$$

证 由引理 1.4 易证后一等式成立 . 又因为 $G_n(x)$ 的 n 个根互不相同，故只需再证

$$u_n(1,-2\cos\frac{2l-1}{2n+1}\pi)+u_{n+1}(1,-2\cos\frac{2l-1}{2n+1}\pi)=0\quad l=1,2,\cdots,n.$$

注意到 $\sqrt{(-2\cos\frac{2l-1}{2n+1}\pi)^2-4}=2i\sin\frac{2l-1}{2n+1}\pi\neq 0$，由引理 1.5 便知 $\theta_l=\frac{2l-1}{2n+1}\pi$ 时

$$u_n(1,-2\cos\theta_l)=\frac{1}{2i\sin\theta_l}\left\{\left(\frac{-2\cos\theta_l+2i\sin\theta_l}{2}\right)^n-\left(\frac{-2\cos\theta_l-2i\sin\theta_l}{2}\right)^n\right\}$$

$$=\frac{(-1)^n}{2i\sin\theta_l}\{(\cos n\theta_l-i\sin n\theta_l)-(\cos n\theta_l+i\sin n\theta_l)\}$$

$$=(-1)^{n-1}\frac{\sin n\theta_l}{\sin\theta_l}\qquad (l=1,2,\cdots,n)$$

故 $u_n(1,-2\cos\theta_l)+u_{n+1}(1,-2\cos\theta_l)=(-1)^n\dfrac{\sin(n+1)\theta_l-\sin n\theta_l}{\sin\theta_l}=0 \quad l=1,2,\cdots,n.$

于是定理获证.

综合定理 1.3 和定理 1.5 可知:

$$\sum_{s=0}^{m}(-1)^{[\frac{m-s}{2}]}\binom{[\frac{m+s}{2}]}{s}\Delta_{2m+1}(k,n+s)=0,\quad n=0,1,2,\cdots \tag{1.7}$$

推论 1.10 $G_n(x)$ 满足如下初值与递推关系.

$$G_0(x)=1,\ G_1(x)=x+1,\ G_{n+1}(x)=xG_n(x)-G_{n-1}(x),\quad n=1,2,\cdots$$

$G_n(x)$的前几个是:

$G_0(x)=1,\ G_1(x)=x+1,\ G_2(x)=x^2+x-1,\ G_3(x)=x^3+x^2-2x-1,$

$G_4(x)=x^4+x^3-3x^2-2x+1,\ G_5(x)=x^5+x^4-4x^3-3x^2+3x+1.$

因 $G_3(x)=x^3+x^2-2x-1$, 故由定理 1.3 知

$$\Delta_7(k,n+3)+\Delta_7(k,n+2)-2\Delta_7(k,n+1)-\Delta_7(k,n)=0,\quad n=0,1,2,\cdots$$

这个递推关系首先为孙智伟获得.

由于$G_2(x)=x^2+x-1$,故有

定理 1.6 设 $L_n=v_n(-1,1)$, 则

$$\Delta_5(0,n)=2(-1)^nL_n,\ \Delta_5(\pm 1,n)=(-1)^nL_{n-1},\ \Delta_5(\pm 2,n)=(-1)^{n+1}L_{n+1}$$

证 由定理 1.3 及 $G_2(x)=x^2+x-1$ 知 ,$\Delta_5(k,n)$ 满足

$$\Delta_5(k,n+2)+\Delta_5(k,n+1)-\Delta_5(k,n)=0,\quad n=0,1,2,\cdots$$

经过简单计算知 :$2(-1)^nL_n$、$(-1)^nL_{n-1}$、$(-1)^{n+1}L_{n+1}$ 分别与 $\Delta_5(0,n)$、$\Delta_5(\pm 1,n)$、$\Delta_5(\pm 2,n)$ 有共同初值 $(4,-2)$、$(-1,-2)$、$(-1,3)$. 又它们递推关系相同 , 所以分别相等.

推论 1.11 设 p 为大于 5 的素数 , 则

(1) $\displaystyle\sum_{k=1}^{[\frac{p}{5}]}\frac{(-1)^{k-1}}{k}\equiv\frac{2^p-5+(\frac{5}{p})L_{p+(\frac{5}{p})}}{p} \pmod p$

(2) 当$r\equiv\dfrac{p}{2}\pmod 5$且$1\leqslant r\leqslant 4$时, $\displaystyle\sum_{k=0}^{[\frac{p-r}{5}]}\frac{(-1)^{5k+r-1}}{5k+r}\equiv\frac{2^p-2L_p}{5p} \pmod p$

证 (1) 据推论 1.1 和定理 1.6, 综合 p mod 5 的四种情况即得.

(2) 由引理 1.1 和 $\Delta_5(0,p)=-2L_p$ 立知.

为从推论 1.11 导出 Fibonacci 商 $F_{p-(\frac{5}{p})}/p$, 需 Lucas 序列的若干引理. 这些引理在以后也是必要的.

引理 1.6　设 a、$b\in\mathbb{Z}$, $(a,b)=1$, p 为奇素数 ,$p\nmid a$, 则

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

参见文 [4] 第 111 页 (3) 式和 (4) 式 , 也可见 [2].

引理 1.7　设 $u_n=u_n(a,b)$, $v_n=v_n(a,b)$, $b^2-4a\neq 0$, 则

(1) $v_n=u_{n+1}-au_{n-1}=bu_n-2au_{n-1}=2u_{n+1}-bu_n$

(2) $u_n=\frac{1}{b^2-4a}(v_{n+1}-av_{n-1})=\frac{1}{b^2-4a}(bv_n-2av_{n-1})=\frac{1}{b^2-4a}(2v_{n+1}-bv_n)$

(3) $u_{2n}=u_nv_n$, $v_n^2-(b^2-4a)u_n^2=4a^n$

(4) $u_{2n+1}=u_{n+1}^2-au_n^2$, $v_{2n}=v_n^2-2a^n$

这些结果都是已知的[2],[4], 也可由引理 1.5 直接验证 .

引理 1.8　设 p 为奇素数 ,$b\in\mathbb{Z}$,$p\nmid(b^2+4)$, 记 $\varepsilon=\left(\frac{b^2+4}{p}\right)$, $u_n=u_n(-1,b)$, 则

(1) $v_{p-\varepsilon}\equiv 2\varepsilon\pmod{p^2}$

(2) $u_{p-\varepsilon}\equiv\frac{2}{\varepsilon b}(u_p-\varepsilon)\equiv\frac{2}{b^2+4}(v_p-b)\pmod{p^2}$

(3) $\varepsilon v_{p+\varepsilon}\equiv b^2+2+\frac{b(b^2+4)}{2}u_{p-\varepsilon}\pmod{p^2}$

证　(1) 由引理 1.6 和引理 1.7 知

当$\varepsilon=1$时, $v_{p-1}=2u_p-bu_{p-1}\equiv 2\pmod p$

当$\varepsilon=-1$时, $v_{p+1}=bu_{p+1}+2u_p\equiv -2\pmod p$

即 $v_{p-\varepsilon}\equiv 2\varepsilon\pmod p$

因 $v_{p-\varepsilon}+2\varepsilon\equiv 4\varepsilon\not\equiv 0\pmod p$, 故由引理 1.6 和 1.7(3) 知

$$v_{p-\varepsilon}=2\varepsilon+\frac{v_{p-\varepsilon}^2-4}{v_{p-\varepsilon}+2\varepsilon}=2\varepsilon+\frac{(b^2+4)u_{p-\varepsilon}^2}{v_{p-\varepsilon}+2\varepsilon}\equiv 2\varepsilon\pmod{p^2}$$

(2)、(3) 由 (1) 和引理 1.7 综合 $\varepsilon=1$ 与 $\varepsilon=-1$ 两种情况即知 .

利用这些引理 , 即可得到 Fibonacci 商 .

定理 1.7　设 p 为大于 5 的素数 ,$F_n=u_n(-1,1)$,$r\in\{1,2,3,4\}$ 且 $r\equiv\frac{p}{2}\pmod 5$, $q_p(2)=\frac{2^{p-1}-1}{p}$, 则

(1) (H.C.Williams[1])　$\frac{F_{p-\left(\frac{5}{p}\right)}}{p}\equiv\frac{2}{5}\sum_{k=1}^{[\frac{p}{5}]}\frac{(-1)^{k-1}}{k}-\frac{4}{5}q_p(2)\pmod p$

(2) $\frac{F_{p-\left(\frac{5}{p}\right)}}{p} \equiv \frac{2}{5} q_p(2) - 2 \sum_{k=0}^{\frac{p-5-2r}{10}} \frac{(-1)^{5k+r-1}}{5k+r} \pmod{p}$

证 (1) 由引理 1.8(3) 知 $\left(\frac{5}{p}\right) L_{p+\left(\frac{5}{p}\right)} \equiv 3 + \frac{5}{2} F_{p-\left(\frac{5}{p}\right)} \pmod{p^2}$，把它代入推论 1.11 的 (1) 式即得所需．

(2) 令 $m = \frac{p-2r}{5}$，则 m 为奇数．故

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

$$= \sum_{k=0}^{\frac{m-1}{2}} \left[\frac{(-1)^{5k+r-1}}{5k+r} + \frac{(-1)^{p+(5k+r)}}{p-(5k+r)} \right] \equiv 2 \sum_{k=0}^{\frac{m-1}{2}} \frac{(-1)^{5k+r-1}}{5k+r} \pmod{p}$$

再由推论 1.11(2) 及引理 1.8(2) 得

$$\sum_{k=0}^{\frac{p-5-2r}{10}} \frac{(-1)^{5k+r-1}}{5k+r} \equiv \frac{1}{2} \sum_{k=0}^{\left[\frac{p-r}{5}\right]} \frac{(-1)^{5k+r-1}}{5k+r} \equiv \frac{2^p - 2L_p}{10p} = \frac{1}{5}\left(\frac{2^{p-1}-1}{p} - \frac{L_p - 1}{p} \right)$$

$$\equiv \frac{1}{5} q_p(2) - \frac{1}{2} \cdot \frac{F_{p-\left(\frac{5}{p}\right)}}{p} \pmod{p}$$

即 $F_{p-\left(\frac{5}{p}\right)} / p \equiv \frac{2}{5} q_p(2) - 2 \sum_{k=0}^{\frac{p-5-2r}{10}} \frac{(-1)^{5k+r-1}}{5k+r} \pmod{p}$ 证完．

在实际计算时，(2) 比 (1) 来得方便．在 (Ⅲ) 中我们将给出 Fibonacci 商的另外形式，其中不出现 Fermat 商，因而更便于计算．

1.4 $Q_n(x)$与$\Delta_6(r,n)$

引理 1.9 $u_m(1,x) = 0$ 的全部根为 $2\cos\frac{\pi}{m}, 2\cos\frac{2\pi}{m}, \cdots, 2\cos\frac{m-1}{m}\pi$.

证 由于 $2\cos\frac{\pi}{m}, \cdots, 2\cos\frac{(m-1)\pi}{m}$ 两两不等，而由引理 1.4 知 $u_m(1,x)$ 为 $m-1$ 次多项式，故只需证

$$u_m\left(1, 2\cos\frac{\pi l}{m}\right) = 0 \quad l = 1, 2, \cdots, m-1.$$

事实上，由引理 1.5

$u_m\left(1, 2\cos\frac{\pi l}{m}\right)$

$$=\frac{1}{\sqrt{-4\sin^2\frac{\pi l}{m}}}\left\{\left(\frac{2\cos\frac{\pi l}{m}+\sqrt{-4\sin^2\frac{\pi l}{m}}}{2}\right)^m-\left(\frac{2\cos\frac{\pi l}{m}-\sqrt{-4\sin^2\frac{\pi l}{m}}}{2}\right)^m\right\}$$

$$=\frac{1}{2i\sin\frac{\pi l}{m}}\{(\cos\frac{\pi l}{m}+i\sin\frac{\pi l}{m})^m-(\cos\frac{\pi l}{m}-i\sin\frac{\pi l}{m})^m\}$$

$$=\frac{1}{2i\sin\frac{\pi l}{m}}[(\cos\pi l+i\sin\pi l)-(\cos\pi l-i\sin\pi l)]=0$$

故引理得证.

引理 1.10 (Lucas[2]) 设 $\{U_n\}$ 满足 $U_{n+1}=bU_n-aU_{n-1}$ $(n=1,2,\cdots)$, 则

$$U_{n+k}=v_k(a,b)U_n-a^kU_{n-k}$$

特别地有 $u_{kn}(a,b)/u_k(a,b)=u_n(a^k,v_k(a,b))$.

定理 1.8 设 $Q_n(x)=\prod_{l=1}^{n}(x-2-2\cos\frac{\pi l}{n+1})$, 则

$$Q_n(x)=u_{n+1}(1,x-2)=x^nu_{2n+2}(\frac{1}{x},1)=\sum_{k=0}^{n}(-1)^{n-k}\binom{n+1+k}{n-k}x^k$$

证 首先由引理 1.9 知 $Q_n(x)=u_{n+1}(1,x-2)$. 其次由引理 1.10 知 $u_{2n+2}(\frac{1}{x},1)=(1-\frac{2}{x})u_{2n}(\frac{1}{x},1)-\frac{1}{x^2}u_{2n-2}(\frac{1}{x},1)$,故

$$x^nu_{2n+2}(\frac{1}{x},1)=(x-2)x^{n-1}u_{2n}(\frac{1}{x},1)-x^{n-2}u_{2n-2}(\frac{1}{x},1)$$

于是 $x^nu_{2n+2}(\frac{1}{x},1)$ 与 $u_{n+1}(1,x-2)$ 满足相同递推关系. 又它们初值相等, 因此

$u_{n+1}(1,x-2)=x^nu_{2n+2}(1/x,1)$ $(n=0,1,\cdots)$.

另一方面, 由引理 1.4 知

$$x^nu_{2n+2}(\frac{1}{x},1)=\sum_{r=0}^{n}\binom{2n+1-r}{r}(-1)^rx^{n-r}=\sum_{k=0}^{n}(-1)^{n-k}\binom{n+1+k}{n-k}x^k$$

故综上定理得证.

由此定理和定理 1.4 可得

$$\sum_{k=0}^{m}(-1)^{m-k}\binom{m+1+k}{m-k}\Delta_{2m+2}(r,n+2k)=0\quad(n=1,2,\cdots)\tag{1.8}$$

$Q_n(x)$ 的前几个是:

$$Q_0(x)=1,\ Q_1(x)=x-2,\ Q_2(x)=x^2-4x+3,$$
$$Q_3(x)=x^3-6x^2+10x-4,\ Q_4(x)=x^4-8x^3+21x^2-20x+5,$$

$$Q_5(x)=x^5-10x^4+36x^3-56x^2+35x-6.$$

因 $Q_2(x)$ 是二次的，故可直接给出 $\Delta_6(k,n)$.

定理 1.9 设 $n\in\mathbb{Z}$，$\Delta_6(k,n)=6T^n_{[\frac{n}{2}]+k(6)}-2^n$，则

(1) 当$2\nmid n$时，$\Delta_6(1,n)=\Delta_6(0,n)=3^{\frac{n+1}{2}}+1$,

$\Delta_6(2,n)=\Delta_6(5,n)=-2$, $\Delta_6(3,n)=\Delta_6(4,n)=1-3^{\frac{n+1}{2}}$

(2) 当$2|n$时，$\Delta_6(0,n)=2\times 3^{\frac{n}{2}}+2$, $\Delta_6(\pm 1,n)=3^{\frac{n}{2}}-1$

$\Delta_6(\pm 2,n)=-3^{\frac{n}{2}}-1$, $\Delta_6(3,n)=2-2\times 3^{\frac{n}{2}}$

证：由 $\Delta_6(k,n+4)=4\Delta_6(k,n+2)-3\Delta_6(k,n)$ $(n=1,2,\cdots)$，固定 k 对 n 归纳即得.

由此定理容易确定 Legendre 符号$\left(\frac{3}{p}\right)$.

推论 1.12 设 p 为大于 3 的素数，则

(1) $\sum_{k=1}^{[\frac{p}{6}]}\frac{1}{k}\equiv -2q_p(2)-\frac{3}{2}q_p(3) \pmod p$

(2) $\sum_{k=0}^{[\frac{p-3}{6}]}\frac{1}{2k+1}\equiv q_p(2)-\frac{3}{4}q_p(3) \pmod p$

(3) $\sum_{k=1}^{[\frac{p+1}{6}]}\frac{1}{3k-1}\equiv -\frac{2}{3}q_p(2)+\frac{1}{2}q_p(3)ct(p\equiv 1(3)) \pmod p$

(4) $\sum_{k=1}^{[\frac{p+3}{6}]}\frac{1}{3k-2}\equiv -\frac{2}{3}q_p(2)+\frac{1}{2}q_p(3)ct(p\equiv 2(3) \pmod p$

证：由定理 1.9、引理 1.1 和推论 1.1 计算可得.

参考文献

1 Williams, H. C., A note on the Fibonacci quotient Fp−ε/p, Canad. Math. Bull., 25(1982),366−370.

2 Dickson, L. E., History of the Theory of Numbers (Vol. I), Chelsea Publishing Company, New York, 1952,105−112,393−407.

3 徐利治等，计算组合数学，上海科学技术出版社，1983.

4 柯召、孙琦，数论讲义(上)，高等教育出版社，1986.

5 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.