《数学学报》中文版 (Acta Math. Sinica Chin. Ser.) **67** (2024), 286–295.

关于一些行列式与积和式

孙智伟

南京大学数学系，邮编 210093
电子邮箱：zwsun@nju.edu.cn

摘要. 本文研究了一些行列式与积和式. 特别地, 我们探讨了新型行列式

$$\det[(i^2+cij+dj^2)^{p-2}]_{0\leqslant i,j\leqslant p-1}\quad 与\quad \det[(i^2+cij+dj^2)^{p-2}]_{1\leqslant i,j\leqslant p-1}$$

模奇素数 p, 其中 c 与 d 为整数. 我们也提出一些猜想以供进一步的研究.

1. 引言

交换环上 n 阶方阵 $A=[a_{i,j}]_{1\leqslant i,j\leqslant n}$ 的行列式与积和式分别由

$$\det(A)=\sum_{\sigma\in S_n}\mathrm{sign}(\sigma)\prod_{i=1}^n a_{i,\sigma(i)}\quad 与\quad \mathrm{per}(A)=\sum_{\sigma\in S_n}\prod_{i=1}^n a_{i,\sigma(i)}$$

给出, 这里 S_n 是由 $\{1,\ldots,n\}$ 上所有置换构成的对称群, 置换 $\sigma\in S_n$ 的符号 $\mathrm{sign}(\sigma)$ 在 σ 是偶置换时取值 1, 在 σ 是奇置换时取值 -1.

对于 $i,j=1,\ldots,n$, 定义

$$p_{ij}=\begin{cases}1 & 如果\ i+j\ 为素数,\\ 0 & 此外.\end{cases}$$

已知 $|\det[p_{ij}]_{1\leqslant i,j\leqslant n}|$ 总为完全平方 (参见 [3]). 我们的下述定理进一步推广了此结果.

定理 1.1. *设 $A=[a_{i,j}]_{1\leqslant i,j\leqslant n}$ 为交换环上的 n 阶方阵, 又设只要 $i+j$ 为大于 2 的偶数就有 $a_{i,j}=0$.*

(i) *如果 $n=2m$ (其中 $m\in\mathbb{Z}^+=\{1,2,3,\ldots\}$), 则*

$$\mathrm{per}(A)=\mathrm{per}[a_{2i,2j-1}]_{1\leqslant i,j\leqslant m}\,\mathrm{per}[a_{2i-1,2j}]_{1\leqslant i,j\leqslant m},\tag{1.1}$$

并且

$$\det(A)=(-1)^m\det[a_{2i,2j-1}]_{1\leqslant i,j\leqslant m}\,\det[a_{2i-1,2j}]_{1\leqslant i,j\leqslant m}.\tag{1.2}$$

(ii) *如果 $n=2m+1$ (其中 $m\in\mathbb{Z}^+$), 则*

$$\mathrm{per}(A)=a_{1,1}\,\mathrm{per}[a_{2i,2j+1}]_{1\leqslant i,j\leqslant m}\,\mathrm{per}[a_{2i+1,2j}]_{1\leqslant i,j\leqslant m},\tag{1.3}$$

关键词: 行列式, 积和式, p 进同余式, Legendre 符号.

2020 数学主题分类号. 11C20, 15A15; 11A07, 11A15.

本工作得到国家自然科学基金面上项目 (项目号 12371004) 的资助.

并且

$$\det(A)=(-1)^m a_{1,1}\det[a_{2i,2j+1}]_{1\leqslant i,j\leqslant m}\det[a_{2i+1,2j}]_{1\leqslant i,j\leqslant m}. \tag{1.4}$$

显然定理 1.1有下述推论.

推论 1.1. 设 $A=[a_{i,j}]_{1\leqslant i,j\leqslant n}$ 为交换环上对称矩阵, 而且 $i+j\in\{2q:\ q=2,3,\ldots\}$ 时 $a_{i,j}=0$.

(i) 如果 n 为偶数, 则

$$\mathrm{per}(A)=\mathrm{per}[a_{2i,2j-1}]^2_{1\leqslant i,j\leqslant n/2},$$

并且

$$(-1)^{n/2}\det(A)=\det[a_{2i,2j-1}]^2_{1\leqslant i,j\leqslant n/2}.$$

(ii) 如果 n 为大于 1 的奇数, 则

$$\mathrm{per}(A)=a_{11}\,\mathrm{per}[a_{2i,2j+1}]^2_{1\leqslant i,j\leqslant (n-1)/2},$$

并且

$$(-1)^{(n-1)/2}\det(A)=a_{1,1}\det[a_{2i,2j-1}]^2_{1\leqslant i,j\leqslant (n-1)/2}.$$

注记 1.1. 根据 B. Cloitre 在链接 [3] 中的评论, 他的一个同事在 2002 年证明了下述结果: 如果 $A=[a_{ij}]_{1\leqslant i,j\leqslant n}$ 为交换环 R 上对称矩阵, 其中 a_{11} 为平方元, 而且 $i+j\in\{2q:\ q=2,3,\ldots\}$ 时 $a_{ij}=0$, 则 $|\det(A)|\in\{r^2:\ r\in R\}$.

对于交换环上 n 阶方阵 $A=[a_{ij}]_{1\leqslant i,j\leqslant n}$, 如果对所有 $i,j=1,\ldots,n$ 都有 $a_{ji}=-a_{ij}$, 则称 A 为斜对称的 (skew-symmetric). 对这样的 n 阶方阵 A, 显然 n 为奇数时 $\det(A)=\mathrm{per}(A)=0$.

定理 1.1也有下述推论.

推论 1.2. 设 $A=[a_{ij}]_{1\leqslant i,j\leqslant 2m}$ 是交换环上的偶数阶斜对称矩阵, 而且 $i+j\in\{2q:\ q=2,3,\ldots\}$ 时总有 $a_{ij}=0$. 那么,

$$\mathrm{per}(A)=(-1)^m\mathrm{per}[a_{2i,2j-1}]^2_{1\leqslant i,j\leqslant m},$$

并且

$$\det(A)=\det[a_{2i,2j-1}]^2_{1\leqslant i,j\leqslant m}.$$

注记 1.2. 根据 Cayley 的一个定理 (参见 [2, 第 23-24 页]), 整数环 $\mathbb{Z}$ 上的偶数阶斜对称矩阵的行列式总是平方数.

设 p 为奇素数, $(\frac{\cdot}{p})$ 为 Legendre 符号. 当 $p\equiv 3\ (\mathrm{mod}\ 4)$ 时, 对任何 $i,j=1,\ldots,(p-1)/2$ 都有 $i^2+j^2\not\equiv 0\ (\mathrm{mod}\ p)$, 作者 [4, 定理 1.4(ii)] 证明了

$$\det\left[\frac{1}{i^2+j^2}\right]_{1\leqslant i,j\leqslant (p-1)/2}\equiv\left(\frac{2}{p}\right)\ (\mathrm{mod}\ p).$$

在 $p\equiv 2\ (\mathrm{mod}\ 3)$ 的情形, 作者 [4, 注记 1.3] 猜测有整数 $x\not\equiv 0\ (\mathrm{mod}\ p)$ 使得

$$\det\left[\frac{1}{i^2-ij+j^2}\right]_{1\leqslant i,j\leqslant p-1}\equiv 2x^2\ (\mathrm{mod}\ p).$$

这在最近被伍海亮、余跃峰与尼贺霞 [5] 所证明. 对任给的整数 $x\not\equiv 0\ (\mathrm{mod}\ p)$, 依 Fermat 小定理显然有 $\frac{1}{x}\equiv x^{p-2}\ (\mathrm{mod}\ p)$.

假设 $P(x,y)\in F[x,y]$, 这里 F 为域. 如果对 $j=1,\ldots,n$ 有

$$P(x,j)=\sum_{k=0}^{n-1}a_{jk}x^k,$$

则由一个已知结果 (参见 [2]) 知

$$\det[P(x_i,j)]_{1\leqslant i,j\leqslant n}=\det[a_{jk}]_{\substack{1\leqslant j\leqslant n\\0\leqslant k<n}}\times\prod_{1\leqslant i<j\leqslant n}(x_j-x_i).$$

因此

$$\deg P<n-1\implies\det[P(i,j)]_{1\leqslant i,j\leqslant n}=0.$$

现在陈述我们的第二个定理.

定理 1.2. 设 $c,d\in\mathbb{Z}$. 对任何素数 $p>3$ 与 $n\in\{(p+1)/2,\ldots,p-2\}$, 我们有

$$\det[(i^2+cij+dj^2)^n]_{0\leqslant i,j\leqslant p-1}\equiv 0\ (\mathrm{mod}\ p).\tag{1.5}$$

注记 1.3. 对于 $p=3$ 与 $c,d\in\mathbb{Z}$, 易见

$$\det[(i^2+cij+dj^2)^{p-2}]_{0\leqslant i,j\leqslant p-1}=\det[i^2+cij+dj^2]_{0\leqslant i,j\leqslant 2}=-4cd.$$

定义 1.1. 对任何 $c,d\in\mathbb{Z}$ 与奇素数 p, 我们让

$$D_p(c,d):=\det[(i^2+cij+dj^2)^{p-2}]_{1\leqslant i,j\leqslant p-1}.\tag{1.6}$$

设 $c,d\in\mathbb{Z}$ 且 p 为奇素数. 考虑到

$$\begin{aligned}&\det[((p-i)^2+c(p-i)j+dj^2)^{p-2}]_{1\leqslant i,j\leqslant p-1}\\=&(-1)^{\sum_{k=1}^{p-2}k}\det[(i^2+cij+dj^2)^{p-2}]_{1\leqslant i,j\leqslant p-1},\end{aligned}$$

我们有

$$D_p(-c,d)\equiv\left(\frac{-1}{p}\right)D_p(c,d)\ (\mathrm{mod}\ p).\tag{1.7}$$

下面给出本文的第三个定理.

定理 1.3. 设 $p>3$ 为素数.

(i) 如果 $p\equiv 3\ (\mathrm{mod}\ 4)$, 则对任何 $c\in\mathbb{Z}$ 有

$$D_p(c,-1)\equiv 0\ (\mathrm{mod}\ p).$$

(ii) 当 $p\equiv 3\ (\mathrm{mod}\ 4)$ 时, 我们有

$$D_p(2,2)\equiv 0\ (\mathrm{mod}\ p).$$

如果 $p\equiv\pm1\pmod{12}$, 则

$$D_p(6,6)\equiv 0\pmod p.$$

我们将在第 2 节与第 3 节中分别证明定理 1.1 与定理 1.2-1.3. 在第 4 节中, 我们将提出关于行列式与积和式的一些猜想.

2. 定理 1.1 的证明

定理 1.1(i) 的证明. 设 $n=2m$, 这里 $m\in\mathbb{Z}^+$. 注意

$$\mathrm{per}(A)=\sum_{\sigma\in S_{2m}}\prod_{i=1}^{2m}a_{i,\sigma(i)}\ \text{且}\ \det(A)=\sum_{\sigma\in S_{2m}}\mathrm{sign}(\sigma)\prod_{i=1}^{2m}a_{i,\sigma(i)}.$$

假设 $\sigma\in S_{2m}$ 且 $\prod_{i=1}^{2m}a_{i,\sigma(i)}\ne0$, 显然有 $\tau_1,\tau_2\in S_m$ 使得对 $i,j=1,\ldots,m$ 都有

$$\sigma(2i)=2\tau_1(i)-1\ \ \text{并且}\ \ \sigma(2j-1)=2\tau_2(j).$$

对 $i=1,\ldots,m$, 令 $\sigma'(i)=\sigma(2i)$ 且 $\sigma'(m+i)=\sigma(2i-1)$. 易见有置换 $\rho\in S_{2m}$ 使得 $\sigma'=\rho\sigma$, 而且 ρ 是 $1+2+\cdots+m$ 个对换的乘积. 因此

$$\mathrm{sign}(\sigma')=(-1)^{m(m+1)/2}\mathrm{sign}(\sigma).$$

注意对 $i=1,\ldots,m$ 有 $\sigma'(i)=2\tau_1(i)-1$ 与 $\sigma'(m+i)=2\tau_2(i)$. 为弄清 σ' 的符号, 我们来考察其逆序对个数的奇偶性. 当 $1\leqslant i<j\leqslant m$ 时,

$$\sigma'(i)>\sigma'(j)\iff 2\tau_1(i)-1>2\tau_1(j)-1\iff\tau_1(i)>\tau_1(j),$$

而且

$$\sigma'(m+i)>\sigma'(m+j)\iff 2\tau_2(i)>2\tau_2(j)\iff\tau_2(i)>\tau_2(j).$$

此外,

$$\begin{aligned}&|\{(i,m+j):\ 1\leqslant i,j\leqslant m\ \text{且}\ \sigma'(i)>\sigma'(m+j)\}|\\&=|\{(i,j):\ 1\leqslant i,j\leqslant m\ \text{且}\ 2\tau_1(i)-1>2\tau_2(j)\}|\\&=|\{(\tau_1(i),\tau_2(j)):\ 1\leqslant i,j\leqslant m\ \text{且}\ 2\tau_1(i)-1>2\tau_2(j)\}|\\&=|\{(s,t):\ 1\leqslant s,t\leqslant m\ \text{且}\ 2s-1>2t\}|=\sum_{s=1}^m\sum_{0<t<s}1=\sum_{s=1}^m(s-1).\end{aligned}$$

因此

$$\mathrm{sign}(\sigma')=(-1)^{\sum_{s=1}^m(s-1)}\mathrm{sign}(\tau_1)\mathrm{sign}(\tau_2)=(-1)^{m(m+1)/2-m}\mathrm{sign}(\tau_1)\mathrm{sign}(\tau_2),$$

从而

$$\mathrm{sign}(\sigma)=(-1)^{m(m+1)/2}\mathrm{sign}(\sigma')=(-1)^m\mathrm{sign}(\tau_1)\mathrm{sign}(\tau_2).$$

于是

$$\prod_{i=1}^{2m}a_{i,\sigma(i)}=\prod_{i=1}^m a_{2i,2\tau_1(i)-1}\times\prod_{j=1}^m a_{2j-1,2\tau_2(j)},$$

并且

$$\operatorname{sign}(\sigma)\prod_{i=1}^{2m}a_{i,\sigma(i)}=(-1)^m\operatorname{sign}(\tau_1)\prod_{i=1}^{m}a_{2i,2\tau_1(i)-1}\times\operatorname{sign}(\tau_2)\prod_{j=1}^{m}a_{2j-1,2\tau_2(j)}.$$

由上,

$$\begin{aligned}\operatorname{per}(A)=&\sum_{\sigma\in S_{2m}}\prod_{i=1}^{2m}a_{i,\sigma(i)}\\=&\Big(\sum_{\tau_1\in S_m}\prod_{i=1}^{m}a_{2i,2\tau_1(i)-1}\Big)\sum_{\tau_2\in S_m}\prod_{j=1}^{m}a_{2j-1,2\tau_2(j)}\\=&\operatorname{per}[a_{2i,2j-1}]_{1\leqslant i,j\leqslant m}\times\operatorname{per}[a_{2i-1,2j}]_{1\leqslant i,j\leqslant m},\end{aligned}$$

并且

$$\begin{aligned}\det(A)=&\sum_{\sigma\in S_{2m}}\operatorname{sign}(\sigma)\prod_{i=1}^{2m}a_{i,\sigma(i)}\\=&(-1)^m\sum_{\tau_1\in S_m}\operatorname{sign}(\tau_1)a_{2i,2\tau_1(i)-1}\sum_{\tau_2\in S_m}\operatorname{sign}(\tau_2)\prod_{j=1}^{m}a_{2j-1,2\tau_2(j)}\\=&(-1)^m\det[a_{2i,2j-1}]_{1\leqslant i,j\leqslant m}\times\det[a_{2i-1,2j}]_{1\leqslant i,j\leqslant m}.\end{aligned}$$

证毕. □

定理 1.1(ii) 的证明. 设 $n=2m+1$, 其中 $m\in\mathbb{Z}^+$. 我们有

$$\operatorname{per}(A)=\sum_{\sigma\in S_{2m+1}}\prod_{i=1}^{2m+1}a_{i,\sigma(i)}\text{ 且 }\det(A)=\sum_{\sigma\in S_{2m+1}}\operatorname{sign}(\sigma)\prod_{i=1}^{2m+1}a_{i,\sigma(i)}.$$

假设 $\sigma\in S_{2m+1}$ 且 $\prod_{i=1}^{2m+1}a_{i,\sigma(i)}\neq0$, 那么

$$\{i+\sigma(i):\ i=1,\ldots,2m+1\}\cap\{2q:\ q=2,\ldots,m\}=\emptyset.$$

如果 $\sigma(1)\neq1$, 则诸 $\sigma(2i+1)$ $(0\leqslant i\leqslant m)$ 为两两不同的偶数, 这与 $|\{2j:\ j=1,\ldots,m\}|<m+1$ 矛盾. 因此 $\sigma(1)=1$. 由于 $\sigma(2i)$ $(1\leqslant i\leqslant m)$ 是两两不同的奇数, 存在 $\tau_1\in S_m$ 使得对 $i=1,\ldots,m$ 都有 $\sigma(2i)=2\tau_1(i)+1$. 考虑到 $\sigma(2i+1)$ $(1\leqslant i\leqslant m)$ 是不同的正偶数, 存在 $\tau_2\in S_m$ 使得对 $i=1,\ldots,m$ 都有 $\sigma(2i+1)=2\tau_2(i)$. 令 $\sigma'(1)=1$, 并对 $i=1,\ldots,m$ 让 $\sigma'(i+1)=\sigma(2i)$ 且 $\sigma'(m+1+i)=\sigma(2i+1)$. 易见有 $\lambda\in S_{2m+1}$ 使得 $\sigma'=\lambda\sigma$, 而且 λ 是 $\sum_{0<k<m}k=m(m-1)/2$ 个对换的乘积. 因此

$$\operatorname{sign}(\sigma')=(-1)^{m(m-1)/2}\operatorname{sign}(\sigma).$$

注意对 $i=1,\ldots,m$ 有 $\sigma'(i+1)=2\tau_1(i)+1$ 与 $\sigma'(m+1+i)=2\tau_2(i)$. 当 $1\leqslant i<j\leqslant m$ 时,

$$\sigma'(i+1)>\sigma'(j+1)\iff2\tau_1(i)+1>2\tau_1(j)+1\iff\tau_1(i)>\tau_1(j),$$

而且

$$\sigma'(m+1+i)>\sigma'(m+1+j)\iff2\tau_2(i)>2\tau_2(j)\iff\tau_2(i)>\tau_2(j).$$

此外,

$$\begin{aligned}
&|\{(i+1,m+1+j):\ 1\leqslant i,j\leqslant m\ \text{且}\ \sigma'(i+1)>\sigma'(m+1+j)\}|\\
&=|\{(i,j):\ 1\leqslant i,j\leqslant m\ \text{且}\ 2\tau_1(i)+1>2\tau_2(j)\}|\\
&=|\{(\tau_1(i),\tau_2(j)):\ 1\leqslant i,j\leqslant m\ \text{且}\ 2\tau_1(i)+1>2\tau_2(j)\}|\\
&=|\{(s,t):\ 1\leqslant s,t\leqslant m\ \text{且}\ 2s+1>2t\}|=\sum_{s=1}^{m}\sum_{t=1}^{s}1=\sum_{s=1}^{m}s.
\end{aligned}$$

因此

$$\operatorname{sign}(\sigma')=(-1)^{\sum_{s=1}^{m}s}\operatorname{sign}(\tau_1)\operatorname{sign}(\tau_2)=(-1)^{m(m-1)/2+m}\operatorname{sign}(\tau_1)\operatorname{sign}(\tau_2),$$

从而

$$\operatorname{sign}(\sigma)=(-1)^{m(m-1)/2}\operatorname{sign}(\sigma')=(-1)^{m}\operatorname{sign}(\tau_1)\operatorname{sign}(\tau_2).$$

注意

$$\prod_{i=1}^{2m+1}a_{i,\sigma(i)}=a_{1,1}\prod_{i=1}^{m}a_{2i,2\tau_1(i)+1}\times\prod_{i=1}^{m}a_{2i+1,2\tau_2(i)},$$

并且

$$\operatorname{sign}(\sigma)\prod_{i=1}^{2m+1}a_{i,\sigma(i)}=(-1)^{m}a_{1,1}\operatorname{sign}(\tau_1)\prod_{i=1}^{m}a_{2i,2\tau_1(i)+1}\times\operatorname{sign}(\tau_2)\prod_{i=1}^{m}a_{2i+1,2\tau_2(i)}.$$

由上可见,

$$\begin{aligned}
\operatorname{per}(A)&=a_{1,1}\Bigg(\sum_{\tau_1\in S_m}\prod_{i=1}^{m}a_{2i,2\tau_1(i)+1}\Bigg)\sum_{\tau_2\in S_m}\prod_{i=1}^{m}a_{2i+1,2\tau_2(i)}\\
&=a_{1,1}\operatorname{per}[a_{2i,2j+1}]_{1\leqslant i,j\leqslant m}\times\operatorname{per}[a_{2i+1,2j}]_{1\leqslant i,j\leqslant m},
\end{aligned}$$

并且

$$\begin{aligned}
\det(A)&=(-1)^{m}a_{1,1}\Bigg(\sum_{\tau_1\in S_m}\operatorname{sign}(\tau_1)\prod_{i=1}^{m}a_{2i,2\tau_1(i)+1}\Bigg)\sum_{\tau_2\in S_m}\operatorname{sign}(\tau_2)\prod_{i=1}^{m}a_{2i+1,2\tau_2(i)}\\
&=(-1)^{m}a_{1,1}\det[a_{2i,2j+1}]_{1\leqslant i,j\leqslant m}\times\det[a_{2i+1,2j}]_{1\leqslant i,j\leqslant m}.
\end{aligned}$$

证毕. □

3. 定理 1.2 与定理 1.3 的证明

定理 1.2 的证明. 对 $i,j=0,\dots,p-1$, 让 $a_{ij}=(i^2+cij+dj^2)^n$. 如果 $p\mid d$, 则对 $j=0,\dots,p-1$ 都有 $a_{0j}\equiv 0\pmod p$, 从而 $\det[a_{ij}]_{0\leqslant i,j\leqslant p-1}\equiv 0\pmod p$.

下面假定 $p\nmid d$. 固定 $j\in\{1,\dots,p-1\}$, 则有

$$\begin{aligned}
4^n\sum_{i=0}^{p-1}a_{ij}&=\sum_{i=0}^{p-1}(4i^2+4cij+4dj^2)^n=\sum_{i=0}^{p-1}((2i+cj)^2+(4d-c^2)j^2)^n\\
&\equiv\sum_{i=1}^{p}(i^2+(4d-c^2)j^2)^n=\sum_{i=1}^{p}\sum_{k=0}^{n}\binom{n}{k}i^{2k}((4d-c^2)j^2)^{n-k}
\end{aligned}$$

$$=\sum_{k=0}^{n}\binom{n}{k}(4d-c^2)^{n-k}j^{2(n-k)}\sum_{i=1}^{p}i^{2k}\ (\mathrm{mod}\ p).$$

显然 $\sum_{i=1}^{p}i^0=p\equiv 0\ (\mathrm{mod}\ p)$. 如果 $k\in\{1,\ldots,p-2\}$ 但 $k\neq(p-1)/2$, 则因 $p-1\nmid 2k$ 有

$$\sum_{i=1}^{p}i^{2k}\equiv\sum_{i=1}^{p-1}i^{2k}\equiv 0\ (\mathrm{mod}\ p)$$

(参见 [1, 第 235 页]). 对于 $k=(p-1)/2$, 根据 Fermat 小定理我们有

$$\sum_{i=1}^{p}i^{2k}\equiv\sum_{i=1}^{p-1}i^{p-1}\equiv\sum_{i=1}^{p-1}1\equiv -1\ (\mathrm{mod}\ p).$$

因此

$$4^n\sum_{i=0}^{p-1}a_{ij}\equiv-\binom{n}{(p-1)/2}(4d-c^2)^{n-(p-1)/2}j^{2(n-(p-1)/2)}\ (\mathrm{mod}\ p),$$

从而利用 Fermat 小定理得

$$\sum_{i=0}^{p-1}a_{ij}\equiv-\left(\frac{j}{2}\right)^{2n}\binom{n}{(p-1)/2}(4d-c^2)^{n-(p-1)/2}\ (\mathrm{mod}\ p).$$

由于 $a_{0j}=(dj^2)^n$, 我们得到

$$\left(1+\frac{(4d-c^2)^{n-(p-1)/2}}{(4d)^n}\binom{n}{(p-1)/2}\right)a_{0j}+\sum_{i=1}^{p-1}a_{ij}\equiv 0\ (\mathrm{mod}\ p). \tag{3.1}$$

考虑到 $2n\not\equiv 0\ (\mathrm{mod}\ p-1)$, 我们有

$$\left(1+\frac{(4d-c^2)^{n-(p-1)/2}}{(4d)^n}\binom{n}{(p-1)/2}\right)a_{00}+\sum_{i=1}^{p-1}a_{i0}=\sum_{i=1}^{p-1}i^{2n}\equiv 0\ (\mathrm{mod}\ p).$$

将此与上一段相结合, 我们得到

$$\left(1+\frac{(4d-c^2)^{n-(p-1)/2}}{(4d)^n}\binom{n}{(p-1)/2}\right)a_{0j}+\sum_{i=1}^{p-1}a_{ij}\equiv 0\ (\mathrm{mod}\ p)\quad(j=0,\ldots,p-1).$$

故有所要结果

$$\det[a_{ij}]_{0\leqslant i,j\leqslant p-1}\equiv 0\ (\mathrm{mod}\ p).$$

综上, 定理 1.2获证. □

定理 1.3 的证明. (i) 假设 $p\equiv 3\ (\mathrm{mod}\ 4)$. 任给 $c\in\mathbb{Z}$, 借助(1.7)我们得到

$$\begin{aligned}D_p(c,-1)&=\det[(j^2+cij-i^2)^{p-2}]_{1\leqslant i,j\leqslant p-1}\\&=\det[-(i^2-cij-j^2)^{p-2}]_{1\leqslant i,j\leqslant p-1}=D_p(-c,-1)\\&\equiv\left(\frac{-1}{p}\right)D_p(c,-1)=-D_p(c,-1)\ (\mathrm{mod}\ p),\end{aligned}$$

因此 $D_p(c,-1)\equiv 0\ (\mathrm{mod}\ p)$.

(ii) 假设 $c,d\in\mathbb{Z}$ 且 $p\nmid d(c^2-4d)$. 根据 $n=p-2$ 时的(3.1)、Fermat 小定理以及同余式

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

对任何 $j=1,\ldots,p-1$ 我们有

$$\begin{aligned}\sum_{i=1}^{p-1}(i^2+cij+dj^2)^{p-2}&\equiv-\left(1+\frac{(4d-c^2)^{(p-3)/2}}{(4d)^{p-2}}\binom{p-2}{(p-1)/2}\right)(dj^2)^{p-2}\\&\equiv-\left(1+\frac{4d}{4d-c^2}\left(\frac{4d-c^2}{p}\right)\frac{1}{2}\binom{p-1}{(p-1)/2}\right)\frac{1}{dj^2}\\&\equiv\left(\frac{2d}{c^2-4d}\left(\frac{c^2-4d}{p}\right)-1\right)\frac{1}{dj^2}\pmod p.\end{aligned}$$

因此

$$\frac{c^2-4d}{2d}\equiv\left(\frac{c^2-4d}{p}\right)\pmod p\Longrightarrow D_p(c,d)\equiv0\pmod p.$$

于是, $p\equiv3\pmod4$ 时 $D_p(2,2)\equiv0\pmod p$, 当 $p\equiv\pm1\pmod{12}$ 时 $D_p(6,6)\equiv0\pmod p$.

综上, 我们证明了定理 1.3. □

4. 一些猜想

受前几节工作的启发, 基于计算我们提出下述猜想.

猜想 4.1. 设 $n>3$ 为奇数, $c,d\in\mathbb{Z}$, 且 Jacobi 符号 $(\frac{d}{n})$ 等于 -1, 则

$$\det[(i^2+cij+dj^2)^{n-2}]_{0\leqslant i,j\leqslant n-1}\equiv0\pmod{n^2}.$$

猜想 4.2. 对于素数 $p\equiv1\pmod4$, 如果还有 $p\equiv\pm2\pmod5$, 则

$$\left(\frac{D_p(1,-1)}{p}\right)=1.$$

猜想 4.3. 任给奇素数 p, 我们有

$$\left(\frac{D_p(2,-1)}{p}\right)=-1\iff p\equiv5\pmod8.$$

猜想 4.4. 对于奇素数 $p\equiv\pm2\pmod5$, 我们有

$$\left(\frac{D_p(3,1)}{p}\right)=\begin{cases}(\frac{6}{p})&\text{如果 }p\equiv1\pmod4,\\0&\text{如果 }p\equiv3\pmod4.\end{cases}$$

猜想 4.5. 设 $p>3$ 为素数, $(\frac{p}{7})=-1$ 且 $p\not\equiv15\pmod{16}$, 则

$$\left(\frac{D_p(1,16)}{p}\right)=\left(\frac{-2}{p}\right).$$

猜想 4.6. 设 p 为素数. 如果 $p\equiv5\pmod{24}$, 则 $D_p(6,6)$ 不是 p 的倍数. 如果 $p\equiv19\pmod{24}$, 则 $D_p(6,6)$ 不是模 p 的平方非剩余.

对正整数 n, 让 $D(n)$ 表示所有 $1,\ldots,n$ 的错位排列构成的集合, 亦即,

$$D(n)=\{\tau\in S_n:\ \text{对任何}j=1,\ldots,n\text{都有}\tau(j)\neq j\}.$$

猜想 4.7. 对任何奇素数 p, 我们有

$$\sum_{\tau\in D(p-1)}\prod_{j=1}^{p-1}\frac{1}{j-\tau(j)}\equiv\left(\frac{-1}{p}\right)\pmod{p^2},$$

并且

$$\sum_{\tau\in D(p-1)}\mathrm{sign}(\tau)\prod_{j=1}^{p-1}\frac{1}{j-\tau(j)}\equiv 1\pmod{p^2}.$$

猜想 4.8. (i) 对任何奇素数 p, 我们有

$$\sum_{\tau\in D(p-1)}\prod_{j=1}^{p-1}\frac{j+\tau(j)}{j-\tau(j)}\equiv 1-2\left(\frac{-1}{p}\right)\pmod{p}.$$

(ii) 任给素数 $p>3$,

$$\frac{1}{p^{3-(\frac{-1}{p})}}\sum_{\tau\in D(p-1)}\mathrm{sign}(\tau)\prod_{j=1}^{p-1}\frac{j+\tau(j)}{j-\tau(j)}$$

是模 p 的平方剩余.

为方便起见, 我们约定空乘积 $\prod_{i\in\emptyset}a_i$ 取值 1.

猜想 4.9. 设 p 为奇素数, 则

$$\sum_{\tau\in S_{p-1}}\prod_{\substack{j=1\\ \tau(j)\neq j}}^{p-1}\frac{1}{j-\tau(j)}\equiv 1+\left(\frac{-1}{p}\right)\pmod{p},$$

当 $p\equiv 3\pmod 4$ 时还有

$$\sum_{\tau\in S_{(p-1)/2}}\prod_{\substack{j=1\\ \tau(j)\neq j}}^{(p-1)/2}\frac{1}{j^2-\tau(j)^2}\equiv 1\pmod{p}.$$

猜想 4.10. 设 p 为奇素数, 则

$$\sum_{\tau\in S_p}\prod_{\substack{j=1\\ \tau(j)\neq j}}^{p}\frac{j+\tau(j)}{j-\tau(j)}\equiv 1-\left(\frac{-1}{p}\right)\pmod{p},$$

并且

$$\sum_{\tau\in S_p}\mathrm{sign}(\tau)\prod_{\substack{j=1\\ \tau(j)\neq j}}^{p}\frac{j+\tau(j)}{j-\tau(j)}\equiv-\frac{p}{2}\pmod{p^2}.$$

猜想 4.11. (i) 任给素数 p, 我们有

$$\sum_{\tau\in S_{p-1}}\prod_{\substack{j=1\\ \tau(j)\neq j}}^{p-1}\frac{j+\tau(j)}{j-\tau(j)}\equiv((p-2)!!)^2\pmod{p^2}.$$

(ii) 如果 p 为奇素数, 则

$$\sum_{\tau\in S_{p-1}}\mathrm{sign}(\tau)\prod_{\substack{j=1\\ \tau(j)\neq j}}^{p-1}\frac{j+\tau(j)}{j-\tau(j)}\equiv\frac{(-1)^{(p+1)/2}}{p-2}((p-2)!!)^2\pmod{p^2}.$$

猜想 4.12. 设 $p>3$ 为素数. 如果 $p\equiv 3\pmod 4$, 则

$$\sum_{\tau\in S_{(p-1)/2}}\mathrm{sign}(\tau)\prod_{\substack{j=1\\ \tau(j)\neq j}}^{(p-1)/2}\frac{j^2+\tau(j)^2}{j^2-\tau(j)^2}\equiv 0\pmod{p^2}.$$

当 $p\equiv 7\pmod 8$ 时, 我们有

$$\sum_{\tau\in S_{(p-1)/2}}\mathrm{sign}(\tau)\prod_{\substack{j=1\\ \tau(j)\neq j}}^{(p-1)/2}\frac{j^2+\tau(j)^2}{j^2-\tau(j)^2}\equiv 0\pmod{p^3}.$$

参考文献

[1] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, 2nd Edition, Grad. Texts. Math., vol. 84, Springer, New York, 1990.

[2] C. Krattenthaler, *Advanced determinant calculus*, Séminaire Lotharingien Combin. 42 (1999), Article B42q, 67pp.

[3] S. Spadaro, Sequence A069191 at OEIS (The On-Line Encyclopedia of Integer Sequences), 2002. `http://oeis.org/A069191`

[4] Z.-W. Sun, *On some determinants with Legendre symbol entries*, Finite Fields Appl. **56** (2019), 285–307.

[5] H.-L. Wu, Y.-F. She and H.-X. Ni, *A conjecture of Zhi-Wei Sun on determinants over finite fields*, Bull. Malays. Math. Sci. Soc. **45** (2022), 2405–2412.

On Some Determinants and Permanents

Zhi-Wei Sun

Department of Mathematics, Nanjing University, Nanjing 210093, P.R. China

Abstract

In this paper we study some determinants and permanents. In particular, we investigate the new-type determinants

$$\det[(i^2+cij+dj^2)^{p-2}]_{0\leqslant i,j\leqslant p-1}\quad\text{and}\quad\det[(i^2+cij+dj^2)^{p-2}]_{1\leqslant i,j\leqslant p-1}$$

modulo an odd prime p, where c and d are integers. We also pose some conjectures for further research.