arXiv:2603.02373v1 [math.NT] 2 Mar 2026

勒让德-17带符号分拆数的周期性消失

TAYLOR DANIELS

摘要。对于 $f\colon \mathbb{N}\to\{0,\pm1\}$， f-带符号分拆数 $\mathfrak{p}(n,f)$ 定义为加权分拆和

$$\mathfrak{p}(n,f)=\sum_{\substack{x_1+\cdots+x_k=n\\ x_1\geq\cdots\geq x_k>0\\ k\geq1}} f(x_1)f(x_2)\cdots f(x_k).$$

对于素数 $p>2$，令 $\left(\frac{\cdot}{p}\right)$ 表示模 p 的勒让德符号。

本文前半部分推导了满足 $p\equiv1$（模 4）的 $p<24$（即 $p=5$、13、17）对应的量 $\mathfrak{p}(n,\pm\left(\frac{\cdot}{p}\right))$ 的拉德马赫型级数公式，并在推导中揭示了对一般 $p\equiv1$（模 4）的推广。本文后半部分利用 $\mathfrak{p}(n,\pm\left(\frac{\cdot}{17}\right))$ 的级数公式，以及戴德金和及其“特征扭曲”类比的若干性质，证明这两个量在某些（模 34）算术级数上恒为零。

1 引言

给定 $n\in\mathbb{N}$ 的分拆是满足 $x_1+\cdots+x_k=n$ 且 $x_1\geq\cdots\geq x_k>0$ 的整数元组 $(x_1,\ x_2,\ \ldots,\ x_k)$，其中 $k\geq1$ 不受限制。对于给定的 $f\colon \mathbb{N}\to\{0,\pm1\}$，我们将 f-带符号分拆数 $\mathfrak{p}(n,\ f)$ 定义为“加权”分拆和

$$\mathfrak{p}(n,f):=\sum_{\substack{x_1+\cdots+x_k=n\\ x_1\geq\cdots\geq x_k>0\\ k\geq1}} f(x_1)f(x_2)\cdots f(x_k).$$

换言之，对于固定的 n，对 n 的任意分拆 $\pi=(x_1,\ \cdots,\ x_k)$，我们赋予其符号 $f(\pi):=f(x_1)\cdots f(x_k)$，而 $\mathfrak{p}(n,\ f)$ 就是对 n 的所有分拆求和所得的 $\sum_\pi f(\pi)$，其中 π 遍历这些分拆。等价地，也可以通过级数展开来定义 $\mathfrak{p}(n,\ f)$

$$\prod_{n\geq1}(1-f(n)x^n)^{-1}=1+\sum_{n\geq1}\mathfrak{p}(n,f)x^n\qquad(\text{for complex }|x|<1).$$

对于素数 $p>2$，勒让德符号分拆数是指数量 $\mathfrak{p}(n,\pm\left(\frac{\cdot}{p}\right))$，其中 $\left(\frac{\cdot}{p}\right)$ 是模 p 的勒让德符号：也就是说，若 $p\nmid a$，则当 a 模 p 同余于一个平方时，$\left(\frac{a}{p}\right)$ 为 1（否则为 -1），而当 $p|a$ 时，$\left(\frac{a}{p}\right)=0$。本文中，$\chi$ 表示模某个 $p>2$ 的勒让德符号 $\left(\frac{\cdot}{p}\right)$。

2020 数学主题分类。 主要分类：11P82, 11P55.关键词和短语：分拆、勒让德符号、消失系数。

勒让德符号分拆数 $\mathfrak{p}(n,\chi)$ 由 [7], 引入，其中考察了不同 $\mathfrak{p}(n,\chi)$ 在 $n\to\infty$ 时的行为。例如，推论 1.4 和 1.6表明：对于 $p\neq 5$ 满足 $p\not\equiv 1$ (模 8)，当 $n\to\infty$ 时，有

$$\mathfrak{p}(n,\chi)\asymp n^{c_p}\exp\left(\tfrac{1}{2}\kappa_p\sqrt{n}\right)$$

对于某个常数 c_p，其中 $a_n\asymp b_n$ 表示 $a_n=O(b_n)$ 且 $b_n=O(a_n)$，并且

$$\kappa_p:=\pi\sqrt{\tfrac{2}{3}(1-\tfrac{1}{p})}.$$

特别地，对于满足 $p\not\equiv 1$ (模 8) 的 $p\neq 5$，有

$$\mathfrak{p}(n,\chi)\to\infty \qquad \text{as } n\to\infty. \tag{1.1}$$

For 比较而言，我们回顾“普通”分拆数 $\mathfrak{p}(n,1)$ sati sfy

$$\mathfrak{p}(n,1)\sim\left(4\sqrt{3}n\right)^{-1}\exp\left(\kappa\sqrt{n}\right) \qquad \text{with } \kappa=\pi\sqrt{\tfrac{2}{3}},$$

如所示 由哈代和拉马努金 [11], ，其中 $a_n\sim b_n$ 表示 $\frac{a_n}{b_n}\to 1$ 随 $n\to\infty$.

.....的情形 $\mathfrak{p}(n,\ \pm(\frac{\cdot}{5}))$ 与（1.1）形成了令人惊讶的对比。也就是说，如[6],所示，有

$$\mathfrak{p}\left(n,(\tfrac{\cdot}{5})\right)=0 \quad \text{for all } n\equiv 2 \pmod{10}, \tag{1.2}$$

$$\mathfrak{p}\left(n,-(\tfrac{\cdot}{5})\right)=0 \quad \text{for all } n\equiv 6 \pmod{10}. \tag{1.3}$$

鉴于（1.1）–（1.3），自然会想到，哪些满足 $p\equiv 1$ (模 8)的素数（如果存在）也会使量 $\mathfrak{p}(n,\ \pm\chi)$出现周期性消失。在计算 $\mathfrak{p}(n,\ \pm\chi)$ 时，对于$n\le 10000$ 以及素数 $p\le 2000$，只发现了唯一的“候选” $p=17$；本文严格证明了这些经验性消失现象，适用于 $\mathfrak{p}(n,\ \pm(\frac{\cdot}{17}))$，具体陈述如下两个定理。

定理 1.1。有

$$\mathfrak{p}\left(n,(\tfrac{\cdot}{17})\right)=0 \qquad \textit{for all } n\equiv 17,19,25,27 \pmod{34}. \tag{1.4}$$

等价地，只要 n 为奇数且 $-1-24n$ 模 *17* 是四次剩余，就有 $\mathfrak{p}(n,(\frac{\cdot}{17}))=0$。

定理 1.2。有

$$\mathfrak{p}\left(n,-(\tfrac{\cdot}{17})\right)=0 \qquad \textit{for all } n\equiv 11,15,29,33 \pmod{34}. \tag{1.5}$$

等价地，当 n 为奇数且 $1-24n$ 模 *17* 同余于一个二次非四次剩余时，有 $\mathfrak{p}(n,-(\frac{\cdot}{17}))=0$。

定理 1.1 和 1.2 的证明首先通过计算得到 $\mathfrak{p}(n,\pm(\frac{\cdot}{17}))$的拉德马赫型级数公式，随后证明级数系数中出现的克洛斯特曼型和在指定的模 34 剩余类上消失。在证明过程中，我们发现了有力证据支持以下猜想，而数值实验也印证了这一点：

使 $p>2$ 在某些模 $\mathfrak{p}(n,\pm(\frac{\cdot}{p}))$ 算术级数上消失的唯一素数 $2p$ (按（1.2）–（1.5）的含义）是5和17。

本文的结构。本文的前半部分，即第3–7节，遵循 Rademacher $\mathfrak{p}(n,(\frac{\cdot}{p}))$ 和 Lehner [18] 的经典技巧，推导出其精确级数公式 [13]。后半部分的大部分内容，即第8–14节，考察级数 $\mathfrak{p}(n,(\frac{\cdot}{p}))$系数的一些性质，最终导向定理1.1的证明。这些后续章节讨论了戴德金和及其“χ-扭曲”类似物的大量基本性质。

第 15节给出了定理 1.2 的简略证明，最后，第 16 节汇集了一些关于由 p 模 8 的剩余所确定的组合量的初等引理（在本文其他部分使用）。

本文的范围。 我们使用经典方法推导 $\mathfrak{p}(n,\ \pm\chi)$ 的级数公式，并且在我们的证明中可以明显看出将其推广到一般的 $p\equiv 1$ (模 4) 的方式。另一方面，即使在我们的简单情形中，这些公式在记号和范围上也存在明显的“扩张”——一般公式则更加复杂。因此，为了在一般性与简洁性之间取得折中，并且出于我们对 $\mathfrak{p}(n,\ \pm(\frac{\cdot}{17}))$ 的特别兴趣，本文始终只考虑

$$p\quad\text{such that}\quad p<24\quad\text{and}\quad p\equiv 1\ (\mathrm{mod}\ 4).$$

致谢。 我们感谢 Trevor Wooley 在本研究过程中进行的多次有益讨论，也感谢 Ben McReynolds 在本研究部分阶段提供的部分经费支持。此外，还要感谢 Nicolas Robles 协助开展本工作的早期阶段，并感谢Anurag Sahay 对本文部分内容进行细致校对。

2 记号与定义

正如读者所知（或者可以想象），生成函数的泰勒级数（按照 Rademacher [18] 的方法）需要大量——通常是噩梦般的——记号（例如参见 [9, 12, 13]）。为了避免进一步的“膨胀”，我们采用了一些记号（包括标准记号和非标准记号），希望在简洁性、清晰性以及与更广泛文献的一致性之间取得平衡。

除非另有说明，本文始终令 p 为素数，且 $p<24$ 和 $p\equiv 1$（模 4）。我们用 χ 表示一般的勒让德符号 $(\frac{\cdot}{p})$；当 p 固定时，我们写作 χ_a 表示 $(\frac{a}{p})$；除诸如 $\mathfrak{p}(n,\ (\frac{\cdot}{p}))$ 这样的表达式外，我们不使用“带括号”的分数来表示勒让德符号。此外，本文始终

$$q=\frac{p-1}{2},\tag{2.1}$$

除非另有说明。

“二次剩余”和“非二次剩余”这两个称谓分别是“二次剩余”和“二次非剩余”的缩写；而诸如“x 是模 p 的二次剩余”之类的表述，应理解为“x 模 p [同余于]，且 [是模 p 的二次] 剩余”。

对于整数 a 与 k，在 $k\geq 1$ 的条件下，令 $\{a\}_k$ 表示满足下述条件的唯一整数

$$a\equiv\{a\}_k\ (\mathrm{mod}\ k)\qquad\text{and}\qquad 0\leq\{a\}_k<k.\tag{2.2}$$

此外，对于 $k \geq 1$，通过如下方式定义 $\|a\| = \|a\|_k$

$$\|a\|_k = \begin{cases} \{a\}_k, & 0 \leq \{a\}_k \leq \frac{k}{2}, \\ k - \{a\}_k, & \frac{k}{2} \leq \{a\}_k < k, \end{cases} \tag{2.3}$$

从而

$$a \equiv \pm \|a\|_k \pmod{k} \qquad \text{and} \qquad 0 \leq \|a\|_k \leq \tfrac{k}{2}. \tag{2.4}$$

粗体字母 $\mathbf{a}$ 表示 $\{1, \dots, \frac{p-1}{2}\}$ 的子集，且包含 $|\mathbf{a}|$ 个元素。诸如 $\sum_{\mathbf{a}} a^2$ 和 $\prod_{\mathbf{a}} \cos(\pi a)$ 这样的和与乘积，均表示对 $\mathbf{a}$ 中的 a 求和或求积；而诸如 $\|h\mathbf{a}\|$ 这样的表达式，则理解为 $\{\|ha\| : a \in \mathbf{a}\}$。对于固定的 p，我们用 $\mathbf{r}$ 和 $\mathbf{s}$ 分别表示 $\{1, \dots, \frac{p-1}{2}\}$ 中包含二次剩余和非二次剩余（模 p）的子集，但在第16节中，我们必须稍微滥用这一记号。

对于复数 z 和 q，且满足 $|q| < 1$，我们使用标准的 q-波赫哈默 符号

$$(z;q)_\infty = \prod_{n=0}^{\infty} (1 - zq^n) \qquad \text{and} \qquad (z_1, \dots, z_k; q)_\infty = \prod_{m=1}^{k} (z_m; q)_\infty.$$

关系 $a_n \ll b_n$ 表示当 $n \to \infty$ 时，$a_n = O(b_n)$。涉及 ε 的此类不等式，均理解为对任意 $\varepsilon > 0$ 成立，其隐含常数依赖于 ε。

一些重要记号。这里说明两个常用记号，以免它们引起混淆，因此在开篇时先予以强调。

(1) 在本文中，h、k、H 和 K 始终是正整数，并且总有一个 as

$$H = hp \qquad \text{and} \qquad K = kp.$$

因此，H 和 K 始终能被 p整除，但 h和 k 并不先验地与 p互素。

(2) 对于 $k \geq 1$,

$$\sum_{h\,(k)} \text{ abbreviates } \sum_{h=0}^{k-1}, \qquad \text{and} \qquad \sum_{h\,(k)}{}' \text{ abbreviates } \sum_{\substack{h=0 \\ (h,k)=1}}^{k-1}. \tag{2.5}$$

因此，和式 $\sum_{h(k)}$ 并不总是等价于 $\sum_{h \text{ (模 } k)}$。

对于实数 x，表达式 $((x))$ 表示经典戴德金和中出现的标准“锯齿”函数，即

$$((x)) = x - \lfloor x \rfloor - \tfrac{1}{2} + \tfrac{1}{2}\delta(x), \qquad \text{where} \qquad \delta(x) = \mathbb{1}_{\mathbb{Z}}(x). \tag{2.6}$$

定义 2.1. 对于一般的 $p \equiv 1$ **(模 4)** 和整数 $k \geq 1$，令 $\varphi := {}^{p}\!/_{(k,\ p)}$，使得 $\varphi k = \operatorname{lcm}(k,\ p)$。那么，对于 $\mathbf{a} \subset \{1, \dots, \frac{p-1}{2}\}$，定义

$$\omega_{\mathbf{a}}(h,k) = \exp\Bigg\{ \pi i \sum_{a \in \mathbf{a}} \sum_{\substack{\mu\,(\varphi k) \\ \mu \equiv \pm a \pmod{p}}} \Big(\!\Big(\frac{h\mu}{k}\Big)\!\Big) \Big(\!\Big(\frac{\mu}{\varphi k}\Big)\!\Big) \Bigg\}. \tag{2.7}$$

容易证明[1]：对于任意整数值 $h,\ k,\ q \geq 1$，有

$$\omega_{\mathbf{a}}(qh, qk) = \omega_{\mathbf{a}}(h,k). \tag{2.8}$$

定义 2.2。 对于固定的 p 以及 $h,\ k\geq 1$，令

$$\phi_{h,k}:=\omega_{\mathbf{r}}(h,k)\frac{\omega_{\mathbf{s}}(2h,k)}{\omega_{\mathbf{s}}(h,k)}. \tag{2.9}$$

由于 $\mathbf{r}\cup(p-\mathbf{r})$ 和 $\mathbf{s}\cup(p-\mathbf{s})$ 分别穷尽了 $\{1,\dots,p-1\}$ 中的二次剩余和非二次剩余（模 p），不难看出

$$\phi_{h,k}=\exp\Big\{\sum_{\substack{\mu\,(\varphi k)\\ \chi_\mu=1}}\Big(\Big(\frac{h\mu}{k}\Big)\Big)\Big(\Big(\frac{\mu}{\varphi k}\Big)\Big)+\sum_{\substack{\mu\,(\varphi k)\\ \chi_\mu=-1}}\Big[\Big(\Big(\frac{2h\mu}{k}\Big)\Big)-\Big(\Big(\frac{h\mu}{k}\Big)\Big)\Big]\Big(\Big(\frac{\mu}{\varphi k}\Big)\Big)\Big\}, \tag{2.10}$$

这里再次有 $\varphi=\ ^{p}\!/_{(k,p)}$。 对于整数 a 和固定的 p，令

$$\mathcal{B}_a:=6\{a\}_p^2-6p\{a\}_p+p^2. \tag{2.11}$$

我们注意到，如果 $\beta_2(x)$ 是第二个周期伯努利函数，即

$$\beta_2(x):=\begin{cases}x^2-x+\frac{1}{6}, & 0\leq x<1,\\ \beta_2(x-\lfloor x\rfloor) & \text{otherwise},\end{cases}$$

then

$$\mathcal{B}_a=6p^2\beta_2(a/p).$$

3 函数方程

固定 $p\equiv 1$（模 4），对于复数 $|x|<1$，我们将 $\Phi(x)$ 定义为 $\mathfrak{p}(n,\chi)$ 的生成函数，即

$$\Phi(x):=\prod_{a=1}^{p-1}(\chi_a x^a;x^p)^{-1}=1+\sum_{n\geq 1}\mathfrak{p}(n,\chi)x^n. \tag{3.1}$$

我们推导 $\mathfrak{p}(n,\ \chi)$ 的级数公式的第一步，是收集关于 $\Phi(x)$ 的若干“函数方程”，其中 x 位于单位圆盘 $|x|<1$ 的不同区域。

定义 3.1。对于一个 $\subset\{1,\dots,\ ^{p-1}\!/_{2}\}$ 和 $|x|<1$，令

$$F_{\mathbf{a}}(x):=\prod_{\mathbf{a}}(x^a,x^{p-a};x^p)_\infty^{-1}\qquad\text{and}\qquad G_{\mathbf{a}}(x):=\prod_{\mathbf{a}}(-x^a,-x^{p-a};x^p)_\infty^{-1}. \tag{3.2}$$

比较（3.1）和（3.2），并回想$\mathbf{r}$ 和$\mathbf{s}$ 分别是 $\{1,\dots,\ ^{p-1}\!/_{2}\}$中模 p的二次剩余与非二次剩余子集，显然有

$$\Phi(x)=F_{\mathbf{r}}(x)G_{\mathbf{s}}(x)=F_{\mathbf{r}}(x)\frac{F_{\mathbf{s}}(x^2)}{F_{\mathbf{s}}(x)}. \tag{3.3}$$

鉴于此，要推导 $\Phi(x)$ 的函数方程，我们只需找出 $F_{\mathbf{a}}(x)$ 和 $G_{\mathbf{a}}(x)$ 的函数方程。这些推导由 Lehner [13]和 Hagis Jr. [9,10], 完成，而关于 $\Phi(x)$ 的方程则可通过一番繁琐的整理计算得出。

[1]证明与 [20, 定理 1] 的证明类似。

对于满足 $(h,k)=1$ 的 $0<h\le k$，以及满足 $\operatorname{Re} z>0$ 的复数 z，记

$$x=\exp\bigl(2\pi ih/k-2\pi z/k\bigr). \tag{3.4}$$

Wr采用这种方式，我们关于 $\Phi(x)$的函数方程具有如下共同形式

$$\Phi(x)=\lambda_k\phi_{h,k}\exp(\psi_{h,k}(z))\Omega_{h,k}(\tilde{x}), \tag{3.5}$$

其中

(1) λ_k 是有限个余割项的商；(2) $\phi_{h,\,k}$ 是（2.9）中定义的单位根；(3)，$_k$ 是某个初等函数；(4) $\Omega_{h,\,k}$ 是解析函数（复数 $|x|<1$）；(5) $\tilde{x}$ 是一个“变换后”的点，它取决于 x （通过 h、 k和 z）以及 $\gcd(k,\ 2p)$。

Lehner 和 Hagis Jr. 将他们版本的（3.5）分为四种情形，依据的是 $\gcd(k,2p)$。然而，我们还必须根据 h 和 k 模 p的二次剩余性来区分上述每种情形，因而总共有 八种情形。为了陈述这些方程，我们不得不（遗憾地）使用大量记号。

在本节余下部分，我们假设 $(h,\ k)=1$ （不对 $(h,\ p)$ 或 $(k,\ p)$ 作任何假设），并回顾

$$q=\frac{p-1}{2}.$$

此外，给定 $(h,\ k)=1$，我们固定 $\bar{2}$、 $\bar{h}$ 和 $\bar{H}$（仅当 $p\nmid k$ 时），使其满足

$$2\bar{2}\equiv h\bar{h}\equiv H\bar{H}\equiv 1\pmod{k}.$$

当 $p|k$ 的情形。设 $p|k$ 且 $(h,\ k)=1$，因此 $\chi_h\neq 0$。

(1) 当 $2p|k$ 时，有

$$\Phi(x)=\phi_{h,k}\exp\Bigl\{\frac{\pi q}{6k}\bigl(-z^{-1}+z\bigr)\Bigr\}\times\begin{cases}R^+(x') & \text{if } \chi_h=+1,\\ R^-(x') & \text{if } \chi_h=-1,\end{cases} \tag{3.6}$$

其中

$$x'=\exp\bigl(-2\pi i\bar{h}/k-2\pi/kz\bigr), \tag{3.6i}$$

and

$$R^{\pm}(x):=\prod_{\mathbf{r}}(\pm x^r,\pm x^{p-r};x^p)_\infty^{-1}\prod_{\mathbf{s}}(\mp x^s,\mp x^{p-s};x^p)_\infty^{-1}. \tag{3.6ii}$$

(2) 当 $(k,\ 2p)=p$ 时，经过一些基本的代数运算可得

$$\begin{aligned}\Phi(x)=\phi_{h,k}\exp\Bigl\{\frac{\pi q}{6k}\Bigl[\Bigl(\frac{3}{q}\chi_h\Bigl(1-\frac{\chi_2}{4}\Bigr)B_2(\chi)-\frac{1}{4}\Bigr)z^{-1}+z\Bigr]\Bigr\}\\ \times\begin{cases}S^+(y') & \text{if } \chi_h=+1,\\ S^-(y') & \text{if } \chi_h=-1,\end{cases}\end{aligned} \tag{3.7}$$

其中

$$B_2(\chi)=\frac{1}{p}\sum_{\mu=1}^{p-1}\mu^2\chi_\mu,$$

$$y' = \exp\bigl(-2\pi i(\overline{2h})/k - \pi/kz\bigr), \tag{3.7i}$$

and

$$S^+(x) := \prod_{\mathbf{r}} (x^{2r}, x^{2p-2r}; x^{2p})_\infty^{-1} \prod_{\mathbf{s}} (x^{p+2s}, x^{p-2s}; x^{2p})_\infty^{-1}, \tag{3.7ii}$$

$$S^-(x) := \prod_{\mathbf{r}} (x^{p+2r}, x^{p-2r}; x^{2p})_\infty^{-1} \prod_{\mathbf{s}} (x^{2s}, x^{2p-2s}; x^{2p})_\infty^{-1}. \tag{3.7iii}$$

满足 $p\nmid k$ **的情形。** 现在假设 $p\nmid k$，对于整数 t，令

$$\omega_t := \exp(2\pi i t/p) \qquad \text{and} \qquad \bar\omega_t := \exp(-2\pi i t/p),$$

并主张 $H = hp$ 与 $K = kp$。

(3) 当 $(k, 2p) = 2$ 时，有

$$\Phi(x) = \lambda_k \phi_{h,k} \exp\left\{\frac{\pi q}{6k}\Bigl(\frac{1}{p} z^{-1} + z\Bigr)\right\} \times \begin{cases} T^+(x'') & \text{if } \chi_k = +1, \\ T^-(x'') & \text{if } \chi_k = -1, \end{cases} \tag{3.8}$$

其中

$$\lambda_k = 2^{-\frac{p-1}{4}} \prod_{\mathbf{r}} \csc(\pi \|\bar k r\|/p) \prod_{\mathbf{s}} \frac{\csc(\pi\|2\bar k s\|/p)}{\csc(\pi\|\bar k s\|/p)} \qquad (k\bar k \equiv 1 \pmod p), \tag{3.8i}$$

$$x'' = \exp\bigl(-2\pi i \bar H/k - 2\pi/Kz\bigr), \tag{3.8ii}$$

and

$$T^\pm(x) := \prod_{\mathbf{r}} (\pm\omega_r x, \pm\bar\omega_r x; x)_\infty^{-1} \prod_{\mathbf{s}} (\mp\omega_s x, \mp\bar\omega_s x; x)_\infty^{-1}. \tag{3.8iii}$$

(4) 当 $(k, 2p) = 1$ 时，有

$$\Phi(x) = \lambda_k \phi_{h,k} \exp\left\{\frac{\pi q}{6k}\Bigl(\frac{1}{4p} z^{-1} + z\Bigr)\right\} \times \begin{cases} U^+(y'') & \text{if } \chi_k = +1, \\ U^-(y'') & \text{if } \chi_k = -1, \end{cases} \tag{3.9}$$

其中

$$\lambda_k = 2^{-\frac{p-1}{4}} \prod_{\mathbf{r}} \csc(\pi \|\bar k r\|/p) \qquad (k\bar k \equiv 1 \pmod p), \tag{3.9i}$$

$$y'' = \exp\bigl(-2\pi i(\overline{2H})/k - \pi/Kz\bigr), \tag{3.9ii}$$

and

$$U^+(x) := \prod_{\mathbf{r}} (\omega_r x^2, \bar\omega_r x^2; x^2)_\infty^{-1} \prod_{\mathbf{s}} (\omega_s x, \bar\omega_s x; x^2)_\infty^{-1}, \tag{3.9iii}$$

$$U^-(x) := \prod_{\mathbf{r}} (\omega_r x, \bar\omega_r x; x^2)_\infty^{-1} \prod_{\mathbf{s}} (\omega_s x^2, \bar\omega_s x^2; x^2)_\infty^{-1}, \tag{3.9iv}$$

注 3.2. 为使方程（3.5）–（3.9）保持一致，令

$$\lambda_k := 1 \qquad \text{when} \qquad p\nmid k. \tag{3.10}$$

4 关于 $\mathfrak{p}(n,\chi)$的初始公式

现在我们开始推导 $\mathfrak{p}(n,\ \chi)$ 在固定 $p\equiv 1$ （模 4）且 $p<24$时的级数公式。我们的工作遵循哈代和拉马努金 [11] 以及 Rademacher[18], 的研究，因此适当之处省略细节——例如参见 [1, 第 5] 章，其中有详细论述。取正整数 n 和 N，满足 $N\geq 2$，我们从整数值公式开始

$$\mathfrak{p}(n,\chi)=\frac{1}{2\pi i}\int_C \Phi(x)x^{-n-1}\,dx,$$

其中， C 是以原点为圆心、半径为 $\exp(-2\pi N^{-2})$ 的正向圆。我们将区间 $(0,1]$ 分割为互不相交的“法里弧”

$$\xi_{h,k}=\left(\tfrac{h}{k}-\vartheta'_{h,k}\,,\tfrac{h}{k}+\vartheta''_{h,k}\right],$$

对于 $1\leq h\leq k\leq N$ 和 $(h,k)=1$，在弧 $\xi_{h,k}$ 上，我们记

$$x=\exp\left\{2\pi i\left(\frac{h}{k}+\phi\right)-2\pi N^{-2}\right\}=\exp\left\{2\pi i\frac{h}{k}-\frac{2\pi z}{k}\right\},$$

其中

$$z:=k(N^{-2}-i\phi)\qquad\text{and}\qquad -\vartheta'_{h,k}<\phi\leq\vartheta''_{h,k}.$$

为避免混淆，$\vartheta'_{h,k}$ 和 $\vartheta''_{h,k}$ 分别简记为 ϑ' 和 ϑ''。接着，回顾式（2.5）中的求和记号，可得

$$\mathfrak{p}(n,\chi)=\sum_{k\leq N}{\sum_{h\,(k)}}' e^{-2\pi inh/k}\int_{-\vartheta'}^{\vartheta''}\Phi(x)\exp(2\pi nz/k)\,d\phi. \tag{4.1}$$

在按 $\gcd(k,2p)$ 分开各个积分，并使用第 3节中的不同函数方程之前，我们暂且使用以下一般形式的关系

$$\Phi(x)=\lambda_k\phi_{h,k}\exp(\psi_{h,k}(z))\Omega_{h,k}(\tilde{x}),$$

注意到 $\Omega_{h,k}$是 $R^{\pm}$, $S^{\pm}$, $T^{\pm}$和 $U^{\pm}$中的一个，并且 $\tilde{x}$的形式取决于$\gcd(k,2p)$。利用这个一般方程，式（4.1）中的积分为

$$\int_{-\vartheta'}^{\vartheta''}\Phi(x)\exp(2\pi nz/k)\,d\phi=\lambda_k\phi_{h,k}\int_{-\vartheta'}^{\vartheta''}\exp(\psi_{h,k}(z)+2\pi nz/k)\Omega_{h,k}(\tilde{x})\,d\phi,$$

由此得到公式

$$\mathfrak{p}(n,\chi)=\sum_{k\leq N}{\sum_{h\,(k)}}'\lambda_k\phi_{h,k}e^{-2\pi inh/k}\int_{-\vartheta'}^{\vartheta''}\exp(\psi_{h,k}(z)+2\pi nz/k)\Omega_{h,k}(\tilde{x})\,d\phi. \tag{4.2}$$

现在将对 $k\leq N$ 的求和拆分为按 $(k,2p)$ 分组的若干子和，并将这些子和记作 $\mathfrak{p}_{(j)}(n,\chi;\ N)$，于是可写为

$$\mathfrak{p}(n,\chi)=\mathfrak{p}_{(1)}(n,\chi;N)+\mathfrak{p}_{(2)}(n,\chi;N)+\mathfrak{p}_{(p)}(n,\chi;N)+\mathfrak{p}_{(2p)}(n,\chi;N),$$

and 我们针对不同的 j，分别考察 $\mathfrak{p}_{(j)}(n,\ \chi;\ N)$。最后，为便于后续使用，le t

$$\mathfrak{p}_{(j)}(n,\chi):=\lim_{N\to\infty}\mathfrak{p}_{(j)}(n,\chi;N).$$

4.1 (, χ) 和 $\mathfrak{p}_{(2)}(n,\ \chi)$ 的级数公式。为便于阐述，我们先考察 $\mathfrak{p}_{(2)}(n,\ \chi;\ N)$，然后考察 $\mathfrak{p}_{(1)}$ $(n,\ \chi;\ N)$。本节中，我们始终假设 $p\nmid k$ 和 $(h,\ k)\ =1$，并且保持 $H=hp$ 和 $K=kp$。

Supp设 $(k,2p)\ =2$ 并将 x 按式 (3.4) 中的方式表示。回顾第 3 节可知

$$\Phi(x)=\lambda_k\phi_{h,k}\exp\left\{\frac{\pi q}{6k}\Big(\frac{1}{p}z^{-1}+z\Big)\right\}T^{\pm}(x''),$$

其中 λ_k 由式 (3.8i) 给出，$\phi_{h,\ k}$ 是式 (2.10) 中的单位根，

$$x''=\exp(-2\pi i\bar{H}/k-2\pi/Kz),$$

且 $T^{\pm}(x)$ 在式 (3.8iii) 中定义。记作

$$T^{\pm}(x)=\sum_{m=0}^{\infty}t_m^{\pm}x^m,$$

我们得到

$$T^{\pm}(x'')=\sum_{m=0}^{\infty}t_m^{\pm}\exp(-2\pi i\bar{H}m/k-2\pi m/Kz),$$

其中“ $\pm$”由 χ_k决定，而非 χ_h。将这些代入（4.2），可推得

$$\begin{aligned}
&\mathfrak{p}_{(2)}(n,\chi;N)\\
&\quad=\sum_{\substack{k\le N\\(k,2p)=2}}{\sum_{h\,(k)}}'\lambda_k\phi_{h,k}e^{-2\pi inh/k}\int_{-\vartheta'}^{\vartheta''}\exp\left\{\frac{\pi q}{6k}\Big(\frac{1}{p}z^{-1}+z\Big)+\frac{2\pi n}{k}z\right\}\\
&\qquad\qquad\times\left(\sum_{m=0}^{\infty}t_m^{\pm}\exp\left\{-\frac{2\pi i\bar{H}m}{k}-\frac{2\pi m}{K}z^{-1}\right\}\right)d\phi\\
&\quad=\sum_{\substack{k\le N\\(k,2p)=2}}\sum_{m=0}^{\infty}\lambda_k t_m^{\pm}\mathfrak{L}_k(n,m)\int_{-\vartheta'}^{\vartheta''}\exp\left\{\frac{2\pi}{K}\Big(\frac{p-1}{24}-m\Big)z^{-1}+\frac{2\pi\tilde{n}}{k}z\right\}d\phi,\qquad(4.3)
\end{aligned}$$

其中

$$\mathfrak{L}_k(n,m):={\sum_{h\,(k)}}'\phi_{h,k}\exp\big(-2\pi i(nh+m\bar{H})/k\big)\qquad\big(\text{when }(k,2p)=2\big),$$

and

$$\tilde{n}:=n+\frac{p-1}{24}.$$

现在，我们将表达式（4.3）拆分为主项和误差项，先处理后者。由于 λ_k 始终是至多由 $\frac{3p}{2}$ 个量$\csc(\pi a/p)$或$\csc(\pi a/p)^{-1}$的乘积，其中 $0<a<p$ （如（3.8i）、—(3.9i）和（3.10）所示），显然

$$\lambda_k\ll 1,\qquad\text{uniformly in } k.$$

此外，如第 5 节所述，对于 $m\ge 0$ 和 k，当 $(k,2p)\ =2$时，有

$$\mathfrak{L}_k(n,m)\ll n^{1/3}k^{2/3+\varepsilon}.\qquad(4.4)$$

回顾 $z = k(N^{-2} - i\phi)$，可以验证 $\operatorname{Re}(\frac{1}{kz}) \geq \frac{1}{2}$对于 $-\vartheta' \leq \phi \leq \vartheta''$，因此当 z^{-1} 在 (4.3) 中的系数为负时，即当 $m > \frac{p-1}{24}$ 时，有

$$\int_{-\vartheta'}^{\vartheta''} \exp\left\{\frac{2\pi}{K}\left(\frac{p-1}{24} - m\right)z^{-1} + \frac{2\pi\tilde{n}}{k}z\right\} d\phi \ll \int_{-\vartheta'}^{\vartheta''} e^{-\pi m/p} \cdot e^{2\pi n/N^2}\, d\phi \ll \frac{e^{2\pi n/N^2 - \pi m/p}}{kN}.$$

于是，由于我们假设 $p < 24$，对所有 $m \geq 1$我们有 $m > \frac{p-1}{24}$，从而可以推出

$$\begin{aligned}
&\sum_{\substack{k\leq N\\(k,2p)=2}} \sum_{m\geq 1} \lambda_k t_m^{\pm} \mathfrak{L}_k(n,m) \int_{-\vartheta'}^{\vartheta''} \exp\left\{\frac{2\pi}{K}\left(\frac{p-1}{24} - m\right)z^{-1} + \frac{2\pi\tilde{n}}{k}z\right\} d\phi \\
&\quad \ll \sum_{\substack{k\leq N\\(k,2p)=2}} n^{1/3} k^{2/3+\varepsilon} \sum_{m\geq 1} \left(t_m^{\pm} \frac{e^{2\pi n/N^2 - \pi m/p}}{kN}\right) \\
&\quad \ll n^{1/3} e^{2\pi n/N^2} N^{-1} \sum_{k\leq N} k^{-1/3+\varepsilon} \left(\sum_{m\geq 1} t_m^{\pm} e^{-\pi m/p}\right) \\
&\quad \ll n^{1/3} e^{2\pi n/N^2} \left|T^{\pm}(e^{-\pi/p})\right| N^{-1/3+\varepsilon}.
\end{aligned}$$

回到（4.3），于是对 $m \geq 1$ 的求和将成为误差项的一部分，剩下只需考虑 $m = 0$ 项。注意到$t_0^{\pm} = 1$，并记

$$\mathfrak{L}_k(n) = \mathfrak{L}_k(n,0) = \sum_{h\,(k)}{}' \phi_{h,k} \exp(-2\pi i n h/k), \tag{4.5}$$

方程（4.3）化为

$$\begin{aligned}
\mathfrak{p}_{(2)}(n,\chi;N) = \sum_{\substack{k\leq N\\(k,2p)=2}} \lambda_k \mathfrak{L}_k(n) \int_{-\vartheta'}^{\vartheta''} \exp\left\{\frac{2\pi}{K}\left(\frac{p-1}{24}\right)z^{-1} + \frac{2\pi\tilde{n}}{k}z\right\} d\phi \\
+ O\Big(n^{1/3} e^{2\pi n/N^2} N^{-1/3+\varepsilon}\Big).
\end{aligned}$$

然后，按照例如 [1,18], 中的标准论证，我们作变量替换

$$\omega := z/k = N^{-2} - i\phi,$$

我们令 $\mathcal{R}(N,\ k)$为绕原点、顶点为$\{\pm N^{-2} - i\vartheta', \pm N^{-2} + i\vartheta''\}$的正向矩形，从而得到

$$\begin{aligned}
\int_{-\vartheta'}^{\vartheta''} \exp\left\{\frac{2\pi}{K}\left(\frac{p-1}{24}\right)z^{-1} + \frac{2\pi\tilde{n}}{k}z\right\} d\phi = \int_{\mathcal{R}(N,k)} \exp\left\{\frac{2\pi}{k^2}\left(\frac{p-1}{24p}\right)\omega^{-1} + 2\pi\tilde{n}\omega\right\} d\omega \\
+ O\Big(n^{1/3} N^{-1/3+\varepsilon} e^{2\pi n/N^2}\Big).
\end{aligned}$$

利用有关修正贝塞尔函数 $I_n(z)$的经典公式[2]，我们得到

$$\mathfrak{p}_{(2)}(n,\chi;N) = \sqrt{\tfrac{1}{24}(1-\tfrac{1}{p})\tilde{n}^{-1}} \sum_{\substack{k\leq N\\(k,2p)=2}} \frac{\lambda_k}{k} \mathfrak{L}_k(n)\, I_1\Big(\frac{4\pi}{k}\sqrt{\tfrac{1}{24}(1-\tfrac{1}{p})\tilde{n}}\Big) + O(N^{-\frac{1}{3}+\varepsilon}),$$

[2]见引理4.7，位于本节末尾。

其中再次有 $\tilde{n}=n+\frac{p-1}{24}$；为简洁起见，我们作如下定义。

定义 4.1. 对于素数 p，令

$$\kappa_p := \pi\sqrt{\tfrac{2}{3}(1-\tfrac{1}{p})}. \tag{4.6}$$

取 $N\to\infty$，并回顾由定义可知 $\mathfrak{p}_{(2)}(n,\ \chi;\ N)\to\mathfrak{p}_{(2)}(n,\ \chi)$，我们将迄今的推导总结为如下引理。

引理 4.2. 对于 $p<24$，若 $p\equiv 1\ (\mathrm{mod}\ 4)$，则有

$$\mathfrak{p}_{(2)}(n,\chi)=\frac{\kappa_p}{4\pi\sqrt{\tilde{n}}}\sum_{\substack{k=1\\(k,2p)=2}}^{\infty}\frac{\lambda_k}{k}\mathfrak{L}_k(n)I_1\Big(\frac{\kappa_p}{k}\sqrt{\tilde{n}}\Big), \tag{4.7}$$

其中 $\tilde{n}=n+\frac{p-1}{24}$，$\lambda_k$ 由（3.8i）给出，κ_p 由（4.6）给出，且

$$\mathfrak{L}_k(n)=\sum_{h\,(k)}{}'\,\phi_{h,k}\exp(-2\pi inh/k).$$

现在转而讨论 $\mathfrak{p}_{(1)}(n,\ \chi;\ N)$，当 $(k,\ 2p)=1$ 时，几乎相同的计算使我们得到 $\lim_{N\to\infty}\mathfrak{p}_{(1)}(n,\ \chi;\ N)$ 的如下公式，即 $\mathfrak{p}_{(1)}(n,\ \chi)$ 的公式。

引理 4.3. 对于 $p<24$，其中 $p\equiv 1$（模 4），有

$$\mathfrak{p}_{(1)}(n,\chi)=\frac{\kappa_p}{4\pi\sqrt{\tilde{n}}}\sum_{\substack{k=1\\(k,2p)=1}}^{\infty}\frac{\lambda_k}{2k}\mathfrak{L}_k(n)I_1\Big(\frac{\kappa_p}{2k}\sqrt{\tilde{n}}\Big), \tag{4.8}$$

其中 $\tilde{n}=n+\frac{p-1}{24}$，$\lambda_k$ 由 (3.9i) 给出，κ_p 由 (4.6) 给出，并且

$$\mathfrak{L}_k(n)=\sum_{h\,(k)}{}'\,\phi_{h,k}\exp(-2\pi inh/k).$$

4.2 关于 $\mathfrak{p}_{(p)}(n,\ \chi)$ 和 $\mathfrak{p}_{(2p)}(n,\ \chi)$ 的级数公式。 现在我们考察 $\mathfrak{p}_{(p)}$ 和 $\mathfrak{p}_{(2p)}$，先从 $\mathfrak{p}_{(2p)}(n,\ \chi;\ N)$ 开始。首先，我们写出

$$R^{\pm}(x)=\sum_{m=0}^{\infty}\rho_m^{\pm}x^m,$$

其中我们回顾 (3.6) 中，“±”在此由 χ_h 决定，而非 χ_k。此外，我们回顾 (3.6i) 中，($\tilde{x}$ 在 (3.6) 中的 “ 变换后的点 ” 为

$$x'=\exp(-2\pi i\bar{h}/k-2\pi/kz)\qquad(h\bar{h}\equiv 1\ (\mathrm{mod}\ k)).$$

重复第4.1 节中的论证后，我们很快便得到

$$\mathfrak{p}_{(2p)}(n,\chi;N)=\sum_{\substack{k\le N\\(k,2p)=2p}}\sum_{h\,(k)}{}'\sum_{m=0}^{\infty}\lambda_k\rho_m^{\chi_h}\phi_{h,k}\exp\big(-2\pi i(nh+m\bar{h})/k\big)$$
$$\times\int_{-\vartheta'}^{\vartheta''}\exp\left(-\frac{2\pi}{k}\left(\frac{p-1}{24}+m\right)z^{-1}+\frac{2\pi\tilde{n}}{k}z\right)d\phi,$$

其中再次有 $\tilde{n} = n + \frac{p-1}{24}$。由于 χ_h 仅取决于 h （模 p），我们按模 p 的剩余类对 h （模 k）上的求和分组，得到

$$\mathfrak{p}_{(2p)}(n,\chi) = \sum_{\substack{k\le N\\(k,2p)=2p}} {\sum_{d\,(p)}}' \sum_{m=0}^{\infty} \lambda_k \rho_m^{\chi_d} \mathfrak{L}_k(n,m;d) \times \int_{-\vartheta'}^{\vartheta''} \exp\left(-\frac{2\pi}{k}\left(\frac{p-1}{24}+m\right)z^{-1} + \frac{2\pi\tilde{n}}{k}z\right) d\phi, \tag{4.9}$$

其中

$$\mathfrak{L}_k(n,m;d) := {\sum_{\substack{h\,(k)\\ h\equiv d \pmod p}}}' \phi_{h,k} \exp\big(-2\pi i(nh+m\bar{h})/k\big) \qquad (\text{当 } 2p|k), \tag{4.10}$$

在第 5节（具体而言，引理 5.2）中，我们发现

$$\mathfrak{L}_k(n,m;d) \ll n^{1/3}k^{2/3+\varepsilon} \qquad \text{when } 2p|k,$$

对 d一致成立，参见不等式（4.4）。由于 z^{-1} 在（4.9）中的系数始终为负，因此根据类似于第4.1节中的论证可得

$$\mathfrak{p}_{(2p)}(n,\chi;N) \ll n^{1/3} e^{2\pi n/N^2} N^{-1} \sum_{k\le N} k^{-1/3+\varepsilon} \ll N^{-1/3+\varepsilon}.$$

取 $N\to\infty$，我们得到以下引理（这不要求 $p<24$）。

引理4.4. 对于 $p \equiv 1 \pmod 4$，有

$$\mathfrak{p}_{(2p)}(n,\chi) = 0.$$

最后转向 $\mathfrak{p}_{(p)}(n,\chi;N)$，我们将级数 $S^{\pm}(x)$ 从 (3.7) 展开为

$$S^{\pm}(x) = \sum_{m=0}^{\infty} \sigma_m^{\pm} x^m,$$

并回顾由 (3.7i) 可知，变换后的点 $\tilde{x}$ 在此情形下为

$$y' = \exp\big(-2\pi i(\overline{2h})/k - \pi/kz\big),$$

其中 $2h\overline{2h} \equiv 1 \pmod k$。此外，我们还记得

$$B_2(\chi) := \frac{1}{p}\sum_{\mu=1}^{p-1} \mu^2 \chi_\mu.$$

与前面几种情况类似的论证使我们得出

$$\mathfrak{p}_{(p)}(n,\chi;N) = \sum_{\substack{k\le N\\(k,2p)=p}} {\sum_{d\,(p)}}' \sum_{m=0}^{\infty} \sigma_m^{\chi_d} \mathfrak{L}_k(n,m;d) \times \int_{-\vartheta'}^{\vartheta''} \exp\left(\frac{2\pi}{k}\left(\frac{c_{m,d}}{4}\right)z^{-1} + \frac{2\pi\tilde{n}}{k}z\right) d\phi, \tag{4.11}$$

其中同样有 $\tilde{n} = n + \frac{p-1}{24}$，其中

$$\mathfrak{L}_k(n,m;d) := \sum_{\substack{h\,(k)\\ h\equiv d \pmod p}}{}' \phi_{h,k}\exp\bigl(-2\pi i(nh+m\overline{2h})/k\bigr) \qquad (\text{when } (k,2p)=p), \quad (4.12)$$

并且其中

$$c_{m,d} := \chi_d\Bigl(1-\frac{\chi_2}{4}\Bigr)B_2(\chi) - \frac{p-1}{24} - 2m. \quad (4.13)$$

为从（4.11）中分离出误差项，我们必须确定 $c_{m,d}$ 作为 m 和 d的函数时的符号。令 $L(s,\chi)$ 表示通常的 狄利克雷 L-函数，注意到[3]当 $p\equiv 1 \pmod 4$ 时， $B_2(\chi) = \pi^{-2}p^{\frac{3}{2}}L(2,\chi)$，并利用粗略下界 $L(2,\chi) \geq \zeta(4)\zeta(2)(1+p^{-2}) = \frac{\pi^2}{15}(1+p^{-2})$，从而得出

$$\Bigl(1-\frac{\chi_2}{4}\Bigr)B_2(\chi) - \frac{p-1}{24} > 0 \qquad \text{for } p\equiv 1 \pmod 4,$$

即使不施加 $p<24$这一限制也成立。因此$c_{m,d}<0$ 若 $\chi_d=-1$，则模 p 的非二次剩余对（4.11）只贡献误差项。此外，由于 $c_{m,d}$ 在满足 $\chi_d=1$的 d 上为常数，我们令

$$c_m := c_{m,1} = \Bigl(1-\frac{\chi_2}{4}\Bigr)B_2(\chi) - \frac{p-1}{24} - 2m,$$

并对（d 模 p）的二次剩余求和，将（4.11）中的求和“收尾”，写成

$$\mathfrak{p}_{(p)}(n,\chi;N) = \sum_{\substack{k\le N\\ (k,2p)=p}}\sum_{m=0}^{\infty}\sigma_m^+\mathfrak{L}_k^+(n,m)\int_{-\vartheta'}^{\vartheta''}\exp\Bigl(\frac{2\pi}{k}\Bigl(\frac{c_m}{4}\Bigr)z^{-1}+\frac{2\pi\tilde{n}}{k}z\Bigr)\,d\phi$$
$$+ O\Bigl(n^{1/3}e^{2\pi n/N^2}N^{-1/3+\varepsilon}\Bigr),$$

其中

$$\mathfrak{L}_k^+(n,m) := \sum_{\substack{d\,(p)\\ \chi_d=1}}{}'\mathfrak{L}_k(n,m;d) = \sum_{\substack{h\,(k)\\ \chi_h=1}}{}'\phi_{h,k}\exp\bigl(-2\pi i(nh+m\overline{2h})/k\bigr).$$

暂且接受 $\mathfrak{L}_k^+(n,m) \ll n^{1/3}k^{2/3+\varepsilon}$ 当 $(k,2p)=p$时，我们仿照 (4.7) 和 (4.8) 中的做法，并取 $N\to\infty$ 以证明以下引理。

引理 4.5. 对于满足 $p\equiv 1 \pmod 4$ 的 $p<24$，有

$$\mathfrak{p}_{(p)}(n,\chi) = \frac{1}{\sqrt{\tilde{n}}}\sum_{\substack{k=1\\ (k,2p)=p}}^{\infty}\sum_{\substack{m=0\\ c_m\ge 0}}^{\infty}\frac{\sqrt{c_m}}{2k}\sigma_m^+\mathfrak{L}_k^+(n,m)\,I_1\Bigl(\frac{2\pi}{k}\sqrt{c_m\tilde{n}}\Bigr), \quad (4.14)$$

其中

$$\tilde{n} = n + \frac{p-1}{24}, \qquad c_m = \Bigl(1-\frac{\chi_2}{4}\Bigr)B_2(\chi) - \frac{p-1}{24} - 2m,$$

$$\mathfrak{L}_k^+(n,m) = \sum_{\substack{h\,(k)\\ \chi_h=1}}{}'\phi_{h,k}\exp\bigl(-2\pi i(nh+m\overline{2h})/k\bigr),$$

[3]参见，例如， [15, 例 10.1。14]

模 $2h2\overline{h} \equiv 1 \pmod{k}$，且 σ_m^+ 通过级数定义

$$S^+(x) = \prod_{\mathbf{r}} (x^{2r}, x^{2p-2r}; x^{2p})_\infty^{-1} \prod_{\mathbf{s}} (x^{p+2s}, x^{p-2s}; x^{2p})_\infty^{-1} = \sum_{m=0}^{\infty} \sigma_m^+ x^m.$$

注4.6. 对于 $p < 24$，对 m 在（4.14）中的求和仅遍历 $0 \le m \le 2$，但随着p增大，这个范围会显著扩大；事实上，关系式 $B_2(\chi) = \pi^{-2} p^{\frac{3}{2}} L(2, \chi)$ 以及粗略估计

$$\tfrac{\pi^2}{15}(1 + p^{-2}) \le L(2, \chi) \le \tfrac{\pi^2}{6}(1 - p^{-2})$$

表明，当 $p \to \infty$ 时，有

$$\Big(1 - \frac{\chi_2}{4}\Big) B_2(\chi) - \frac{p-1}{24} \asymp p^{\frac{3}{2}}.$$

因此，对于较大的 p，我们预期，对满足 $c_m > 0$ 的 m 求和，其“长度”约为 $p^{3/2}$。

我们以如下经典事实结束本节（按本文需要作了归一化），该事实涉及修正贝塞尔函数 $I_n(z)$。

引理 4.7. 设 a 和 b 为实数且非负，并设 $\mathcal{R}$ 是一个以原点为中心、正向定向的矩形。那么

$$\frac{1}{2\pi i} \int_{\mathcal{R}} \exp\Big(\frac{2\pi b}{k^2}\omega^{-1} + 2\pi a\omega\Big)\, d\omega = \begin{cases} \sqrt{b/a}\, I_1\big(\frac{4\pi}{k}\sqrt{ab}\big)/k, & a > 0, \\ 4\pi b/k^2, & a = 0. \end{cases}$$

5 关于 $\mathfrak{L}_k$ 和 $\mathfrak{L}_k^+$ 的一些粗略界

在本节中，我们证明：(4.5)、(4.10) 和 (4.12) 中定义的和 $\mathfrak{L}_k(n)$ 与 $\mathfrak{L}_k^+(n, m)$ 可以按通常意义表示为 Kloosterman 和。我们回顾，r 与 s 分别是 $\{1, \dots, \frac{p-1}{2}\}$ 中包含二次剩余与非二次剩余（模 p）的子集，并且对 r 与 s 求和是在 r 与 s 分别遍历 r 与 s 时进行的。我们回顾，$\{\mu\}_p$ 的定义使得

$$\mu \equiv \{\mu\}_p \pmod{p} \qquad \text{and} \qquad 0 \le \{\mu\}_p < p,$$

并且

$$q = \frac{p-1}{2}.$$

由于戴德金和与 Kloosterman 和已有充分研究，且我们在以 $\gcd(k, 2p)$ 为条件的四个（严格说来是八个）情形中的论证彼此十分相似（也与 [9, 10, 13] 中的论证相似），我们仅对情形 $2p \mid k$ 证明关于$\mathfrak{L}_k(n, m; d)$ 的所需界，即对于

$$\mathfrak{L}_k(n, m; d) = \sideset{}{'}\sum_{\substack{h \,(k) \\ h \equiv d \pmod{p}}} \phi_{h,k} \exp\big(-2\pi i(nh + m\bar{h})/k\big). \tag{5.1}$$

[4] Niven [16, 第 360] 页提供了一个方便的参考文献——尽管他引用了 Watson [22,第79页和 181]。

注记 5.1. 我们在本节中使用的关于 Kloosterman 和的方法与结果远非“最为人知”。采用这些“较为粗略”的方法，是因为它们简单，并且是为了遵循 Lehner [13] 和 Hagis Jr. [9,10]的工作。

假设 $2p\,|\,k$，并令 $12p = fG$，其中 f 是 $12p$ 的最大因子，且与 k 互素；注意，根据假设，$p|G$。通过以下方式定义 φ 和 Γ

$$f\varphi \equiv 1 \pmod{Gk} \qquad \text{and} \qquad Gk\Gamma \equiv 1 \pmod{f}.$$

于是，根据 [10, 第 405–407] 页以及 $\omega_{\mathbf{s}}(2h,\ k) = \omega_{\mathbf{s}}(h,\ k/2)$ 这一事实，我们有

$$\phi_{h,k} = \omega_{\mathbf{r}}(h,k)\frac{\omega_{\mathbf{s}}(h,k/2)}{\omega_{\mathbf{s}}(h,k)} = \exp\Big\{2\pi i\Big[\frac{\varphi}{G}(3pq - 6\textstyle\sum_{\mathbf{r}}\{hr\}_p) + \frac{\varphi}{Gk}(uh + v\bar{h})\Big]\Big\}, \tag{5.2}$$

其中 $h\bar{h} \equiv 1 \pmod{Gk}$，并且

$$u = -2pq + k\big(6\textstyle\sum_{\mathbf{r}} r + qk - 3pq\big) \tag{5.2a}$$

$$v = -q(\tfrac{1}{2}k^2 + 2p). \tag{5.2b}$$

引理 5.2。 设 $p \equiv 1 \pmod 4$，设 $2p|k$，并设 $(d,p) = 1$。则有

$$\mathfrak{L}_k^{+}(n,m;d) \ll n^{1/3}k^{2/3+\varepsilon},$$

关于 d 一致成立。

证明。 由（5.2）可知

$$\phi_{h,k} = \zeta_{h,k}\exp\left(\varphi(uh + v\bar{h})\frac{2\pi i}{Gk}\right),$$

其中 $\zeta_{h,k}$ 仅取决于 h 模 p的剩余类，即 $h \equiv d$ 模 p。由于 d和 k 固定，在证明余下部分中，令 $\zeta_d := \zeta_{h,k}$。由于$\phi_{h,k}$ 以及（5.1）中的指数函数关于 h都是 k-周期的（根据各自的定义），我们将（5.1）中的求和范围扩展至 h模 Gk，并通过乘以 $1/G$进行相应调整。因此

$$\mathfrak{L}_k(n,m;d) = \frac{\zeta_d}{G}\sideset{}{'}\sum_{\substack{h\ (Gk)\\ h\equiv d\ (\mathrm{mod}\ p)}}\exp\left(\Big[(\varphi u - Gn)h + (\varphi v - Gm)\bar{h}\Big]\frac{2\pi i}{Gk}\right), \tag{5.3}$$

其中 u 和 v 分别如（5.2a）和（5.2b）所示。

利用关系式，通过一个标准论证

$$\frac{1}{p}\sum_{a=1}^{p}\exp(2\pi i(x-y)a/p) = \begin{cases}1, & x \equiv y \pmod p,\\ 0, & \text{otherwise},\end{cases}$$

条件 $h \equiv d$ 模 p的限制在（5.3）中可以通过引入一个常数因子而消除，因此

$$\mathfrak{L}_k(n,m;d) \ll \left|\sideset{}{'}\sum_{h\ (Gk)}\exp\left(\Big[(\varphi u - Gn)h + (\varphi v - Gm)\bar{h}\Big]\frac{2\pi i}{Gk}\right)\right|.$$

由于后一个和是一个“完全”克洛斯特曼和，Salié 界 [21] 表明

$$\mathfrak{L}_k(n,m;d) \ll (\varphi u - Gn, Gk)^{1/3}k^{2/3+\varepsilon}. \tag{5.4}$$

由于 $(f, Gk) = 1$、$fG = 12p$ 和 $f\varphi \equiv 1$（模 Gk），我们观察到

$$(\varphi u - Gn, Gk) = (f\varphi u - fGn, Gk) = (u - 12pn, Gk) \ll (u - 12pn, k).$$

此外，由（5.2a）可知 $u = -2pq + kw$ 对某个整数 w成立，因此

$$(u - 12pn, k) = (-2pq - 12pn, k) \ll n,$$

由此及（5.4）可立即得出结果。 ■

6 关于 λ_k 的一些引理

现在，我们根据（3.8i）、（3.9i）和（3.10）推导余割量 λ_k 的一些公式。本节中，设 $kk \equiv 1$（模 p）当 $(k, p) = 1$时成立；我们不要求 $p < 24$，只要求 $p \equiv 1$（模 4）。再次用 $\mathbf{r}$ 和 $\mathbf{s}$ 分别表示范围 p中的二次剩余和非二次剩余集合（模 $\{1, \dots, \frac{p-1}{2}\}$），我们回顾一下：

$$\lambda_k = 2^{-\frac{p-1}{4}} \prod_{\mathbf{r}} \csc(\pi \|\bar{k}r\|/p) \qquad \text{if } (k, 2p) = 1, \tag{6.1a}$$

$$\lambda_k = 2^{-\frac{p-1}{4}} \prod_{\mathbf{r}} \csc(\pi \|\bar{k}r\|/p) \prod_{\mathbf{s}} \frac{\csc(\pi \|2\bar{k}s\|/p)}{\csc(\pi \|\bar{k}s\|/p)} \qquad \text{if } (k, 2p) = 2, \tag{6.1b}$$

并且

$$\lambda_k = 1 \qquad \text{if } p | k.$$

对于固定的 p，令

$$Q_{\mathbf{r}} := 2^{-\frac{p-1}{4}} \prod_{\mathbf{r}} \csc(\pi r/p) \qquad \text{and} \qquad Q_{\mathbf{s}} := 2^{-\frac{p-1}{4}} \prod_{\mathbf{s}} \csc(\pi s/p),$$

并通过以下方式定义 Q

$$Q = \frac{Q_{\mathbf{r}}^2}{Q_{\mathbf{s}}^2} = \frac{\prod_{\mathbf{s}} \sin^2(\pi s/p)}{\prod_{\mathbf{r}} \sin^2(\pi r/p)}.$$

Remark 6.1. 由于对整数 $1 \le \mu < p$有$\sin(\pi\mu/p) = \sin(\pi(p-\mu)/p)$，我们有 ve

$$Q = \frac{\prod_{\mathbf{s}} \sin(\pi s/p) \sin(\pi(p-s)/p)}{\prod_{\mathbf{r}} \sin(\pi r/p) \sin(\pi(p-r)/p)},$$

并且由于$\mathbf{r} \cup (p - \mathbf{r})$与$\mathbf{s} \cup (p - \mathbf{s})$分别穷尽了全范围 $\{1, \dots, p-1\}$中的二次剩余与非二次剩余（模 p），我们看到 Q 等于初等数论中的一个经典量；参见例如 [8, 第10页及以下]。

由于 $\lambda_k = 1$ 每当 $p|k$，令$(k, p) = 1$。由(6.1a)，显然

$$\lambda_k = \begin{cases} Q_{\mathbf{r}}, & \chi_k = 1, \\ Q_{\mathbf{s}}, & \chi_k = -1, \end{cases} \qquad \text{for odd } k. \tag{6.2}$$

对于偶数 k，我们必须分别考虑 $p \equiv 5$（模 8）和 $p \equiv 1$（模 8）这两种情形。

引理 6.2. 设 $p \equiv 5$（模 8），并设 $k = 2^\nu m$ 满足 $\nu > 0$ 且 $(m,\ p) = 1$。则

$$\lambda_k = \begin{cases} Q^{\frac{1}{2}\chi_m}\lambda_m, & \nu \text{ odd}, \\ Q^{2\chi_m}\lambda_m, & \nu \text{ even}. \end{cases}$$

证明。 我们首先证明，若 $(k, p) = 1$，则

$$\lambda_{2k}/\lambda_k = \begin{cases} Q^{\frac{1}{2}\chi_k}, & k \text{ odd}, \\ Q^{-\frac{3}{2}\chi_k}, & k \text{ even}. \end{cases} \tag{6.3}$$

设 k 为奇数。由于 2 是模 p 的非二次剩余，当 $p \equiv 5$（模 8）时，由方程（6.1b）可得

$$\lambda_{2k} = 2^{-\frac{p-1}{4}} \left(\prod_{\mathbf{r}} \csc(\pi \|\bar{k}r\|/p) \right)^2 \prod_{\mathbf{s}} \sin(\pi \|\bar{k}s\|/p),$$

因此，由（6.1a）和（6.1b）合并可得

$$\frac{\lambda_{2k}}{\lambda_k} = \frac{\prod_{\mathbf{s}} \sin(\pi \|\bar{k}s\|/p)}{\prod_{\mathbf{r}} \sin(\pi \|\bar{k}r\|/p)}.$$

由于 $x \mapsto \|kx\|$ 会固定或交换 $\mathbf{r}$ 和 $\mathbf{s}$，具体取决于 k 是模 p的二次剩余还是非二次剩余，因此我们得到

$$\lambda_{2k}/\lambda_k = Q^{\frac{1}{2}\chi_k} \qquad \text{for } k \text{ odd}.$$

沿用类似的论证，我们很快便可得出

$$\lambda_{2k}/\lambda_k = Q^{-\frac{3}{2}\chi_k} \qquad \text{for } k \text{ even},$$

这就证明了（6.3）。

方程（6.2）和（6.3）使我们能够通过化归到 λ_k 的奇数部分，为偶数 k 构造公式：具体而言，从 k开始，k 为奇数且与 p互素，我们得到

$$\lambda_{2k} = Q^{\frac{1}{2}\chi_k}\lambda_k, \quad \lambda_{4k} = Q^{-\frac{3}{2}\chi_{2k}}\lambda_{2k} = Q^{2\chi_k}\lambda_k, \quad \lambda_{8k} = Q^{-\frac{3}{2}\chi_{4k}}\lambda_{4k} = Q^{\frac{1}{2}\chi_k}\lambda_k,$$

依此类推，结论得证。 ■

引理 6.3。 设 $p \equiv 1$（模 8），且令 $(k, p) = 1$。则有

$$\lambda_k = \begin{cases} Q_{\mathbf{r}}, & \chi_k = 1, \\ Q_{\mathbf{s}}, & \chi_k = -1. \end{cases}$$

证明。 由于 $p \equiv 1$（模 8），任意 μ 是非二次剩余（模 p）当且仅当 2μ 是非二次剩余（模 p）。因此，由（6.1b）可得

$$\prod_{\mathbf{s}} \frac{\csc(\pi \|2\bar{k}s\|/p)}{\csc(\pi \|\bar{k}s\|/p)} = \prod_{\mathbf{s}} \frac{\csc(\pi \|\bar{k}s\|/p)}{\csc(\pi \|\bar{k}s\|/p)} = 1,$$

由此

$$\lambda_k = 2^{-\frac{p-1}{4}} \prod_{\mathbf{r}} \csc(\pi \|\bar{k}r\|/p) \qquad \text{for } k \text{ odd } \textit{or} \text{ even},$$

结果便立即得出。 ■

推论 6.4. 若 $p \equiv 1$ (模 8) 且 $(k, p) = 1$，则 $\lambda_{2k} = \lambda_k$。

我们以几个关于 $Q_{\mathbf{r}}$、 $Q_{\mathbf{s}}$ 和 Q 的具体例子结束本节；利用前面的引理可以计算出 λ_k。对于 $p=5$，有

$$Q_{\mathbf{r}}=\sqrt{\tfrac{1}{2}(1+\tfrac{1}{\sqrt{5}})},\quad Q_{\mathbf{s}}=\sqrt{\tfrac{1}{2}(1-\tfrac{1}{\sqrt{5}})},\quad \text{and}\quad Q=\tfrac{3+\sqrt{5}}{2}.$$

对于 $p=13$，有

$$Q_{\mathbf{r}}=\sqrt{\tfrac{1}{2}(1+\tfrac{3}{\sqrt{13}})},\quad Q_{\mathbf{s}}=\sqrt{\tfrac{1}{2}(1-\tfrac{3}{\sqrt{13}})},\quad \text{and}\quad Q=\tfrac{11+3\sqrt{13}}{2}.$$

对于 $p=17$，有

$$Q_{\mathbf{r}}=\sqrt{1+\tfrac{4}{\sqrt{17}}},\quad Q_{\mathbf{s}}=\sqrt{1-\tfrac{4}{\sqrt{17}}},\quad \text{and}\quad Q=33+8\sqrt{17}.$$

7 $\mathfrak{p}(n,\chi)$ 的完整级数

现在我们给出 $\mathfrak{p}(n,\chi)$ 的精确级数公式，回顾一下，

$$\mathfrak{p}(n,\chi)=\mathfrak{p}_{(1)}(n,\chi)+\mathfrak{p}_{(2)}(n,\chi)+\mathfrak{p}_{(p)}(n,\chi)+\mathfrak{p}_{(2p)}(n,\chi),$$

其中每个 $\mathfrak{p}_{(j)}(n,\chi)$ 仅包含来自既约有理数 $\frac{h}{k}\in(0,1]$ 且满足$(k,2p)=j$的项。在第 4.1 节中，我们发现

$$\mathfrak{p}_{(1)}(n,\chi)=\frac{\kappa_p}{4\pi\sqrt{\tilde{n}}}\sum_{\substack{k=1\\(k,2p)=1}}^{\infty}\frac{\lambda_k}{2k}\mathfrak{L}_k(n)I_1\Big(\frac{\kappa_p}{2k}\sqrt{\tilde{n}}\Big),\tag{7.1}$$

$$\mathfrak{p}_{(2)}(n,\chi)=\frac{\kappa_p}{4\pi\sqrt{\tilde{n}}}\sum_{\substack{k=1\\(k,2p)=2}}^{\infty}\frac{\lambda_k}{k}\mathfrak{L}_k(n)I_1\Big(\frac{\kappa_p}{k}\sqrt{\tilde{n}}\Big),\tag{7.2}$$

其中 λ_k 按第 6 节中的方式确定，

$$\tilde{n}=n+\frac{p-1}{24},\qquad \kappa_p=\pi\sqrt{\tfrac{2}{3}(1-\tfrac{1}{p})},$$

and

$$\mathfrak{L}_k(n)=\sum_{h\,(k)}{}'\,\phi_{h,k}\exp(-2\pi inh/k)\qquad \text{for } (k,p)=1.$$

接下来，我们回顾引理 4.5 指出的结论：

$$\mathfrak{p}_{(p)}(n,\chi)=\frac{1}{\sqrt{\tilde{n}}}\sum_{\substack{k=1\\(k,2p)=p}}^{\infty}\sum_{\substack{m=0\\c_m>0}}^{\infty}\frac{\sqrt{c_m}}{2k}\sigma_m^+\mathfrak{L}_k^+(n,m)\,I_1\Big(\frac{2\pi}{k}\sqrt{c_m\tilde{n}}\Big),$$

其中

$$c_m=\Big(1-\frac{\chi_2}{4}\Big)B_2(\chi)-\frac{p-1}{24}-2m,$$

常数 σ_m^+ 定义为

$$S^+(x)=\prod_{\mathbf{r}}(x^{2r},x^{2p-2r};x^{2p})_\infty^{-1}\prod_{\mathbf{s}}(x^{p+2s},x^{p-2s};x^{2p})_\infty^{-1}=\sum_{m=0}^{\infty}\sigma_m^+x^m,$$

and

$$\mathfrak{L}_k^+(n,m)=\sideset{}{'}\sum_{\substack{h\,(k)\\ \chi_h=1}}\phi_{h,k}\exp\bigl(-2\pi i(nh+m\overline{2h})/k\bigr)\qquad\text{for }(k,2p)=p,$$

其中 $2h2\overline{h}\equiv 1$ （模 k）。最后，我们回顾引理4.4 中的结论：

$$\mathfrak{p}_{(2p)}(n,\chi)=0.$$

对于 k 满足 $(k,2p)=1$，我们注意到，(7.1) 和 (7.2) 中对应于 k 和 $2k$ 的被加数具有相同的“I_1-因子”。因此，我们可以合并 (7.1) 和 (7.2)，然后将对应于满足 k 且满足 $4\,|\,k$ 和 $p\nmid k$的加项分离出来，从而得到以下公式，该公式对 $p\equiv 1$ (模 4) 成立，其中 $p<24$,

$$\begin{aligned}\mathfrak{p}(n,\chi)&=\mathfrak{p}_{(1)}(n,\chi)+\mathfrak{p}_{(2)}(n,\chi)+\mathfrak{p}_{(p)}(n,\chi)\\&=\frac{\kappa_p}{4\pi\sqrt{\tilde n}}\sum_{\substack{k=1\\(k,2p)=1}}^{\infty}\frac{1}{2k}\Bigl\{\lambda_k\mathfrak{L}_k(n)+\lambda_{2k}\mathfrak{L}_{2k}(n)\Bigr\}I_1\Bigl(\frac{\kappa_p}{2k}\sqrt{\tilde n}\Bigr)\\&\quad+\frac{\kappa_p}{4\pi\sqrt{\tilde n}}\sum_{\substack{k=1\\4\,|\,k,\,p\nmid k}}^{\infty}\frac{\lambda_k}{k}\mathfrak{L}_k(n)I_1\Bigl(\frac{\kappa_p}{k}\sqrt{\tilde n}\Bigr)\\&\quad+\frac{1}{\sqrt{\tilde n}}\sum_{\substack{k=1\\(k,2p)=p}}^{\infty}\sum_{\substack{m=0\\c_m\geq 0}}^{\infty}\frac{\sqrt{c_m}}{2k}\sigma_m^+\mathfrak{L}_k^+(n,m)I_1\Bigl(\frac{2\pi}{k}\sqrt{c_m\tilde n}\Bigr).\end{aligned}\tag{7.3}$$

7.1 关于 $\mathfrak{p}(n,(\frac{\cdot}{17}))$ 的公式。当 $p=17$ 时，我们计算得

$$B_2(\chi)=\frac{1}{p}\sum_{\mu=1}^{16}\mu^2\chi_\mu=8,$$

由此

$$c_m=\Bigl(1-\frac{\chi_2}{4}\Bigr)B_2(\chi)-\frac{p-1}{24}-2m=2\Bigl(\frac{8}{3}-m\Bigr),$$

因此，$c_m\geq 0$ 仅当 $m=0$时，1、2；特别地，我们有

$$c_0=\tfrac{16}{3},\quad c_1=\tfrac{10}{3},\quad\text{and}\quad c_2=\tfrac{4}{3}.$$

此外，我们有

$$\kappa_{17}=4\pi\sqrt{\tfrac{2}{51}},\qquad\text{and}\qquad\tilde n=n+\tfrac{2}{3}.$$

对于较小的 m，可以直接计算常数 σ_m^+，我们发现

$$S^+(x)=\sum_{m\geq 0}\sigma_m^+x^m=1+x^2+x^3+2x^4+2x^5+3x^6+4x^7+6x^8+\cdots,$$

据此

$$\sigma_0^+=1,\quad\sigma_1^+=0,\quad\text{and}\quad\sigma_2^+=1.$$

结合这些事实以及以下事实： $\lambda_{2k} = \lambda_k$ 对于 $(k,\ p) = 1$ 代入公式（7.3），对于 $\mathfrak{p}(n,\ (\frac{\cdot}{17}))$ 我们最终得到公式

$$\begin{aligned}\mathfrak{p}(n,(\tfrac{\cdot}{17})) = \sqrt{\tfrac{2}{51}\tilde{n}^{-1}} \sum_{\substack{k=1\\(k,2p)=1}}^{\infty} \frac{\lambda_k}{2k}\Big\{\mathfrak{L}_k(n) + \mathfrak{L}_{2k}(n)\Big\} I_1\Big(\tfrac{2\pi}{k}\sqrt{\tfrac{2}{51}\tilde{n}}\Big) \\ + \sqrt{\tfrac{2}{51}\tilde{n}^{-1}} \sum_{\substack{k=1\\4\mid k,\, p\nmid k}}^{\infty} \frac{\lambda_k}{k}\mathfrak{L}_k(n) I_1\Big(\tfrac{4\pi}{k}\sqrt{\tfrac{2}{51}\tilde{n}}\Big) \\ + \sqrt{\tfrac{1}{3}\tilde{n}^{-1}} \sum_{\substack{k=1\\(k,2p)=p}}^{\infty} \frac{1}{2k}\Big\{4\mathfrak{L}_k^{+}(n,0) I_1\big(\tfrac{8\pi}{3k}\sqrt{3\tilde{n}}\big) + 2\mathfrak{L}_k^{+}(n,2) I_1\big(\tfrac{4\pi}{3k}\sqrt{3\tilde{n}}\big)\Big\}.\end{aligned} \tag{7.4}$$

考察公式 (7.4)，由于 $I_1(t) \sim (2\pi t)^{-\frac{1}{2}} e^t$ 当 $t \to \infty$，且不同的 I_1 项具有不同的自变量，我们可知，$\mathfrak{p}(n, (\frac{\cdot}{17}))$ 的消失等价于因子 $\mathfrak{L}_k(n)$ 和 $\mathfrak{L}_k^{+}(n,m)$ 之间的某些抵消与消失。考察 $\mathfrak{L}_k$ 和 $\mathfrak{L}_k^{+}$ 需要掌握有关戴德金和的术语与理论，这些内容构成了本文后半部分的大部分。

8 消失结果的预备知识

设 $p \equiv 1$（模 4），对 p 的大小不作限制。仍令 $\mathbf{r}$ 和 $\mathbf{s}$ 分别表示 $\{1, \dots, \frac{p-1}{2}\}$ 中（模 p）的二次剩余和非二次剩余集合，并仍将 r 和 s 分别保留用于表示 $\mathbf{r}$ 和 $\mathbf{s}$ 的元素。我们回顾一下，h 和 k 总是正整数，并且

$$H = hp \qquad \text{and} \qquad K = kp$$

始终如此，并且

$$\sum_{\mu\,(k)} \quad \text{and} \quad \sum_{\mu\,(k)}' \quad \text{indicate} \quad \sum_{\mu=0}^{k-1} \quad \text{and} \quad \sum_{\substack{\mu=0\\(\mu,k)=1}}^{k-1}, \quad \text{respectively.}$$

注意： 除非另有说明，本文余下部分用 $[x]$ 表示 x 的整数部分（或下取整）。

8.1 戴德金和 $s(h,\ k)$ 和 $s_\chi(h,\ k)$。

现在我们回顾戴德金和的一些基本性质——更多介绍请参见例如 [19, 20]。函数 $((x))$ 是

$$((x)) = x - [x] - \tfrac{1}{2} + \tfrac{1}{2}\delta(x), \qquad \text{where} \qquad \delta(x) := \mathbb{1}_{\mathbb{Z}}(x),$$

并且，戴德金和 $s(h,\ k)$ 及其辅助和 $t(h,\ k)$ 定义为

$$s(h,k) = \sum_{\mu\,(k)} \Big(\!\Big(\frac{h\mu}{k}\Big)\!\Big)\Big(\!\Big(\frac{\mu}{k}\Big)\!\Big) \tag{8.1}$$

and

$$t(h,k)=\sum_{\mu\,(k)}\mu\Big[\frac{h\mu}{k}\Big]. \tag{8.2}$$

展开 $((x))$ 在（8.1）中的各项后，很容易验证

$$s(h,k)=\tfrac{1}{6}h(k-1)(2-\tfrac{1}{k})-\tfrac{1}{k}t(h,k)-\tfrac{1}{4}(k-1)+\tfrac{1}{4}(d-1), \tag{8.3}$$

其中 $d=(h,\ k)$。已知 [20, 定理 1]，

$$s(qh,qk)=s(h,k)\qquad \text{for any integer } q>0, \tag{8.4}$$

并利用这一点和（8.3），可以直接验证

$$t(qh,qk)=qt(h,k)+\tfrac{1}{12}kq(q-1)\Big\{4hk(q+1)-6h-3(k-1)+3(d-1)\Big\}, \tag{8.5}$$

其中再次有 $d=(h,\ k)$，且 $q>0$ 为任意整数。

现在我们定义并考察 $s(h,\ k)$ 和 $t(h,\ k)$ 的“χ-扭曲”版本，并注意到 χ_a再次专用于勒让德符号 $(\frac{a}{p})$，同时指出，下面的大部分内容都适用于一般的偶狄利克雷特征。

定义 8.1。对于 $k\geq 1$，令 $\varphi:=\ ^{p}_{(k,\ p)}$，使得 $\varphi k=$最小公倍数$(k,\ p)$。然后令

$$s_\chi(h,k):=\sum_{\mu\,(\varphi k)}\chi_\mu\Big(\Big(\frac{h\mu}{k}\Big)\Big)\Big(\Big(\frac{\mu}{\varphi k}\Big)\Big), \tag{8.6}$$

并且，类比于（8.2），令

$$t_\chi(h,k):=\frac{1}{\varphi}\sum_{\mu\,(\varphi k)}\mu\chi_\mu\Big[\frac{h\mu}{k}\Big]. \tag{8.7}$$

注记 8.2。在 [2,第 314 页及后续页]，Berndt 定义

$$S_1(h,k;\psi)=\sum_{\mu\ (\mathrm{mod}\ qk)}\psi(\mu)((h\mu/k))((\mu/qk))$$

当 ψ 是模数为 q 的偶本原特征时。Berndt 的 S_1 与我们的 s_χ 在 $q=p$ 且 $(k,p)\ =1$ 时显然一致，但在 $p|k$ 时表面上并不一致；事实上，很容易验证在后一种情况下二者也等价。尽管二者等价，为方便起见，我们仍保留 s_χ 的定义（8.6），并分别考察 $p|k$ 的情形以及 $p\nmid k$ 的情形。

Akin 对于方程（8.3）的推导，经过简单计算即可验证 t

$$s_\chi(h,k)=\frac{h}{k}B_2(\chi)-\frac{1}{k}t_\chi(h,k), \tag{8.8}$$

这里我们回顾一下

$$B_2(\chi)=\frac{1}{p}\sum_{\mu\,(p)}\mu^2\chi_\mu.$$

接下来，我们证明 s_χ 和 t_χ 具有类似于（8.4）和（8.5）的“缩放关系”。

引理 8.3。 对于任意整数 $q > 0$，有

$$s_\chi(qh, qk) = s_\chi(h, k), \tag{8.9}$$
$$t_\chi(qh, qk) = qt_\chi(h, k). \tag{8.10}$$

证明。 由（8.8）可知

$$s_\chi(qh, qk) = \frac{h}{k}B_2(\chi) - \frac{1}{qk}t_\chi(qh, qk),$$

因此，（8.9）可由（8.10）立即得出。后一个关系可通过直接但繁琐的计算得到：根据 μ（模 qk 或模 pqk）将求和拆分为不同的算术级数，具体取决于 q 和 k 是否能被p整除，因此我们省略细节。 ■

8.2 **周期伯努利数**。 以下定义是关于周期伯努利数[5]的定义和基本结果的简要汇编

定义 8.4。 对于 $p \equiv 1$（模 4），令 $B_0(\chi) = B_1(\chi) = 0$，并令

$$B_2(\chi) = \frac{1}{p}\sum_{\mu\,(p)} \mu^2\chi_\mu.$$

此外，对于实数 y，令

$$B_{1,\chi}(y) := \tfrac{1}{2}\delta(y)\chi_y - \sum_{0\le n\le y} \chi_n \qquad (\delta(y) = \mathbb{1}_{\mathbb{Z}}(y)). \tag{8.11}$$

函数$B_{1,\,\chi}(y)$ 显然是 p-周期的，在 $n \in \mathbb{Z}$ 时于区间 $(n,\ n+1)$ 上为常数（且为整数值），而在 $y \in \mathbb{Z}$ 时为半整数。此外，有 [3]，即

$$B_{1,\chi}(y) = \sum_{\mu\,(p)} \chi_\mu\left(\left(\frac{y+\mu}{p}\right)\right).$$

对于非整数 y，有 $B_{1,\,\chi}(-y) = -B_{1,\,\chi}(y)$。以下关于$B_{1,\,\chi}$ 的附加性质在第 9 节中很有用。

引理 8.5。 假设$(k, p) = 1$。对于实数 y，有

$$\sum_{\lambda\,(p)} B_{1,\chi}(k\lambda + y) = \begin{cases} 0 & p\nmid k, \\ pB_{1,\chi}(y) & p\mid k. \end{cases} \tag{8.12}$$

证明。 由于$B_{1,\,\chi}(x)$ 是 p-周期的，方程 (8.12) 在 $p|k$时显然成立，因此不妨设 $p\nmid k$；同理，假设 $y \in [0, p)$不会失去一般性。由 (8.11) 可得

$$\sum_{\lambda=0}^{p-1} B_{1,\chi}(k\lambda + y) = \tfrac{1}{2}\sum_{\lambda=0}^{p-1} \delta(k\lambda + y)\chi_{k\lambda+y} - \sum_{\lambda=0}^{p-1}\sum_{\nu=0}^{k\lambda+[y]} \chi_\nu, \tag{8.13}$$

[5]我们将 [3, 第 287 页及以下各页] 作为方便的参考资料；不过，正如其中所述，原始结果及其推广可见于同一作者的著作 [4,5]。

其中 $[y]$ 是 y的整数部分。由于（k， p） $=1$，当 λ 遍历模 p的所有剩余类时， $k\lambda+[y]$ 也随之遍历，因此

$$\sum_{\lambda=0}^{p-1}\sum_{\nu=0}^{k\lambda+[y]}\chi_\nu=\sum_{\lambda=0}^{p-1}\sum_{\nu=0}^{\lambda}\chi_\nu.$$

由于 χ 是偶数，很容易看出后一项双重求和为零。等式右边的第一项求和（8.13）也为零：事实上，若 y 不是整数值，则所有 $\delta(k\lambda+y)=0$；若 y 是整数值，则 $k\lambda+y$ 再次遍历模 p 的所有剩余类，正如 λ 一样，因此得到 $\frac{1}{2}\sum_{\lambda=0}^{p-1}\chi_\lambda=0$。 ■

$B_2(\chi)$的以下同余式在我们的推导中起着重要作用。

引理 8.6。 设 $p\equiv 1$ (模 4) 且 $p\neq 5$。则 $B_2(\chi)$ 是整数值，并且

$$B_2(\chi)\equiv\begin{cases}0\pmod 8, & p\equiv 1\pmod 8,\\ 4\pmod 8, & p\equiv 5\pmod 8.\end{cases}\tag{8.14}$$

注 8.7。 在 $p=5$ 的情形下，有 $B_2(\chi)=\frac{4}{5}$。

证明。 我们首先证明 $B_2(\chi)$ 是整数，方法是证明 $\sum_{\mu(p)}\mu^2\chi_\mu\equiv 0$ (模 p)[6]。设 g 是模 p的一个原根。由于 $\chi_\mu\equiv\mu^{(p-1)/2}$ (模 p)，我们有

$$pB_2(\chi)=\sum_{\mu=1}^{p-1}\mu^2\chi_\mu\equiv\sum_{\mu=1}^{p-1}\mu^2\mu^{(p-1)/2}\equiv\sum_{\mu=1}^{p-1}g^{2\mu+\mu(p-1)/2}\pmod p,$$

并按 μ奇偶性分类，可得

$$\equiv\sum_{\nu=1}^{(p-1)/2}g^{4\nu}+\sum_{\nu=0}^{(p-3)/2}g^{4\nu+2+(p-1)/2}\equiv(g^4-g^2)\sum_{\nu=0}^{(p-3)/2}g^{4\nu}\pmod p.$$

由于 $p>5$，我们有 $g^4\not\equiv 1$ （模 p）以及 $g^2\not\equiv -1$ （模 p），因此

$$(g^4-g^2)\sum_{\nu=0}^{(p-3)/2}g^{4\nu}\equiv g^2(g^2-1)\frac{(g^4)^{(p-1)/2}-1}{g^4-1}\equiv g^2\cdot\frac{g^{2(p-1)}-1}{g^2+1}\pmod p.$$

由于 $g^{p-1}\equiv 1$ （模 p），可得同余式 pB_2（χ） $\equiv 0$（模 p），因此 B_2（χ）确为整数。

现在来看模 8 的同余式，由于 χ是偶数，我们有

$$pB_2(\chi)=\sum_{\mu=1}^{p-1}\mu^2\chi_\mu=\sum_{\mu=1}^{(p-1)/2}(\mu^2+(p-\mu)^2)\chi_\mu=-\sum_{\mu=1}^{(p-1)/2}2\mu(p-\mu)\chi_\mu,$$

并且，由于必有 $4|2\mu$（$p-\mu$），模 8 化简后可得

$$-\sum_{\mu=1}^{(p-1)/2}2\mu(p-\mu)\chi_\mu\equiv\sum_{\mu=1}^{(p-1)/2}2\mu(p-\mu)\equiv\tfrac{1}{6}p(p-1)(p+1)\pmod 8.$$

因此 $B_2(\chi)\equiv\frac{1}{6}(p-1)(p+1)$（模 8），且（8.14）成立。 ■

[6]感谢 Trevor Wooley 向我们展示了这一同余的一个初等证明。

注记 8.8. 当 $p \equiv 3 \pmod 4$ 时，运用类似的论证可以轻易验证，$B_2(\chi)$ 再次为整数值，并且在这种情况下，$B_2(\chi) \equiv 1 \pmod 2$。

8.3 **一些互反律与同余式**。现在我们回顾一下 $s(h,\ k)$ 和 $t(h,\ k)$ 的一些著名互反关系。具体来说，对于 $(h,\ k) = 1$，有

$$s(h,k) + s(k,h) = \tfrac{1}{12}(\tfrac{h}{k} + \tfrac{k}{h} + \tfrac{1}{hk}) - \tfrac{1}{4},$$

并且，对于 $(h,\ k) = 1$，同样有 [17, p. 221]

$$ht(h,k) + kt(k,h) = \tfrac{1}{12}(h-1)(k-1)(8hk - h - k - 1).$$

不出所料，$s_\chi(h,\ k)$ 的互反公式更为复杂，因此我们需要给出一个额外的定义。

定义 8.9。对于 $(a,\ b) = 1$ 且 $b > 1$，令

$$\tilde{s}_\chi(a,b) := \sum_{\mu\,(bp)} \left(\!\!\left(\frac{\mu}{bp}\right)\!\!\right) B_{1,\chi}\Big(\frac{a\mu}{b}\Big) = \sum_{\mu\,(bp)} \sum_{\nu\,(p)} \chi_\nu \left(\!\!\left(\frac{\mu}{bp}\right)\!\!\right) \left(\!\!\left(\frac{a\mu + b\nu}{bp}\right)\!\!\right).$$

关于 $\tilde{s}_\chi(a,\ b)$ 的一些性质将在第 9 节讨论。

命题 8.10 (Berndt [3])。对于 $(k,p) = 1$ 与 $(h,k) = 1$，有

$$s_\chi(h,k) + \tilde{s}_\chi(k,h) = \frac{h}{2k} B_2(\chi). \tag{8.15}$$

对于 $K = kp$ 与 $(h, K) = 1$，有

$$s_\chi(h,K) + \tilde{s}_\chi(K,h) = \frac{h^2 + \chi_h}{2hK} B_2(\chi). \tag{8.16}$$

推论 8.11. 设 $K = kp$ 与 $(h, K) = 1$。有

$$\tilde{s}_\chi(K,h) = \chi_h s_\chi(\hat{K},h),$$

ˆ其中 $K\hat{K} \equiv 1$ (模 h)，因此 (8.16) 表明

$$s_\chi(h,K) + \chi_h s_\chi(\hat{K},h) = \frac{h^2 + \chi_h}{2hK} B_2(\chi). \tag{8.17}$$

证明。因为 $\tilde{s}(K,h)$ 中的被加数仅依赖于 μ 模 ph，我们写 te

$$\mu \equiv \lambda h\bar{h} + jp\hat{p} \pmod{ph}, \quad \text{where } h\bar{h} \equiv 1 \pmod p \text{ and } p\hat{p} \equiv 1 \pmod h,$$

以及 $0 \le \lambda < p$ 和 $0 \le j < h$。由此，我们有

$$\begin{aligned}\tilde{s}_\chi(K,h) &= \sum_{j\,(h)} \sum_{\nu\,(p)} \sum_{\lambda\,(p)} \chi_\nu \left(\!\!\left(\frac{\lambda h\bar{h} + jp\hat{p}}{ph}\right)\!\!\right) \left(\!\!\left(\frac{K\lambda h\bar{h} + Kjp\hat{p} + h\nu}{ph}\right)\!\!\right) \\ &= \sum_{j\,(h)} \sum_{\nu\,(p)} \chi_\nu \left(\!\!\left(\frac{Kjp\hat{p} + h\nu}{ph}\right)\!\!\right) \sum_{\lambda\,(p)} \left(\!\!\left(\frac{\lambda\bar{h}}{p} + \frac{j\hat{p}}{h}\right)\!\!\right).\end{aligned}$$

于是，因为 $(h,p)=1$ 与 $\sum_{\lambda(p)}((\lambda/p+x))=((px))$ 对所有实数 x 成立，上式即为

$$=\sum_{j\,(h)}\sum_{\nu\,(p)}\chi_\nu\Big(\Big(\frac{Kjp\hat{p}+h\nu}{ph}\Big)\Big)\Big(\Big(\frac{j}{h}\Big)\Big)=\sum_{j\,(h)}\sum_{\nu\,(p)}\chi_\nu\Big(\Big(\frac{jp\hat{p}+h\nu}{ph}\Big)\Big)\Big(\Big(\frac{\hat{K}j}{h}\Big)\Big)$$
$$=\sum_{j\,(h)}\sum_{\nu\,(p)}\chi_{\bar{h}\nu}\Big(\Big(\frac{\hat{K}j}{h}\Big)\Big)\Big(\Big(\frac{jp\hat{p}+h(\bar{h}\nu)}{ph}\Big)\Big),$$

^ 而后者等于 $\chi_h s_\chi(K,h)$，因为 $(h,p)=1$。 ■

9 关于 $\tilde{s}_\chi$ 的引理

鉴于命题 8.10，我们看到 $B_2(\chi)$ 与 $\tilde{s}_\chi$ 的同余式可以用来导出 s_χ 的同余式。由于推论 8.11使我们能够“避开” $\tilde{s}_\chi$ （当 $p|K$ 时），我们需要一条关于 $\tilde{s}_\chi(k,h)$ 在 k 与 p 互素时的引理。

引理 9.1. 设 $p\equiv 1\pmod 4$，设 $b>1$，并设 $(a,b)=(a,p)=1$。则 $\tilde{s}_\chi(a,b)$ 为整数值，并且

$$\tilde{s}_\chi(a,b)\equiv\tfrac{1}{2}(\chi_a-1)\pmod 2.$$

引理 9.1 的证明较为技术性，因此我们首先展开并化简关于 $\tilde{s}_\chi(a,b)$ 的公式。将 $\mu=\lambda b+j$ 写成含 $0\le j<b$ 与 $0\le\lambda<p$的形式，并展开 $((\mu/bp))$，我们利用引理8.5 推得

$$\tilde{s}_\chi(a,b)=\sum_{j\,(b)}\sum_{\lambda\,(p)}\Big(\frac{\lambda b+j}{bp}-\frac{1}{2}\Big)B_{1,\chi}\Big(a\lambda+\frac{aj}{b}\Big)=\sum_{j\,(b)}\sum_{\lambda\,(p)}\frac{\lambda}{p}B_{1,\chi}\Big(a\lambda+\frac{aj}{b}\Big).$$

展开 $B_{1,\chi}(a\lambda+\frac{aj}{b})$ 及其中的 $((x))$ 项，并再次化简（利用 $\sum_{\nu(p)}\chi_\nu=0$ 这一事实），我们得到公式

$$\tilde{s}_\chi(a,b)=\frac{1}{p}\sum_{j\,(b)}\sum_{\lambda\,(p)}\sum_{\nu\,(p)}\lambda\chi_\nu\Big[\frac{a\lambda+a(j/b)+\nu}{p}\Big],$$

这促使我们给出以下定义。

定义 **n 9.2.** 固定 a 和 p，其中 $p\equiv 1$（模 4），且 $(a,p)=1$，对于实数 y，令

$$S(y):=S(a,p;y):=\sum_{\mu\,(p)}\sum_{\nu\,(p)}\mu\chi_\nu\Big[\frac{a\mu+ay+\nu}{p}\Big].$$

Now

$$\tilde{s}_\chi(a,b)=\frac{1}{p}\sum_{j=0}^{b-1}S\Big(\frac{j}{b}\Big),\tag{9.1}$$

并通过三个关于 9.1 的“子引理”来证明引理 $S(y)$。

引理 9.3. 固定上述的 a 和 p，令 $S(y)=S(a,p;y)$。

(1) 对所有 y，都有 $S(y)\equiv 0$ (模 p)，因此 $\frac{1}{p}S(y)$ 始终为整数值。

(2) 如果 y 不是 $\frac{1}{a}\mathbb{Z}$的元素，那么

$$S(1-y) = S(y).$$

在证明引理 9.3 之前，我们先作一些说明：暂且设 $(a,p) = 1$且 $(a,b) = 1$，并假设引理 9.3 成立。那么 $\frac{1}{b}, \ldots, \frac{b-1}{b}$均不在 $\frac{1}{a}\mathbb{Z}$中，因此对于 $0 < j < b$， $S(\frac{j}{b}) = S(\frac{b-j}{b})$，而 (9.1) 中的大多数被加数 $S(\frac{j}{b})$都会在模 2 下相互抵消。因此，在这种情况下，我们可推出

$$\tilde{s}_\chi(a,b) \equiv \begin{cases} S(0) \pmod 2 & \text{if } b \text{ is odd,} \\ S(0) + S(\frac{1}{2}) \pmod 2 & \text{if } b \text{ is even.} \end{cases} \tag{9.2}$$

引理的证明 *9.3*。 对于部分 (1) 令 $c := [ay]$，于是 $[\frac{a\mu+ay+\nu}{p}] = [\frac{a\mu+c+\nu}{p}]$，而对于 $0 \le \mu < p$ 令

$$a\mu + c = q_\mu p - r_\mu \qquad \text{with } 1 \le r_\mu \le p.$$

由于 $\sum_{\nu(p)} \chi_\nu = 0$，总和 $S(y)$ 为

$$= \sum_{\mu,\nu\,(p)} \mu\chi_\nu \left[\frac{q_\mu p - r_\mu + \nu}{p}\right] = \sum_{\mu,\nu\,(p)} \mu\chi_\nu \left(q_\mu + \left[\frac{\nu - r_\mu}{p}\right]\right) = (-1)\sum_{\mu=0}^{p-1}\sum_{\nu=0}^{r_\mu - 1} \mu\chi_\nu.$$

由于 $(\mathrm{mod}\ p)$，当 μ 遍历同一范围时，量 $r_\mu - 1$ 也遍历 $\{0, 1, \ldots, p\}$，因此我们可推出

$$S(y) \equiv \bar{a}\sum_{\mu=0}^{p-1}\big((r_\mu - 1) + c + 1\big)\sum_{\nu=0}^{r_\mu - 1}\chi_\nu \equiv \bar{a}\sum_{\mu=0}^{p-1}(\mu + c + 1)\sum_{\nu=0}^{\mu}\chi_\nu \pmod p,$$

其中 $a\bar{a} \equiv 1$ （模 p）。由于 $\mu = 0$ 和 $\nu = 0$ 加项显然为 0，将它们舍去，然后交换求和次序，上式为

$$\equiv \bar{a}\sum_{\nu=1}^{p-1}\chi_\nu\sum_{\mu=\nu}^{p-1}(\mu + c + 1) \equiv -\frac{\bar{a}}{2}\sum_{\nu=1}^{p-1}\big(\nu^2 + (1+2c)\nu\big)\chi_\nu \equiv -\frac{\bar{a}}{2}\sum_{\nu=1}^{p-1}\nu^2\chi_\nu \pmod p.$$

后一个量等于 $-\frac{1}{2}\bar{a}pB_2(\chi)$，并且，由于 $B_2(\chi)$是偶数且为整数值（如引理 8.6所示），因此 $S(y) \equiv 0$ （模 p），从而证明了引理的第 (1) 部分。

对于第 (2) 部分，现在假设 $y \notin \frac{1}{a}\mathbb{Z}$，并注意到

$$S(1-y) = \sum_{\mu=0}^{p-1}\sum_{\nu=0}^{p-1}\mu\chi_\nu\left[\frac{a(\mu+1) - ay + \nu}{p}\right] = \sum_{\mu=1}^{p}\sum_{\nu=1}^{p-1}(\mu-1)\chi_\nu\left[\frac{a\mu + [-ay] + \nu}{p}\right].$$

再次令 $c := [ay]$，并利用以下事实：

$$[-ay] = -1 - [ay] + \delta(ay) = -1 - c,$$

我们将上文中的 μ 和 ν 分别替换为 $p-\mu$ 和 $p-\nu$，并化简后推出

$$S(1-y) = \sum_{\mu,\nu\,(p)}(p - \mu - 1)\chi_\nu\left[\frac{-a\mu - c - \nu - 1}{p}\right].$$

再次利用恒等式 $[-x]=-1-[x]+\delta(x)$，我们有

$$S(1-y)=\sum_{\mu,\nu\,(p)}(\mu+1-p)\chi_\nu\left(\left[\frac{a\mu+c+\nu+1}{p}\right]-\delta\left(\frac{a\mu+c+\nu+1}{p}\right)\right),$$

并利用这一观察：

$$\left[\frac{n+1}{p}\right]=\left[\frac{n}{p}\right]+\delta\left(\frac{n+1}{p}\right)\qquad\text{for integer } n,$$

由此可得

$$S(1-y)=\sum_{\mu,\nu\,(p)}(\mu+1-p)\chi_\nu\left[\frac{a\mu+c+\nu}{p}\right]=S(y)+(1-p)\sum_{\mu,\nu\,(p)}\chi_\nu\left[\frac{a\mu+c+\nu}{p}\right].$$

从这里开始，采用与处理项 (1)时类似的论证，可以很容易地证明此处后一个和为 0，从而得到断言 $S(1-y)=S(y)$。■

注 9.4。</style}若 $y\in\frac{1}{a}\mathbb{Z}$，设 $y=\frac{c}{a}$，同样容易推出

$$S(1-y)=S(y)-\sum_{\mu\,(p)}\mu\chi_{a\mu+c}.$$

如式（9.2）之前的讨论所述，若 $(a,\ b)=1$ 且 $(a,\ p)=1$，则 $\tilde{s}_\chi(a,\ b)$ 等价于 $S(0)$ 或 $S(0)+S(\frac{1}{2})$ 模 2。下一个引理表明，事实上，无论 b 的奇偶性如何，$\tilde{s}_\chi(a,\ b)\equiv S(0)$（模 2）。

引理 9.5。固定 $p\equiv 1$（模 4），并设 a 为奇数，且 $(a,p)=1$。那么

$$S(\tfrac{1}{2})\equiv 0\ (\mathrm{mod}\ 2).$$

证明。设 $a=2c+1$；由于 $S(y)$ 仅取决于 a（模 p），我们不妨假设 $0\le c\le\frac{p-3}{2}$。模 2 化简后，得到

$$\begin{aligned}S\left(\frac{1}{2}\right)&=\sum_{\mu,\nu=0}^{p-1}\mu\chi_\nu\left[\frac{a\mu+c+\nu}{p}\right]\equiv\sum_{j=1}^{(p-1)/2}\sum_{\nu=1}^{p-1}\left[\frac{a(2j-1)+c+\nu}{p}\right]\\&\equiv\sum_{\mu,\nu=1}^{p-1}\left[\frac{a\mu+c+\nu}{p}\right]-\sum_{j=1}^{(p-1)/2}\sum_{\nu=1}^{p-1}\left[\frac{2aj+c+\nu}{p}\right]\ (\mathrm{mod}\ 2).\end{aligned}\tag{9.3}$$

对于（9.3）中的第一个和，直接计算（采用与前一个引理类似的论证）可得

$$\sum_{\mu,\nu=1}^{p-1}\left[\frac{a\mu+c+\nu}{p}\right]\equiv c\ (\mathrm{mod}\ 2).$$

对于（9.3）中的第二个求和，我们同样可以推导出

$$\sum_{j=1}^{(p-1)/2}\sum_{\nu=1}^{p-1}\left[\frac{2aj+c+\nu}{p}\right]\equiv\sum_{j=1}^{(p-1)/2}\left[\frac{2aj+c}{p}\right]\ (\mathrm{mod}\ 2).$$

因此，要得出 $S(\frac{1}{2}) \equiv 0 \pmod 2$，只需证明

$$\sum_{j=1}^{(p-1)/2} \left[\frac{2aj+c}{p}\right] \equiv c \pmod 2 \qquad (a = 2c+1). \tag{9.4}$$

令 A_j 表示 j在（9.4）中的第 j个加项。首先，若 $a = 1$ 且 $c = 0$，则 $A_j = [\frac{2j}{p}] = 0$ 当 $1 \le j \le \frac{p-1}{2}$时，（9.4）成立。因此，设 $a > 1$，于是 $c > 0$。记

$$\sum_{1\le j\le \frac{p-1}{2}} A_j = A_{\frac{p-1}{4}} + A_{\frac{p-1}{2}} + \sum_{1\le j<\frac{p-1}{4}} \left(A_j + A_{\frac{p-1}{2}-j}\right),$$

我们的证明剩下的部分归结为证明

$$A_{\frac{p-1}{4}} \equiv c \pmod 2, \qquad A_{\frac{p-1}{2}} \equiv 0 \pmod 2,$$

and

$$A_j \equiv A_{\frac{p-1}{2}-j} \pmod 2 \qquad (1 \le j < \tfrac{p-1}{4}).$$

前两个同余式很容易验证，因此我们只证明最后一个。固定 $1 \le j < \frac{p-1}{4}$，可得

$$A_{\frac{p-1}{2}-j} = \left[\frac{2a(\frac{p-1}{2}-j)+c}{p}\right] = a + \left[\frac{-2aj-a+c}{p}\right] \equiv 1 + \left[\frac{-2aj-c-1}{p}\right] \pmod 2.$$

由于 $[-x] = -1 - [x] + \delta(x)$，这意味着

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

利用 $[\frac{n+1}{p}] - \delta(\frac{n+1}{p})$ 这一事实，其中 $n = 2aj + c$，可得

$$A_j + A_{\frac{p-1}{2}-j} \equiv \left[\frac{2aj+c}{p}\right] + \left[\frac{2aj+c}{p}\right] \equiv 0 \pmod 2,$$

如所声称，引理的断言得证。 ∎

现在已经证明，无论 b 的奇偶性如何，$\tilde{s}_\chi(a, b) \equiv S(0) \pmod 2$，因此只需考虑 $S(0)$。

引理 9.6. 固定 $p \equiv 1 \pmod 4$ 以及 $(a, p) = 1$，并令 $S(y) = S(a, p; y)$。则

$$S(0) \equiv \tfrac{1}{2}(\chi_a - 1) \pmod 2.$$

证明。由于对 $0 < \nu < p$ 有 $\chi_\nu \equiv 1 \pmod 2$，我们立即得到

$$S(0) \equiv \sum_{j=1}^{(p-1)/2} \sum_{\nu=1}^{p-1} \left[\frac{a(2j-1)+\nu}{p}\right] \equiv \sum_{\mu,\nu=1}^{p-1} \left[\frac{a\mu+\nu}{p}\right] - \sum_{j=1}^{(p-1)/2} \sum_{\nu=1}^{p-1} \left[\frac{2aj+\nu}{p}\right] \pmod 2. \tag{9.5}$$

暂且令 $\{x\} = x - [x]$ 表示 x 的<款式 id='2'>小数部分，由 a 和 p 的互素性可立即推出

$$\begin{aligned}\sum_{\mu,\nu=1}^{p-1} \left[\frac{a\mu+\nu}{p}\right] &= \tfrac{1}{2}(a+1)(p-1)^2 - \sum_{\mu,\nu=1}^{p-1} \left\{\frac{a\mu+\nu}{p}\right\} \\ &= \tfrac{1}{2}(a+1)(p-1)^2 - \tfrac{1}{2}(p-1)(p-2) \equiv 0 \pmod 2,\end{aligned}$$

因此，只需考虑（9.5）中的后一个求和。此次，对于 $1 \le j \le \frac{p-1}{2}$ 我们写成

$$2aj = q_j p + r_j, \qquad \text{with } 1 \le r_j < p,$$

注意到 $r_j = p$ 不可能，因此

$$S(0) \equiv \sum_{j=1}^{(p-1)/2} \sum_{\nu=1}^{p-1} \left[\frac{2aj+\nu}{p}\right] \equiv \sum_{j=1}^{(p-1)/2} \sum_{\nu=1}^{p-1} \left[\frac{\nu+r_j}{p}\right] \equiv \sum_{j=1}^{(p-1)/2} \sum_{\nu=p-r_j}^{p-1} 1 \equiv \sum_{j=1}^{(p-1)/2} r_j \pmod 2.$$

另一方面，我们有 $r_j = 2aj - p[\frac{2aj}{p}] \equiv [\frac{2aj}{p}]$（模 2），由此推得

$$S(0) \equiv \sum_{j=1}^{(p-1)/2} \left[\frac{2aj}{p}\right] \pmod 2.$$

于是，根据众所周知的同余关系（例如参见 [19, 第 32 页及后续页]），即可得到该结果

$$\sum_{j=1}^{(b-1)/2} \left[\frac{2aj}{b}\right] \equiv \frac{1}{2}\left(\left(\frac{a}{b}\right) - 1\right) \pmod 2 \qquad (\text{for } b \text{ odd and } (a,b)=1),$$

其中，在这个等式中，$(\frac{a}{b})$ 是初等数论中的雅可比符号。 ■

最后，随着引理 9.3–9.6 已得到证明，并且公式 (9.1) 已在手，引理 9.1 的证明便完成了。

10 $\mathfrak{L}_k + \mathfrak{L}_{2k}$ 与 $\mathfrak{L}_{4k}$ 的消失

现在我们回到关于 $\mathfrak{p}(n, (\frac{\cdot}{17}))$ 的级数公式，即

$$\begin{aligned}\mathfrak{p}(n,(\tfrac{\cdot}{17})) = {} & \sqrt{\tfrac{2}{51}\tilde{n}^{-1}} \sum_{\substack{k=1\\(k,2p)=1}}^{\infty} \frac{\lambda_k}{2k}\Big\{\mathfrak{L}_k(n) + \mathfrak{L}_{2k}(n)\Big\} I_1\Big(\tfrac{2\pi}{k}\sqrt{\tfrac{2}{51}\tilde{n}}\Big) \\ & + \sqrt{\tfrac{2}{51}\tilde{n}^{-1}} \sum_{\substack{k=1\\4\mid k,\, p\nmid k}}^{\infty} \frac{\lambda_k}{k}\mathfrak{L}_k(n) I_1\Big(\tfrac{4\pi}{k}\sqrt{\tfrac{2}{51}\tilde{n}}\Big) \\ & + \sqrt{\tfrac{1}{3}\tilde{n}^{-1}} \sum_{\substack{k=1\\(k,2p)=p}}^{\infty} \frac{1}{2k}\Big\{4\mathfrak{L}_k^{+}(n,0) I_1\big(\tfrac{8\pi}{3k}\sqrt{3\tilde{n}}\big) + 2\mathfrak{L}_k^{+}(n,2) I_1\big(\tfrac{4\pi}{3k}\sqrt{3\tilde{n}}\big)\Big\}\end{aligned} \tag{10.1}$$

其中 $\tilde{n} = n + \frac{2}{3}$，

$$\mathfrak{L}_k(n) = \sum_{h\,(k)}{}' \phi_{h,k} \exp(-2\pi i n h/k) \qquad \text{when } p\nmid k,$$

and

$$\mathfrak{L}_k^{+}(n,m) = \sum_{\substack{h\,(k)\\ \chi_h = 1}}{}' \phi_{h,k} \exp\Big\{-2\pi i(nh + m\overline{2h})/k\Big\} \qquad \text{when } (k,2p) = p,$$

其中 $2h\overline{2h} \equiv 1 \pmod{k}$。为了处理 $\mathfrak{L}_k$ 和 $\mathfrak{L}_k^+$，我们回顾关于 的公式（2.10），$_k$ 并引入该公式中指数的记号。

定义 **n 10.1.** 设 $(h,k) = 1$，并令 $\varphi := {}^{p}{}_{(k,p),}$ 使得 $\varphi k = \mathrm{lcm}(p,k)$。我们定义 e

$$\Lambda(h,k) = \sum_{\substack{\mu\,(\varphi k)\\ \chi_\mu=+1}} \Big(\!\Big(\frac{h\mu}{k}\Big)\!\Big)\Big(\!\Big(\frac{\mu}{\varphi k}\Big)\!\Big) + \sum_{\substack{\mu\,(\varphi k)\\ \chi_\mu=-1}} \Big\{\Big(\!\Big(\frac{2h\mu}{k}\Big)\!\Big) - \Big(\!\Big(\frac{h\mu}{k}\Big)\!\Big)\Big\}\Big(\!\Big(\frac{\mu}{\varphi k}\Big)\!\Big). \tag{10.2}$$

根据上述定义，有 $\phi_{h,k} = \exp \pi i \Lambda(h,k)$，因此

$$\mathfrak{L}_k(n) = \sum_{h\,(k)}{}' \exp\Big\{\pi i \Lambda(h,k) - 2\pi i n h/k\Big\} \qquad \text{when } p\nmid k, \tag{10.3}$$

and

$$\mathfrak{L}_k^+(n,m) = \sum_{\substack{h\,(k)\\ \chi_h=1}}{}' \exp\Big\{\pi i \Lambda(h,k) - 2\pi i (nh + m\overline{2h})/k\Big\} \qquad \text{when } (k,2p) = p,$$

其中再次有 $2h2h\overline{} \equiv 1 \pmod{k}$。通过使用 $_1{}_2(1 \pm \chi_\mu)$ 作为集合 $\{\mu : \chi_\mu = \pm 1\}$ 的示性函数，可由 (10.2) 轻易推出将 $\Lambda(h,k)$ 与戴德金和 s 和 s_χ 联系起来的下述公式；为强调起见，我们将其表述为一个引理。

引理 10.2. 对于 $k \geq 1$ 和 $(h,k) = 1$，有

$$\Lambda(h,k) = \tfrac{1}{2}\Big\{2s_\chi(h,k) - s_\chi(2h,k)\Big\} + \tfrac{1}{2}\Big\{s(2h,k) - s(2hp,k)\Big\}. \tag{10.4}$$

现在证明，(10.1) 中的第一项和在 n 为奇数时为零。

引理 10.3。 固定 $p \equiv 1 \pmod 8$。对于满足 $(k、\ p) = 1$ 的奇数 k，有

$$\mathfrak{L}_{2k}(n) = (-1)^n \mathfrak{L}_k(n).$$

证明。令 φ 表示欧拉函数。给定 $(k,\ 2p) = 1$，我们注意到：若 h 遍历模 k 的 $\varphi(k)$ 个可逆元剩余类，则 $2h+k$ 遍历模 $2k$ 的 $\varphi(2k)$ 个 $= \varphi(k)$ 可逆元剩余类。由 $\mathfrak{L}_{2k}(n)$ 的定义可得

$$\begin{aligned}\mathfrak{L}_{2k}(n) &= \sum_{h\,(k)}{}' \exp\Big\{\pi i \Lambda(2h+k,2k) - 2\pi i n(2h+k)/2k\Big\}\\ &= (-1)^n \sum_{h\,(k)}{}' \exp\Big\{\pi i \Lambda(2h+k,2k) - 2\pi i n h/k\Big\}.\end{aligned}$$

将其与 (10.3) 比较，只需证明

$$\Lambda(2h+k,2k) - \Lambda(h,k) \equiv 0 \pmod 2$$

对于 $(h,\ k) = 1$。根据公式 (10.4)，有

$$\Lambda(2h+k,2k) = \frac{1}{2}\Big\{2s_\chi(2h+k,2k) - s_\chi(4h+2k,2k)\Big\} + \frac{1}{2}\Big\{s(4h+2k,2k) - s(4hp+2kp,2k)\Big\}.$$

利用 k-周期性（在 h 中）以及 s 和 s_χ，并结合“缩放性质”（8.4）和（8.9），可化简为

$$\Lambda(2h+k,2k) = \tfrac{1}{2}\Big\{2s_\chi(2h+k,2k) - s_\chi(2h,k)\Big\} + \tfrac{1}{2}\Big\{s(2h,k) - s(2hp,k)\Big\},$$

由此可得

$$\Lambda(2h+k,2k)-\Lambda(h,k)=s_\chi(2h+k,2k)-s_\chi(h,k). \tag{10.5}$$

利用互反公式（8.15），（10.5）的右侧为

$$\begin{aligned}s_\chi(2h+k,2k)-s_\chi(h,k)&=\Big\{\frac{2h+k}{4k}B_2(\chi)-\tilde{s}_\chi(2k,2h+k)\Big\}-\Big\{\frac{h}{2k}B_2(\chi)-\tilde{s}_\chi(k,h)\Big\}\\&=\tfrac14 B_2(\chi)+\tilde{s}_\chi(k,h)-\tilde{s}_\chi(2k,2h+k),\end{aligned}$$

因此

$$\Lambda(2h+k,2k)-\Lambda(h,k)=\tfrac14 B_2(\chi)+\tilde{s}_\chi(k,h)-\tilde{s}_\chi(2k,2h+k).$$

因此，我们需要考虑后一个量模 2 的情形。由于 $(2k,2h+k)=1$ 根据我们对 h 和 k的假设，由引理 8.6 和 9.1 可推出

$$s_\chi(2h+k,2k)-s_\chi(h,k)\equiv\tfrac12(\chi_k-1)-\tfrac12(\chi_{2k}-1)\equiv\tfrac12(\chi_k-\chi_2\chi_k)\pmod 2,$$

结果由此得出，因为 $\chi_2=1$ 对于 $p\equiv1$ （模 8）。 ■

引理 10.4. 固定 $p\equiv1$ （模 8），并令 $(k,p)=1$。有

$$\mathfrak{L}_{4k}(n)=0\qquad \textit{for odd } n\geq1.$$

证明。由观察可知

$$\begin{aligned}\mathfrak{L}_{4k}(n)&=\sum_{h\,(2k)}{}'\left(\exp\Big\{\pi i\Lambda(h,4k)-2\pi i\frac{nh}{4k}\Big\}+\exp\Big\{\pi i\Lambda(h+2k,4k)-2\pi i\frac{(h+2k)n}{4k}\Big\}\right)\\&=\sum_{h\,(2k)}{}'\Big(\exp\big\{\pi i\Lambda(h,4k)\big\}+(-1)^n\exp\big\{\pi i\Lambda(h+2k,4k)\big\}\Big)\exp\Big\{-\pi i\frac{nh}{2k}\Big\},\end{aligned}$$

我们看到，只需证明（对于相关的 h）

$$\Lambda(h+2k,4k)-\Lambda(h,4k)\equiv0\pmod 2.$$

以类似于（10.5）的方式，我们很快得到

$$\Lambda(h+2k,4k)-\Lambda(h,4k)=s_\chi(h+2k,4k)-s_\chi(h,4k).$$

由于 $(h,\ 2k)=1$ 必然成立，显然 $(h+2k,\ 4k)=(h,\ 4k)=1$，并且由此可得（如引理 10.3的证明所示），$s_\chi(h+2k,\ 4k)-s_\chi(h,\ 4k)$ 等于

$$\tfrac14 B_2(\chi)+\tilde{s}_\chi(4k,h)-\tilde{s}_\chi(4k,h+2k)\equiv\tfrac12\big(\chi_{4k}-\chi_{4k}\big)\equiv0\pmod 2,$$

结论得证。 ■

本节的结果表明：对于奇数 n，级数（10.1）化简为

$$\mathfrak{p}(n,(\tfrac{-}{17}))=\sqrt{\tfrac13\tilde{n}^{-1}}\sum_{\substack{k=1\\(k,2p)=p}}^{\infty}\frac{1}{2k}\Big\{4\mathfrak{L}_k^+(n,0)I_1\Big(\tfrac{8\pi}{3k}\sqrt{3\tilde{n}}\Big)+2\mathfrak{L}_k^+(n,2)I_1\Big(\tfrac{4\pi}{3k}\sqrt{3\tilde{n}}\Big)\Big\}. \tag{10.6}$$

因此，为完成定理 1.1 的证明，还需考察以下求和式 $\mathfrak{L}_k^+(n,m)$，其中 $(k,2p)=1$。

11 和 $\mathfrak{L}_K^+(n,\ m)$ 的和

下文中，为强调被 p 整除，我们用 $K=kp$ 代替 k。转而考察$\mathfrak{L}_K^+(n,\ m)$，我们回顾如下事实:

$$\mathfrak{L}_K^+(n,m)=\sum_{\substack{h\,(K)\\ \chi_h=1}}{}'\exp\Big\{\pi i\Lambda(h,K)-2\pi i(nh+m\overline{2h})/K\Big\},\tag{11.1}$$

满足 $x\bar{x}\equiv 1$ (模 K)。现在我们来证明

$$\mathfrak{L}_K^+(n,0)=\mathfrak{L}_K^+(n,2)=0\qquad \text{for } n\equiv 0,2,8,10 \pmod{17},\tag{11.2}$$

由此，结合（10.6），可得定理 1.1。为证明（11.2），我们证明（以用于（11.1））：对于适当的 m 和 n，对每个模 h_1（模 K）的可逆元，若其为四次剩余（模 p），则存在唯一的模 h_2（模 K）可逆元，它是二次剩余但非四次剩余（模 p），且满足

$$\exp\Big\{\pi i\Lambda(h_1,K)-2\pi i\frac{h_1n+\overline{2h}_1m}{K}\Big\}=(-1)^n\exp\Big\{\pi i\Lambda(h_2,K)-2\pi i\frac{h_2n+\overline{2h}_2m}{K}\Big\}.$$

这个关系等价于

$$\Big\{\Lambda(h_1,K)-\frac{2(h_1n+\overline{2h}_1m)}{K}\Big\}-\Big\{\Lambda(h_2,K)-\frac{2(h_2n+\overline{2h}_2m)}{K}\Big\}\equiv 1 \pmod 2,$$

这又等价于

$$24K\Big\{\Lambda(h_1,K)-\Lambda(h_2,K)\Big\}-48\Big\{(h_1-h_2)n+\bar{2}(\bar{h}_1-\bar{h}_2)m\Big\}\equiv 24K \pmod{48K}.\tag{11.3}$$

为证明这一模 $48K$ 的同余关系，我们将该关系拆分为模 16 和 $3K$ 的同余关系，并在接下来的两节中分别处理。

12 $\Lambda(h,\ K)$ 模 $3K$ 的同余式

固定奇数 $K=kp$，我们首先考察 $24K\Lambda(h,\ K)$ 模 K、3 和 $3K$ 的情形。在本节中，我们始终假设 $(h,\ K)=1$，并令

$$\vartheta:=(3,K)=(3,k).$$

回顾方程 (10.4)，可知

$$24K\Lambda(h,K)=12K\Big\{2s_\chi(h,K)-s_\chi(2h,K)\Big\}+12K\Big\{s(2h,K)-s(2hp,K)\Big\},\tag{12.1}$$

我们将此表达式分为两部分来考虑，首先考察 $12K\{2s_\chi(h,\ K)-s_\chi(2h,\ K)\}$。为此，我们回顾互反律（见 (8.15) 和 (8.17)）

$$2ks_\chi(h,k)=hB_2(\chi)-2k\tilde{s}_\chi(k,h)\qquad (p\nmid k),\tag{12.2a}$$

$$2hKs_\chi(h,K)=(h^2+\chi_h)B_2(\chi)-2hK\chi_hs_\chi(\hat{K},h)\qquad (p|K),\tag{12.2b}$$

$\hat{}\,\hat{}\,\hat{}$，其中 $K\hat{K}\equiv 1$ (模 h)。由于 $s_\chi(K,\ h)$ 仅取决于 K (模 h)，我们可以假设

$$K\hat{K}\equiv 1 \pmod{2h}\qquad\text{and}\qquad \hat{K}>0.$$

ˆ当 $(h,\ p)=1$ 时，我们将 (12.2a) 用于 $s_\chi(K,\ h)$ 在 (12.2b) 中，然后化简可得

$$2hKs_\chi(h,K)=\Big(h^2+(1-K\hat{K})\chi_h\Big)B_2(\chi)+2\chi_h hK\tilde{s}_\chi(h,\hat{K}). \tag{12.3}$$

应用（12.3）于 s_χ（$h,\ K$）和 s_χ（$2h,\ K$），则可得

$$\begin{aligned}12hK\Big\{2s_\chi(h,K)-s_\chi(2h,K)\Big\}&=3\chi_h(4-\chi_2)(1-\hat{K}K)B_2(\chi)\\&\quad+12\chi_h hK\Big\{2\tilde{s}_\chi(h,\hat{K})-\chi_2\tilde{s}_\chi(2h,\hat{K})\Big\}.\end{aligned} \tag{12.4}$$

在第9节中，我们看到 $\tilde{s}_\chi$（$a,\ b$）是整数值，当且仅当（$a,\ b$）$=1$ 且（$a,\ p$）$=1$。由于 $\vartheta K\,|\,3K$和 h 是模 ϑK可逆元，因此可得

$$12K\Big\{2s_\chi(h,K)-s_\chi(2h,K)\Big\}\equiv 3\chi_h\bar{h}(4-\chi_2)B_2(\chi)\ (\mathrm{mod}\ \vartheta K), \tag{12.5}$$

¯其中 $h\bar{h}\equiv 1$（模 ϑK）。

现在回到（12.1）并考察 $12K\{s$（$2h,\ K$）$-s$（$2hp,\ K$）$\}$，我们将其乘以 $2h$，然后使用缩放关系（8.4）可得

$$\begin{aligned}24hK\Big\{s(2h,K)-s(2hp,K)\Big\}&=24hKs(2h,K)-24hKs(2h,k)\\&=12(2h)(K)s(2h,K)-p\cdot 12(2h)(k)s(2h,k).\end{aligned} \tag{12.6}$$

根据戴德金和理论，我们回顾如下[7]：对于（$c,\ d$）$=1$，有

$$12dc\cdot s(d,c)\equiv d^2+1\ \big(\mathrm{mod}\,(3,c)c\big),$$

由此可得

$$\begin{aligned}12(2h)(K)s(2h,K)&\equiv 4h^2+1\ (\mathrm{mod}\ \vartheta K),\\12(2h)(k)s(2h,k)&\equiv 4h^2+1\ (\mathrm{mod}\ \vartheta k).\end{aligned}$$

将这些同余式代入（12.6），可推出

$$12K\Big\{s(2h,K)-s(2H,K)\Big\}\equiv(1-p)(2h+\overline{2h})\ (\mathrm{mod}\ \vartheta K), \tag{12.8}$$

并结合（12.5）和（12.8），我们得到了下列引理的第一部分。

引理 12.1. 设 $p\equiv 1$（模 4），设 $K=kp$ 为奇数，且（h,K）$=1$。则

$$24K\Lambda(h,K)\equiv 3\chi_h\bar{h}(4-\chi_2)B_2(\chi)-(p-1)(2h+\overline{2h})\ (\mathrm{mod}\ \vartheta K),$$

其中 $\vartheta=(3,\ K)$ 且 $x\bar{x}\equiv 1$（模 ϑK）。此外，若 $3\nmid K$，则

$$24K\Lambda(h,K)\equiv 0\ (\mathrm{mod}\ 3). \tag{12.9}$$

证明。只需证明（12.9），因此设 $3\nmid K$ 并回忆

$$24K\Lambda(h,K)=12K\Big\{2s_\chi(h,K)-s_\chi(2h,K)\Big\}+12K\Big\{s(2h,K)-s(2hp,K)\Big\}.$$

ˆ首先，将方程（12.4）两边除以 h，并注意到 $h\,|\,(1-KK)$，其中ˆ$KK\equiv 1$ (模 $2h$)，我们立即看到

$$12K\Big\{2s_\chi(h,K)-s_\chi(2h,K)\Big\}\equiv 0\ (\mathrm{mod}\ 3).$$

[7]参见，例如，[20, 第 395 页及后续页。]

其次，由于 $2(3,c)c\cdot s(d,c)$ 对所有 c 和 d (例如参见 [19, 第 27] 页），显然

$$12K\Big\{s(2h,K)-s(2hp,K)\Big\}\equiv 0 \pmod 3,$$

且（12.9）立即得出。 ■

推论 12.2. 在引理 *12.1* 的条件下，若 $p\equiv 1$ (模 8) 且 h 是二次剩余 (模 p)，则

$$24K\Lambda(h,K)\equiv 9\bar{h}B_2(\chi)-(p-1)(2h+\overline{2h}) \pmod{\vartheta K}.$$

13 $\Lambda(h,\ K)$ 模 16 的同余式

为了确定 $24K\Lambda(h,\ K)$ 模 16，我们先给出一个公式，将该量与一个“组合”量 $\tau_{\mathbf{es}}(h,K)$ 联系起来，如下述引理所示。

引理 13.1. 固定 $p\equiv 1$ (模 4)，令 $K=kp$ 为奇数，并令 $(h,K)=1$。有

$$24K\Lambda(h,K)\equiv 4(\chi_h-1)+2(2h-1)(p-1)+8\tau_{\mathbf{es}}(2h,K) \pmod{16},$$

其中

$$\tau_{\mathbf{es}}(h,K):=$$
$$\#\Big\{0<\mu<K : p\nmid\mu,\ 2|\mu,\ \mu\ is\ a\ \underline{non}quadratic \pmod p,\ and\ \{h\mu\}_K\ is\ odd\Big\},$$

其中 $\{h\mu\}_K$ 定义见 (2.2)。

证明。 在作出上述假设后，我们首先回顾

$$24K\Lambda(h,K)=12K\Big\{2s_\chi(h,K)-s_\chi(2h,K)\Big\}+12K\Big\{s(2h,K)-s(2H,K)\Big\}. \quad (13.1)$$

概括地说，我们利用这些和式的已知性质 s、t、s_χ 和 t_χ，逐步将（13.1）模 16 “削减”，从其中前面那个“带大括号”的量开始。由（8.8）回忆得

$$Ks_\chi(h,K)=hB_2(\chi)-t_\chi(h,K), \quad (13.2)$$

我们有

$$12K\Big\{2s_\chi(h,K)-s_\chi(2h,K)\Big\}=12t_\chi(2h,K)-24t_\chi(h,K),$$

并利用方程（13.2）中的公式（12.3），可写为

$$24t_\chi(h,K)=12\big(h-(1-K\hat{K})/h\big)B_2(\chi)-24K\tilde{s}_\chi(h,\hat{K}),$$

其中 $K\hat{K}\equiv 1$ (模 h) 且 $\hat{K}>0$。那么，回顾引理 8.6 中的结论 $4\,|\,B_2(\chi)$，并回顾引理 9.1中关于 $\tilde{s}_\chi$ 的结果，可得

$$24t_\chi(h,K)\equiv -12K(\chi_h-1)\equiv 4(\chi_h-1) \pmod{16},$$

并且，随后，

$$12K\Big\{2s_\chi(h,K)-s_\chi(2h,K)\Big\}\equiv 12t_\chi(2h,K)+4(\chi_h-1) \pmod{16}. \quad (13.3)$$

现在回到（13.1），并考察 $24K\{s(2h, K) - s(2H, K)\}$，我们回忆方程（8.3）指出

$$12Ks(h,K) = (K-1)\Big(2h(2K-1) - 3K\Big) - 12t(h,K),$$

由此可知

$$\begin{aligned} 12K\Big\{s(2h,K) - s(2H,K)\Big\} &= 2h(1-p)(K-1)(2K-1) + 12\Big\{t(2H,K) - t(2h,K)\Big\} \\ &\equiv 12\Big\{t(2H,K) - t(2h,K)\Big\} \pmod{16}. \end{aligned} \tag{13.4}$$

结合（13.1）、（13.3）和（13.4），我们即可推得

$$24K\Lambda(h,K) \equiv 4(\chi_h - 1) + 12\big\{t_\chi(2h,K) + t(2H,K) - t(2h,K)\big\} \pmod{16}.$$

这为我们提供了 $24K\Lambda(h, K)$ 模 16 的首次“约化”。为方便起见，令

$$T(h,K) := t_\chi(h,K) + t(H,K) - t(h,K),$$

从而上述关系表明

$$24K\Lambda(h,K) \equiv 4(\chi_h - 1) + 12T(2h,K) \pmod{16}. \tag{13.5}$$

要通过（$24K\Lambda(h, K)$ 模 16，利用（13.5），只需确定 $T(h, K)$ 模 4 的一般公式，以便将其应用于 $T(2h, K)$。

我们回顾一下，利用（8.2）和（8.7）可得

$$t(h,k) = \sum_{\mu\,(k)} \mu\Big[\frac{h\mu}{k}\Big] \quad \text{and} \quad t_\chi(h,k) = \frac{1}{\varphi}\sum_{\mu\,(\varphi k)} \mu\chi_\mu\Big[\frac{h\mu}{\varphi k}\Big],$$

分别，其中 $\varphi = \frac{p}{(k,p)}$，并回顾一个众所周知的恒等式（参见例如 [14, 第 186] 页）y

$$\sum_{\mu\,(k)} \Big[\frac{h\mu}{k}\Big] = \frac{(h-1)(k-1)}{2} \qquad \text{for } (h,k) = 1.$$

转向 $T(h, K)$，我们利用缩放关系（8.5）观察到

$$t(H,K) = t(hp,kp) \equiv p\cdot t(h,k) \pmod 4,$$

由此

$$\begin{aligned} t(H,K) - t(h,K) &= t(H,K) - \Bigg(\sum_{\substack{\mu\,(K)\\ p\nmid\mu}} \mu\Big[\frac{h\mu}{K}\Big] + \sum_{\substack{\mu\,(K)\\ p\mid\mu}} \mu\Big[\frac{h\mu}{K}\Big]\Bigg) \\ &\equiv p\cdot t(h,k) - \sum_{\substack{\mu\,(K)\\ p\nmid\mu}} \mu\Big[\frac{h\mu}{K}\Big] - p\cdot t(h,k) \equiv -\sum_{\substack{\mu\,(K)\\ p\nmid\mu}} \mu\Big[\frac{h\mu}{K}\Big] \pmod 4. \end{aligned}$$

那么，由 $t_\chi(h, K)$ 的定义可得

$$T(h,K) = t_\chi(h,K) + t(H,K) - t(h,K) \equiv \sum_{\substack{\mu\,(K)\\ p\nmid\mu}} \mu(\chi_\mu - 1)\Big[\frac{h\mu}{K}\Big] \pmod 4. \tag{13.6}$$

现在，如果 $p\nmid\mu$那么 $\chi_\mu-1$是偶数，因此（13.6）等价于同余

$$T(h,K)\equiv\sum_{\substack{\mu\,(K)\\(\mu,2p)=1}}(\chi_\mu-1)\Big[\frac{h\mu}{K}\Big]\pmod 4,$$

这显然等价于同余式

$$\tfrac12 T(h,K)\equiv\sum_{\substack{\mu\,(K)\\(\mu,2p)=1}}\Big(\frac{\chi_\mu-1}{2}\Big)\Big[\frac{h\mu}{K}\Big]\pmod 2. \tag{13.7}$$

在（13.7）中，我们的求和仅遍及奇数 μ，但为了推导，求和遍及偶数 μ更为方便。从

$$\sum_{\substack{\mu\,(K)\\(\mu,2p)=1}}\Big(\frac{\chi_\mu-1}{2}\Big)\Big[\frac{h\mu}{K}\Big]=\sum_{\substack{\mu\,(K)\\p\nmid\mu}}\Big(\frac{\chi_\mu-1}{2}\Big)\Big[\frac{h\mu}{K}\Big]-\sum_{\substack{\mu\,(K)\\(\mu,2p)=2}}\Big(\frac{\chi_\mu-1}{2}\Big)\Big[\frac{h\mu}{K}\Big],$$

我们利用以下事实[8]：

$$\sum_{\substack{\mu\,(K)\\p\nmid\mu}}\chi_\mu\Big[\frac{h\mu}{K}\Big]=0\qquad\text{and}\qquad\sum_{\substack{\mu\,(K)\\p\nmid\mu}}\Big[\frac{h\mu}{K}\Big]=\frac{(h-1)(p-1)k}{2}$$

由此可推得

$$\sum_{\substack{\mu\,(K)\\(\mu,2p)=1}}\Big(\frac{\chi_\mu-1}{2}\Big)\Big[\frac{h\mu}{K}\Big]\equiv\frac{(h-1)(p-1)}{4}+\sum_{\substack{\mu\,(K)\\(\mu,2p)=2}}\Big(\frac{\chi_\mu-1}{2}\Big)\Big[\frac{h\mu}{K}\Big]\pmod 2. \tag{13.8}$$

现在令 $[x]=x-\{x\}=\{x\}\in[0,1)$，则有

$$[h\mu/K]\equiv K[h\mu/K]\equiv h\mu+K\{h\mu/K\}\pmod 2.$$

事实上，由于 $K\{h\mu/K\}$ 等价于由（ $\{h\mu\}_K$ ）中的整数2.2，我们有

$$[h\mu/K]\equiv h\mu+\{h\mu\}_K\pmod 2,$$

并且由（13.8立即可得

$$\tfrac12 T(h,K)\equiv\frac{(h-1)(p-1)}{4}+\sum_{\substack{\mu\,(K)\\(\mu,2p)=2}}\Big(\frac{\chi_\mu-1}{2}\Big)\{h\mu\}_K\pmod 2. \tag{13.9}$$

显然，（13.9中的后一个和模2同余于

$$\#\Big\{0<\mu<K:p\nmid\mu,\,2|\mu,\,\mu\text{ is a nonquadratic }(\mathrm{mod}\ p),\text{ and }\{h\mu\}_K\text{ is odd}\Big\},$$

即 $\tau_{\mathbf{es}}$（h，K），将（ h 替换为 $2h$ ，并利用（13.9中的结果（13.5）即可得出引理的结论。■

由于确定 $\tau_{\mathbf{es}}(h,K)$ 模 2 较为技术性且繁琐，目前我们先陈述必要的结果，并在第16节给出证明。

[8]这些方程可通过简单的直接计算得出：令 $[x]=x-\{x\}$，利用 h 与 K 的互素性，并使用以下事实：$\sum_{\mu\ (K)}[h\mu/K]=\frac12(h-1)(K-1)$。

引理13.2. 固定 $p \equiv 1 \pmod 4$，设 $K = kp$ 为奇数，设 $(h, K) = 1$，并假设 h 是二次剩余 $\pmod p$。则

$$\tau_{\mathbf{es}}(h,K) \equiv \begin{cases} 0 \pmod 2 & \text{if } h \text{ is a quartic } \pmod p, \\ 1 \pmod 2 & \text{if } h \text{ is a quadratic-nonquartic } \pmod p. \end{cases}$$

推论 13.3. 固定 $p \equiv 1$ （模 8），令 $K = kp$ 为奇数，令 （h、 K） $= 1$，并假设 h 是二次剩余（模 p）。那么

$$24K\Lambda(h,K) \equiv \begin{cases} 0 \pmod{16} & \text{if } 2h \text{ is a quartic } \pmod p, \\ 8 \pmod{16} & \text{if } 2h \text{ is a quadratic-nonquartic } \pmod p. \end{cases}$$

证明。 这直接由引理13.1 和 13.2得出，因为 2 是二次剩余（模 p），当且仅当$p \equiv 1$（模 8）。 ■

14 的消失 $\mathfrak{L}_K^+$（n， m）；定理 1.1 的证明

我们终于可以证明定理 1.1了，为此我们回顾一下（来自第 11 节）： 还需证明（对于奇数 $K = kp$）

$$\mathfrak{L}_K^+(n,0) = \mathfrak{L}_K^+(n,2) = 0 \qquad \text{for } n \equiv 0,2,8,10 \pmod{17}. \tag{14.1}$$

我们还要回顾一下，我们要寻找的是由四次剩余和二次非四次剩余组成的数对（h_1， h_2）（模 p），使得

$$24K\Big\{\Lambda(h_1,K) - \Lambda(h_2,K)\Big\} - 48\Big\{(h_1-h_2)n + \bar{2}(\bar{h}_1 - \bar{h}_2)m\Big\} \equiv 24K \pmod{48K},$$

其中 $x\bar{x} \equiv 1$ （模 K）。下面的引理说明 $1 - 24n$ 和 $1 - 24m$ 模 17 的剩余类如何影响所需数对（h_1， h_2）的存在性。

引理 14.1。 固定 $p = 17$，令 $K = 17k$ 为奇数，并令 $n > 0$ 和 $m \geq 0$。固定 $g = 3$，使得 g 是一个原根 （模17），假设

$$\begin{aligned} 1 - 24n &\equiv g^{4\nu+\alpha+1} \pmod p, \\ 1 - 24m &\equiv \overline{24}(1 - g^{4\mu+\alpha}) \pmod p, \end{aligned} \qquad \text{for some } 0 \leq \alpha,\mu,\nu \leq 3. \tag{14.2}$$

那么，对于每个可逆元 h_1 （模 K），若其是四次剩余 （模 p），则存在唯一的可逆元 h_2 （模 K），它是二次非四次剩余 （模 p），并满足关系

$$24K\Big\{\Lambda(h_1,K) - \Lambda(h_2,K)\Big\} - 48\Big\{(h_1-h_2)n + \bar{2}(\bar{h}_1 - \bar{h}_2)m\Big\} \equiv 24K \pmod{48K}, \tag{14.3}$$

其中 $\bar{x}$ 表示模 $(3, K)K$ 的逆元。

推论 14.2。 在引理 *14.1*的假设下，有 $\mathfrak{L}_K^+(n,m) = 0$。

注记14.3. 尽管在下文的证明中我们固定了 $p = 17$ 和 $g = 3$，但为了说明这些量在证明中的存在及其作用，我们仍继续写作 p 和 g。

引理的证明 *14.1*。为方便起见，我们先回顾一些引理：若 $\vartheta = (3,\ K)$，$(h,\ K) = 1$，且 h 是一个二次剩余（模 p），则

$$24K\Lambda(h,K) \equiv 9\bar{h}B_2(\chi) - (p-1)(2h + \overline{2h}) \pmod{\vartheta K}. \tag{14.4a}$$

若 $(h,\ K) = 1$ 且 $3\nmid K$，则

$$24K\Lambda(h,K) \equiv 0 \pmod 3. \tag{14.4b}$$

最后，由于 2是（二次非四次剩余）（模 17），推论 13.3表明：若$(h,\ K) = 1$ 且 h 是（二次剩余）（模 p），则

$$24K\Lambda(h,K) \equiv \begin{cases} 8 \pmod{16} & \text{if } h \text{ is a quartic } (\bmod p), \\ 0 \pmod{16} & \text{if } h \text{ is a quadratic-nonquartic } (\bmod p). \end{cases} \tag{14.4c}$$

现在固定 h_1，它是模 K 的一个可逆四次剩余，并设 h_2 是某个尚待确定的模 K 可逆二次非四次剩余。由于同余式 (14.4a) 的形式与 $\vartheta = (3,\ K)$ 无关，为简单起见，我们只证明$3\nmid K$的情形，因此 $\vartheta K = K$。观察 (14.3)，令

$$D_K := 24K\Big(\Lambda(h_1,K) - \Lambda(h_2,K)\Big) - 48\Big((h_1-h_2)n + \bar{2}(\bar{h}_1 - \bar{h}_2)m\Big) - 24K,$$

因此我们的任务是证明

$$D_K \equiv 0 \pmod{48K}.$$

由 (14.4b) 可立即得到

$$D_K \equiv 0 \pmod 3,$$

由（14.4c）可得

$$D_K \equiv 8 - 0 - 8 \equiv 0 \pmod{16},$$

因此，只需证明 $D_K \equiv 0$ （模 K）。

暂且令

$$X := h_1 - h_2, \quad Y := \bar{h}_1 - \bar{h}_2, \quad \text{and} \quad Z := 9B_2(\chi) - \bar{2}(p+1),$$

利用（14.4a），可得

$$\begin{aligned} D_K &\equiv 9YB_2(\chi) - (2X + \bar{2}Y)p - \bar{2}Y + 2(1-24n)X - 24Ym \pmod K \\ &\equiv YZ - 2pX + 2(1-24n)X + (1-24m)Y \pmod K. \end{aligned}$$

注意到

$$X = h_1h_2(\bar{h}_2 - \bar{h}_1) = -h_1h_2Y,$$

我们进一步化简

$$\begin{aligned} D_K &\equiv Y\Big(Z + 2ph_1h_2 - 2h_1h_2(1-24n) + (1-24m)\Big) \pmod K \\ &\equiv (\bar{h}_2 - \bar{h}_1)\Big(2h_1h_2(1-24n-p) - (1-24m) - Z\Big) \pmod K \\ &\equiv (\bar{h}_2 - \bar{h}_1)d_K(h_2) \pmod K, \end{aligned}$$

其中

$$d_K(x) := 2h_1(1-24n-p)x - (1-24m) - 9B_2(\chi) + \bar{2}(p+1).$$

由于 m、 n和 h_1 是固定的，我们的证明归结为表明存在唯一的可逆元h_2 （模 K），它是模 p的二次非四次剩余，并且满足

$$D_K \equiv (\bar{h}_2 - \bar{h}_1) d_K(h_2) \equiv 0 \pmod{K}. \tag{14.5}$$

令 $K = p^a k$ 为 $a \geq 1$，并令（k, p）为 $= 1$。只需指定 $h_2 \equiv h_1$ （模 k），即可确保

$$D_K \equiv (\bar{h}_2 - \bar{h}_1) d_K(h_2) \equiv 0 \pmod{k},$$

因此只需确保 $D_K \equiv 0$ （模 p^a）。

在关于 h_1 和 h_2的假设下，令

$$h_1 \equiv g^{4\eta} \pmod{p} \qquad \text{and} \qquad h_2 \equiv g^{4\lambda+2} \pmod{p},$$

其中 $0 \leq \eta, \lambda \leq 3$，并回顾我们的假设：

$$1 - 24n \equiv g^{4\nu+\alpha+1} \pmod{p} \qquad \text{and} \qquad 1 - 24m \equiv \overline{24}(1 - g^{4\mu+\alpha}) \pmod{p}.$$

计算（对于 $p = 17$ 和 $g = 3$）可得

$$2 \equiv \bar{g}^2 \pmod{p}, \quad \overline{24} \equiv 5 \equiv g^5 \pmod{p}, \quad \text{and} \quad Z \equiv 12 \pmod{p},$$

我们有

$$d_K(h_2) \equiv g^{4(\eta+\lambda+\nu)+\alpha+1} - 5(1 - g^{4\mu+\alpha}) - 12 \equiv \left(g^{4(\eta+\lambda+\nu)} + g^{4(\mu+1)}\right) g^{\alpha+1} \pmod{p}.$$

要使 $d_K(h_2) \equiv 0$ (模 p)，那么我们需要

$$g^{4(\eta+\lambda+\nu)} \equiv -g^{4(\mu+1)} \equiv g^{4(\mu+3)} \pmod{p},$$

因此，只需满足 $\eta + \lambda + \nu \equiv \mu + 3$ (模 4)。也就是说，只需有

$$\lambda \equiv \mu - \nu - \eta + 3 \pmod{4}. \tag{14.6}$$

因此，按照（ $0 \leq \lambda \leq 3$ 14.6）进行选取，并选取某个 $h_* \equiv g^{4\lambda+2}$ （模 p），所述 h_* 确实是一个二次非四次剩余（模 p），使得 d_K（h_*） $\equiv 0$ （模 p）。

导数

$$d'_K(x) = 2h_1(1 - 24n - p) \equiv 2h_1(1 - 24n) \not\equiv 0 \pmod{p},$$

由此，亨泽尔引理保证存在唯一的 h_2 (模 p^a)，使得

$$h_2 \equiv h_* \pmod{p} \qquad \text{and} \qquad d_K(h_2) \equiv 0 \pmod{p^a}.$$

确定了 h_2 (模 p^a)，并指定 $h_2 \equiv h_1$ (模 k)后，中国剩余定理给出唯一的 h_2 (模 K)，它具有所需性质，并满足（14.5），引理得证。■

定理 1.1 的证明。现在回到方程（10.6），我们利用推论 14.2来验证关于 $\mathfrak{L}_K^+(n,\ 0)$ 和 $\mathfrak{L}_K^+(n,\ 2)$ 在（14.1）中的断言；我们再次固定 $p = 17$和 $g = 3$，它是模 17的原根。

当 $m = 0$ 在（14.2）中时，我们看到 α 必须满足

$$1 \equiv \overline{24}(1 - g^{4\mu+\alpha}) \pmod{17}, \qquad \text{which implies that} \qquad \alpha = 3.$$

因此，我们要求 $1-24n \equiv g^{4(\nu+1)}$ （模 **17**），也就是说 $1-24n$ 是一个四次剩余（模17）。当 $m=2$ 我们再次发现 $\alpha=3$，因此 $1-24n$ 必须再次是一个四次剩余（模17）。由推论14.2 可知

$$\mathfrak{L}_K^+(n,0) = \mathfrak{L}_K^+(n,2) = 0 \qquad \text{when } n \equiv 0,2,8,10 \pmod{17}. \tag{14.7}$$

根据方程 **(**10.6**)**，对于奇数 n 我们有

$$\mathfrak{p}(n,(\tfrac{\cdot}{17})) = \sqrt{\tfrac{1}{3}\tilde{n}^{-1}} \sum_{\substack{k=1\\(k,2p)=p}}^{\infty} \frac{1}{2k}\Big\{4\mathfrak{L}_k^+(n,0) I_1\Big(\tfrac{8\pi}{3k}\sqrt{3\tilde{n}}\Big) + 2\mathfrak{L}_k^+(n,2) I_1\Big(\tfrac{4\pi}{3k}\sqrt{3\tilde{n}}\Big)\Big\},$$

因此，我们得出

$$\mathfrak{p}(n,(\tfrac{\cdot}{17})) = 0 \qquad \text{for} \quad n \equiv \begin{cases} 1 & \pmod 2, \\ 0,2,8,10 & \pmod{17}. \end{cases}$$

这显然等价于

$$\mathfrak{p}(n,(\tfrac{\cdot}{17})) = 0 \qquad \text{for} \quad n \equiv 17,19,25,27 \pmod{34},$$

并且定理 1.1的证明至此完成。

15 $\mathfrak{p}$的消失$(n,\ -(\frac{\cdot}{17}))$ —

现在我们转而讨论 $\mathfrak{p}(n,-(\frac{\cdot}{17}))$ 并证明定理 1.2，该定理指出

$$\mathfrak{p}(n,-(\tfrac{\cdot}{17})) = 0 \qquad \text{for all } n \equiv 11,15,29,33 \pmod{34}.$$

我们注意到，关于 n 的这个同余条件等价于以下条件： n 为奇数，且 $1-24n$ 是模17的二次非四次剩余。定理 1.2 的证明与定理 1.1的证明相当相似，因此我们只说明两者之间的细微差别。

粗略地说，生成函数的函数方程

$$\Phi^\dagger(x) = \prod_{a=1}^{p-1}(-\chi_a x^a; x^p)_\infty^{-1} = \sum_{n=0}^{\infty}\mathfrak{p}(n,-\chi)x^n$$

始终与 $\Phi(x)$ 的函数方程相呼应，但其中的集合 $\mathbf{r}$ 和 $\mathbf{s}$ 互换。特别地，我们有

$$\Phi^\dagger(x) = \frac{F_{\mathbf{r}}(x^2)}{F_{\mathbf{r}}(x)}F_{\mathbf{s}}(x), \qquad \text{while} \qquad \Phi(x) = F_{\mathbf{r}}(x)\frac{F_{\mathbf{s}}(x^2)}{F_{\mathbf{s}}(x)}.$$

15.1 **关于** $\mathfrak{p}(n,-(\frac{\cdot}{17}))$**的拉德马赫级数展开。** 我们首先简要讨论类似于（7.4）的公式如何推导，用于 $\mathfrak{p}(n,-(\frac{\cdot}{17}))$。我们回顾一下， —

$$q := \frac{p-1}{2} \qquad \text{and} \qquad \sum_{\mu\in\mathbf{r}\cup\mathbf{s}}\mathcal{B}_\mu = \sum_{\mu=1}^{(p-1)/2}\mathcal{B}_\mu = -pq.$$

类比于（2.9）和（2.10），令

$$\phi^{\dagger}_{h,k}=\frac{\omega_{\mathbf{r}}(2h,k)}{\omega_{\mathbf{r}}(h,k)}\omega_{\mathbf{s}}(h,k)=\exp\{\pi i\Lambda^{\dagger}(h,k)\},$$

其中（参见（10.2）和（10.4））

$$\begin{aligned}\Lambda^{\dagger}(h,k):=&\sum_{\substack{\mu\,(\varphi k)\\ \chi_\mu=1}}\left\{\left(\!\!\left(\frac{2h\mu}{k}\right)\!\!\right)-\left(\!\!\left(\frac{h\mu}{k}\right)\!\!\right)\right\}\left(\!\!\left(\frac{\mu}{\varphi k}\right)\!\!\right)+\sum_{\substack{\mu\,(\varphi k)\\ \chi_\mu=-1}}\left(\!\!\left(\frac{h\mu}{k}\right)\!\!\right)\left(\!\!\left(\frac{\mu}{\varphi k}\right)\!\!\right)\\ =&\frac12\Big\{s_\chi(2h,k)-2s_\chi(h,k)\Big\}+\frac12\Big\{s(2h,k)-s(2H,k)\Big\},\end{aligned}\tag{15.1}$$

再次有 $\varphi=\ ^{k}\!/_{(k,\ p)}$。

当 $(k,\ 2p)\ =p$ 时，$\Phi^{\dagger}(x)$ 的函数方程为

$$\Phi^{\dagger}(x)=\phi^{\dagger}_{h,k}\exp\left\{\frac{\pi q}{6k}\left[\left(-\frac{3}{q}\chi_h\Big(1-\frac{\chi_2}{4}\Big)B_2(\chi)-\frac14\right)z^{-1}+z\right]\right\}\times\begin{cases}S^{+}(y'),&\text{if }\chi_h=-1,\\ S^{-}(y'),&\text{if }\chi_h=+1,\end{cases}\tag{15.2}$$

其中 $S^{\pm}(y')$ 由（3.7ii）和（3.7iii）给出；注意（15.2）与（3.7）中的符号差异。这种符号差异造成的一个结果是：级数$\mathfrak{p}_{(p)}(n,\ \chi)$ 的“主项” h 对应于二次剩余（模 p），而级数 $\mathfrak{p}_{(p)}(n,\ -\chi)$ 的类似“主项” h 则对应于 非二次剩余（模 p）。特别地，我们推导出类似的公式

$$\mathfrak{p}_{(p)}(n,-\chi)=\frac{1}{\sqrt{\tilde n}}\sum_{\substack{k=1\\(k,2p)=p}}^{\infty}\sum_{\substack{m=0\\c_m>0}}^{\infty}\frac{\sqrt{c_m}}{2k}\sigma^{+}_m\big(\mathfrak{L}^{\dagger}_k\big)^{-}(n,m)\,I_1\Big(\tfrac{2\pi}{k}\sqrt{c_m\tilde n}\Big),$$

其中

$$c_m=\Big(1-\frac{\chi_2}{4}\Big)B_2(\chi)-\frac{p-1}{24}-2m,\qquad \tilde n=n+\frac{p-1}{24},$$

$$\big(\mathfrak{L}^{\dagger}_k\big)^{-}(n,m)=\sum_{\substack{h\,(k)\\ \chi_h=-1}}{}'\ \phi^{\dagger}_{h,k}\exp\big(-2\pi i(nh+m\overline{2h})/k\big)\quad\big(\text{for }(K,2p)=p\big),$$

且σ^{+}_m 是 $S^{+}(x)$的级数系数。

仿照（3.8i）和（3.9i）的平行方式，对于 k 与 p 互素，令

$$\lambda^{\dagger}_k:=2^{-\frac{p-1}{4}}\prod_{\mathbf{r}}\frac{\csc(\pi\|2\bar kr\|/p)}{\csc(\pi\|\bar kr\|/p)}\prod_{\mathbf{s}}\csc(\pi\|\bar ks\|/p)\qquad\text{if }2|k,$$

并令

$$\lambda^{\dagger}_k:=2^{-\frac{p-1}{4}}\prod_{\mathbf{s}}\csc(\pi\|\bar ks\|/p)\qquad\text{if }2\nmid k.$$

对于克洛斯特曼型和 $\mathfrak{L}^{\dagger}_k$ 和 $\big(\mathfrak{L}^{\dagger}_k\big)^{-}$，第 5 节的公式和界可以直接应用于 $\mathfrak{L}^{\dagger}_k$ 和 $\big(\mathfrak{L}^{\dagger}_k\big)^{-}$，因为这些“匕首和”的相关公式与 $\mathfrak{L}_k$ 和 $\mathfrak{L}^{+}_k$ 的相同，只需将$\mathbf{r}$ 和 $\mathbf{s}$ 互换即可。

按照与（7.3）相同的步骤，我们得到，同样对于 $p<24$，有

$$\begin{aligned}\mathfrak{p}(n,-\chi)&=\mathfrak{p}_{(1)}(n,-\chi)+\mathfrak{p}_{(2)}(n,-\chi)+\mathfrak{p}_{(p)}(n,-\chi)\\&=\frac{\kappa_p}{4\pi\sqrt{\tilde{n}}}\sum_{\substack{k=1\\(k,2p)=1}}^{\infty}\frac{1}{2k}\Big\{\lambda_k^\dagger\mathfrak{L}_k^\dagger(n)+\lambda_{2k}^\dagger\mathfrak{L}_{2k}^\dagger(n)\Big\}I_1\Big(\frac{\kappa_p}{2k}\sqrt{\tilde{n}}\Big)\\&\quad+\frac{\kappa_p}{4\pi\sqrt{\tilde{n}}}\sum_{\substack{k=1\\4\mid k,\,p\nmid k}}^{\infty}\frac{\lambda_k^\dagger}{k}\mathfrak{L}_k^\dagger(n)I_1\Big(\frac{\kappa_p}{k}\sqrt{\tilde{n}}\Big)\\&\quad+\frac{1}{\sqrt{\tilde{n}}}\sum_{\substack{k=1\\(k,2p)=p}}^{\infty}\sum_{\substack{m=0\\c_m>0}}^{\infty}\frac{\sqrt{c_m}}{2k}\sigma_m^-\big(\mathfrak{L}_k^\dagger\big)^-(n,m)\,I_1\Big(\frac{2\pi}{k}\sqrt{c_m\tilde{n}}\Big).\end{aligned}$$

对于 $p=17$，于是我们有

$$\begin{aligned}\mathfrak{p}(n,-(\tfrac{\cdot}{17}))&=\sqrt{\tfrac{2}{51}\tilde{n}^{-1}}\sum_{\substack{k=1\\(k,2p)=1}}^{\infty}\frac{\lambda_k^\dagger}{2k}\Big\{\mathfrak{L}_k^\dagger(n)+\mathfrak{L}_{2k}^\dagger(n)\Big\}I_1\Big(\tfrac{2\pi}{k}\sqrt{\tfrac{2}{51}\tilde{n}}\Big)\\&\quad+\sqrt{\tfrac{2}{51}\tilde{n}^{-1}}\sum_{\substack{k=1\\4\mid k,\,p\nmid k}}^{\infty}\frac{\lambda_k^\dagger}{k}\mathfrak{L}_k^\dagger(n)I_1\Big(\tfrac{4\pi}{k}\sqrt{\tfrac{2}{51}\tilde{n}}\Big)\\&\quad+\sqrt{\tfrac{1}{3}\tilde{n}^{-1}}\sum_{\substack{k=1\\(k,2p)=p}}^{\infty}\frac{1}{2k}\Big\{4\big(\mathfrak{L}_k^\dagger\big)^-(n,0)I_1\Big(\tfrac{8\pi}{3k}\sqrt{3\tilde{n}}\Big)+2\big(\mathfrak{L}_k^\dagger\big)^-(n,2)I_1\Big(\tfrac{4\pi}{3k}\sqrt{3\tilde{n}}\Big)\Big\}.\end{aligned}$$

15.2 $\Lambda^\dagger(h,\ K)$的同余式。

引理 15.1（参见引理 12.1 和推论 12.2）。设 $p\equiv 1\pmod 8$，设 $K=kp$ 为奇数，并设 $(h,K)=1$ 且 $\chi_h=-1$。那么

$$24K\Lambda^\dagger(h,K)\equiv -9\bar{h}B_2(\chi)-(p-1)(2h+\overline{2h})\pmod{\vartheta K},$$

其中 $\vartheta=(3,K)$ 且 $x\bar{x}\equiv 1$(模 ϑK)。此外，若 $3\nmid K$，则

$$24K\Lambda^\dagger(h,K)\equiv 0\pmod 3.$$

证明。利用（15.1），证明与引理 12.1 的证明几乎完全相同 . ■

或许，Λ（h，K）与 $\Lambda^\dagger$（h，K）之间最显著的差异在于它们分别模16的同余式，尤其是引理13.1和推论13.3的“dagger-类比”。由（15.1）可得

$$24K\Lambda^\dagger(h,K)=12K\big\{s_\chi(2h,K)-2s_\chi(h,K)\big\}+12K\big\{s(2h,K)-s(2H,K)\big\},$$

并且，正如方程（13.1）导出引理 13.1一样，这个关于 $24K\Lambda^\dagger(h,\ K)$ 的公式导出关系式

$$24K\Lambda^\dagger(h,K)\equiv 4(\chi_h-1)+2(2h-1)(p-1)+8\tau_{\mathbf{er}}(2h,K)\pmod{16},\tag{15.4}$$

其中

$$\tau_{\mathbf{er}}(h,K) := \#\Big\{0<\mu<K : p\nmid\mu,\ 2|\mu,\ \mu \text{ is a quadratic } (\mathrm{mod}\ p), \text{ and } \{h\mu\}_K \text{ is odd}\Big\}.$$

如第13节所述，我们暂且只记录$\tau_{\mathbf{er}}(h,K)$ 模 2 的必要同余式，并将证明留待第 16节。

引理 15.2。 设 $p\equiv 1$ **(模 4)**，取 g 为模 p的一个原根，令 $K=kp$ 为奇数，并令 h 为一个非二次剩余 **(模** p**)**，且 $(h,K)=1$。有

$$\tau_{\mathbf{er}}(h,K)\equiv\begin{cases}1\ (\mathrm{mod}\ 2) & \textit{if } \bar{g}h \textit{ is a quartic } (\mathrm{mod}\ p),\\ 0\ (\mathrm{mod}\ 2) & \textit{if } \bar{g}h \textit{ is a quadratic-nonquartic } (\mathrm{mod}\ p).\end{cases}$$

推论 15.3。 固定 $p=17$ 和 $g=3$，使得 g 为模 p的一个原根；令$K=17k$ 为奇数，并令 h 为一个非二次剩余 **(模** p**)**，且 $(h,K)=1$。有

$$24K\Lambda^{\dagger}(h,K)\equiv\begin{cases}8\ (\mathrm{mod}\ 16) & \textit{if } \bar{g}h \textit{ is a quartic } (\mathrm{mod}\ p),\\ 0\ (\mathrm{mod}\ 16) & \textit{if } \bar{g}h \textit{ is a quadratic-nonquartic } (\mathrm{mod}\ p).\end{cases}$$

证明。 这由方程 **(**15.4**)**、引理 15.2，以及以下事实得出：2 是模 17的二次剩余但非四次剩余。 ■

15.3 **定理 1.2的证明**。 以下引理的形式分别与引理 10.3 和 10.4完全相同，其相应证明也一样，只需作相应的修改。

引理 15.4. 设 $p\equiv 1$ （模 8），并设（k,p）$=1$，其中 k 为奇数。则有 s

$$\mathfrak{L}^{\dagger}_{2k}(n)=(-1)^n\mathfrak{L}^{\dagger}_{k}(n)\qquad \textit{for } n\geq 1.$$

引理 15.5. 设 $p\equiv 1$ （模 8），并设（k,p）$=1$。则有

$$\mathfrak{L}^{\dagger}_{4k}(n)=0\qquad \textit{for odd } n\geq 1.$$

现在回顾一下

$$\big(\mathfrak{L}^{\dagger}_{K}\big)^{-}(n,m)=\sum_{\substack{h\,(K)\\ \chi_h=-1}}{}' \exp\Big\{\pi i\Lambda^{\dagger}(h,K)-2\pi i(nh+m\overline{2h})/K\Big\},$$

其中 $2h\overline{2h}\equiv 1$ （模 K）。

引理 15.6 （参见引理 14.1和推论 14.2）。 固定 $p=17$ 和 $g=3$，使得 g 是模 p的原根，令 $K=17k$ 为奇数，并令 $n>0$ 和 $m\geq 0$。若有

$$\begin{aligned}1-24n &\equiv g^{4\nu+\alpha} && (\mathrm{mod}\ p),\\ 1-24m &\equiv \overline{24}(1-g^{4\mu+\alpha+1}) && (\mathrm{mod}\ p),\end{aligned}$$

对某些 $0\leq\alpha,\mu,\nu\leq 3$ 成立，则 $\big(\mathfrak{L}^{\dagger}_{K}\big)^{-}(n,m)=0$。

证明。 这可以通过与证明引理 14.1和推论 14.2时几乎相同的论证得出，其中分别用引理 15.1 和推论15.3 代替引理12.1和推论 13.3。 ■

仿照方程（14.7）的计算（保持 $K = 17k$ 为奇数），当 $m = 0$关系 $1 \equiv 24\ (1 - g^{4\mu+\alpha+1})$ 模 **17** 意味着 $\alpha = \overline{2,}$ 因此 $1 - 24n$ 必为二次非四次剩余（模 17）。当 $m = 2$ 我们再次得到 $\alpha = 2,$ 由此

$$\left(\mathfrak{L}_K^{\dagger}\right)^{-}(n, 0) = \left(\mathfrak{L}_K^{\dagger}\right)^{-}(n, 2) = 0 \qquad \text{when } n \equiv 11, 12, 15, 16 \pmod{17}.$$

因此，有

$$\mathfrak{p}(n, -(\tfrac{\cdot}{17})) = 0 \qquad \text{for } n \equiv \begin{cases} 1 & \pmod 2, \\ 11, 12, 15, 16 & \pmod{17}, \end{cases}$$

这等价于如下陈述：

$$\mathfrak{p}(n, -(\tfrac{\cdot}{17})) = 0 \qquad \text{for } n \equiv 11, 15, 29, 33 \pmod{34},$$

且定理 1.2 的证明至此完成。

16 传递引理

最后，我们利用引理 $\tau_{\mathbf{er}}$ 和 $\tau_{\mathbf{es}}$ 建立其模 2 初等同余式15.2 和13.2；首先回顾

$$\tau_{\mathbf{er}}(h, K) = \#\Big\{0 < \mu < K : p\nmid\mu,\ 2|\mu,\ \mu \text{ is a quadratic } (\mathrm{mod}\ p), \text{ and } \{h\mu\}_K \text{ is odd}\Big\},$$

and

$$\tau_{\mathbf{es}}(h, K) = \#\Big\{0 < \mu < K : p\nmid\mu,\ 2|\mu,\ \mu \text{ is a nonquadratic } (\mathrm{mod}\ p), \text{ and } \{h\mu\}_K \text{ is odd}\Big\},$$

其中 $\{x\}_K$ 满足

$$x \equiv \{x\}_K \pmod p \qquad \text{and} \qquad 0 \le \{x\}_K < K.$$

出于独立的兴趣，我们还推导了类似的 τ量的同余式，这些量对 μ(mod p)的奇偶性与“剩余性”具有不同的条件对。为说明我们的计算，我们首先需要适度的记号“投入”。

(1) 对 $k \ge 1$，令

$$\mathbf{e}(k) := \{0 < e < k : p\nmid e,\ e \text{ even}\},$$
$$\mathbf{o}(k) := \{0 < o < k : p\nmid o,\ o \text{ odd}\},$$

并进一步令

$$\mathbf{r}(k) := \{0 < r < k : p\nmid r,\ r \text{ is a quadratic } (\mathrm{mod}\ p)\},$$
$$\mathbf{s}(k) := \{0 < s < k : p\nmid s,\ s \text{ is a nonquadratic } (\mathrm{mod}\ p)\}.$$

注： 我们此前用 **r** 和 **s** 分别表示范围 $\{1, \ldots, \frac{p-1}{2}\}$ 内的二次剩余集合与非二次剩余集合。为避免进一步“符号泛滥”，本节（且仅限本节）专门使用上文定义的 **r**(k) 和 **s**(k)。

(2) 对于 $k \geq 1$，令 $\mathbf{er}(k)$ 和 $\mathbf{es}(k)$ 分别表示 $\mathbf{r}(k)$ 和 $\mathbf{s}(k)$ 中偶元素的集合；也就是说，令

$$\mathbf{er}(k) := \mathbf{e}(k) \cap \mathbf{r}(k) \qquad \text{and} \qquad \mathbf{es}(k) := \mathbf{e}(k) \cap \mathbf{s}(k).$$

奇元素的集合 $\mathbf{or}(k)$ 和 $\mathbf{os}(k)$ 的定义类似。

(3) 对于 $K = kp$ 奇数且 h 满足 $(h, K) = 1$ 的情形，根据其定义，我们有 e

$$\tau_{\mathbf{er}}(h, K) = \#\{r \in \mathbf{er}(K) : \{hr\}_K \text{ is odd}\},$$
$$\tau_{\mathbf{es}}(h, K) = \#\{s \in \mathbf{es}(K) : \{hs\}_K \text{ is odd}\},$$

并以显而易见的类似方式定义 $\tau_{\mathbf{or}}(h, K)$ 和 $\tau_{\mathbf{os}}(h, K)$。

(4) 对于固定的一般 $p \equiv 1$ (模 4)，令 $g = g(p)$ 为 p 模下的一个原根，并定义 $i = i(p)$ 使得

$$i \equiv g^{\frac{p-1}{4}} \pmod{p} \qquad \text{and} \qquad 0 < i < p.$$

最后，令 $\varepsilon = \varepsilon(p)$ 为 $\{0, 1\}$ 中满足 [9] 的量

$$(\tfrac{p-1}{2})! \equiv (-1)^{\varepsilon} i \pmod{p}. \tag{16.1}$$

在开始计算之前，我们将不同τ量的模 2 同余列在一张表中。这里我们使用记号

$$[p]_4 := \frac{p-1}{4}.$$

例如，我们从表中读到：在上述假设下，若有$h \equiv g^{4\eta+3}$ （模 p）对某个 η 成立，则 $\tau_{\mathbf{es}}$（h, K）$\equiv 1 + \varepsilon$ （模 2）。

		$\tau_*(h, K)$（模 2）			
		er	**es**	**or**	**os**
$h \equiv g^{4\eta+*}\ (p)$	0	0	0	$[p]_4$	$[p]_4$
	1	$1+\varepsilon$	ε	$1+\varepsilon+[p]_4$	$\varepsilon+[p]_4$
	2	1	1	$1+[p]_4$	$1+[p]_4$
	3	ε	$1+\varepsilon$	$\varepsilon+[p]_4$	$1+\varepsilon+[p]_4$

表 1. 不同 τ 量的模 2 同余式。

我们现在验证 $\varepsilon = \varepsilon(p)$ 在方程（16.1）中确实是良定义的。固定$p \equiv 1$ （模 4）并定义 g 与 i 如上，威尔逊定理蕴含

$$\Big(\prod_{\substack{\mu=1\\ \mu \text{ even}}}^{p-1} \mu\Big)^2 = \Big(\prod_{\substack{\mu=1\\ \mu \text{ even}}}^{p-1} \mu\Big)\Big(\prod_{\substack{\mu=1\\ \mu \text{ odd}}}^{p-1} (p-\mu)\Big) \equiv (-1)^{\frac{p-1}{2}} \Big(\prod_{\mu=1}^{p-1} \mu\Big) \equiv -1 \pmod{p},$$

由此

$$\prod_{\substack{\mu=1\\ \mu \text{ even}}}^{p-1} \mu \equiv \pm i \pmod{p}.$$

[9] 这一点 ε 由式（16.2）证明。当然， g 的选择会影响 i 和 ε的值。

另一方面，

$$\prod_{\substack{\mu=1\\ \mu \text{ even}}}^{p-1} \mu = 2^{\frac{p-1}{2}}(\tfrac{p-1}{2})!,$$

并且由于 $2^{(p-1)/2} \equiv \pm 1$ （模 p），可得

$$(\tfrac{p-1}{2})! \equiv \pm i \pmod p. \tag{16.2}$$

因此， ε （16.1）中的值由（16.2）中的符号确定。注意到

$$\varepsilon = 0 \qquad \text{when} \qquad p = 17.$$

现在我们验证表1中所述的各种模 2 同余。为简洁起见，形式为 $\prod_{\mathbf{r}\ (k)} r$ 和 $\prod_{\mathbf{er}\ (k)} r$ 的乘积，分别理解为 r 遍历$\mathbf{r}(k)$和$\mathbf{er}(k)$。

引理 16.1。 固定 $p \equiv 1$ （模 4），令 $K = kp$ 为奇数，令 （h, K） $= 1$，并假设h 是一个二次剩余（模 p）。那么

$$\tau_{\mathbf{er}}(h, K) \equiv \begin{cases} 0 \pmod 2 & \textit{if } h \textit{ is a quartic} \pmod p, \\ 1 \pmod 2 & \textit{if } h \textit{ is a quadratic-nonquartic} \pmod p. \end{cases} \tag{16.3}$$

此外，有

$$\tau_{\mathbf{es}}(h, K) \equiv \tau_{\mathbf{er}}(h, K) \pmod 2. \tag{16.4}$$

证明。 我们从 $\mathbf{er}(K)$ 开始，也就是满足以下条件的 $0 < r < K$ 集合

$$(r, p) = 1, \quad r \text{ is even}, \quad \text{and} \quad r \text{ is a quadratic} \pmod p,$$

注意到 $|\mathbf{er}(K)| = {}^{k}{}_{(p-1)\ 4}$。将这些 r 乘以 h，再模 K 化简，得到的量 $0 < \{hr\}_K < K$ 仍与 p 互素，并且仍是模 p 的二次剩余。将所有这样的 奇数 $\{hr\}_K$ 替换为 $K - \{hr\}_K$，显然可得

$$h^{\frac{k(p-1)}{4}}\Big(\prod_{\mathbf{er}(K)} r\Big) \equiv \Big(\prod_{\mathbf{er}(K)} \{hr\}_K\Big) \equiv (-1)^{\tau_{\mathbf{er}}(h,K)}\Big(\prod_{\mathbf{er}(K)} r\Big) \pmod K.$$

根据假设， $h^{(p-1)/2} \equiv 1$ （模 p），由此推得

$$(-1)^{\tau_{\mathbf{er}}(h,K)} \equiv h^{\frac{p-1}{4}}\big(h^{\frac{p-1}{2}}\big)^{\frac{k-1}{2}} \equiv h^{\frac{p-1}{4}} \pmod p,$$

且（16.3）立即成立。只需将上述论证中的 $\mathbf{es}(K)$ 替换为 $\mathbf{er}(K)$，并作相应调整，便可很快看出 $\tau_{\mathbf{es}}(h, K)$ 与 $\tau_{\mathbf{er}}(h, K)$ 模 2下具有相同的同余式，这就证明了（16.4）。 ■

现在考虑当 h 是模 p 的非二次剩余时， $\tau_{\mathbf{er}}(h, K)$（模 2）的情形。

引理 16.2. 固定 $p \equiv 1$ （模 4），令 $K = kp$ 为奇数，并沿用g、 i和 ε的定义。若 （h、K） $= 1$ 且 h 是非二次剩余 （模 p），则

$$\tau_{\mathbf{er}}(h, K) \equiv \begin{cases} 1 + \varepsilon \pmod 2 & \textit{if } \bar{g}h \textit{ is a quartic} \pmod p, \\ \varepsilon \pmod 2 & \textit{if } \bar{g}h \textit{ is a quadratic-nonquartic} \pmod p. \end{cases}$$

证明。 由于 h 是非二次剩余（模 p），我们有

$$h^{\frac{k(p-1)}{4}}\Big(\prod_{\mathbf{er}(K)} r\Big) \equiv \Big(\prod_{\mathbf{er}(K)} \{hr\}_K\Big) \equiv (-1)^{\tau_{\mathbf{er}}(h,K)}\Big(\prod_{\mathbf{es}(K)} s\Big) \pmod K.$$

将等式两边乘以 $\prod_{\mathbf{er}(K)} r$，得到

$$h^{\frac{p-1}{4}}\big(h^{\frac{p-1}{2}}\big)^{\frac{k-1}{2}}\Big(\prod_{\mathbf{er}(K)} r\Big)^2 \equiv (-1)^{\tau_{\mathbf{er}}(h,K)}\Big(\prod_{\mathbf{e}(K)} e\Big) \pmod K, \tag{16.5}$$

并考察该关系模 p 的化简。首先，由于

$$\mathbf{er}(K) = \mathbf{er}(p) \cup \left(\bigcup_{j=1}^{(k-1)/2} \big(2jp + \mathbf{er}(p)\big)\right) \cup \left(\bigcup_{j=1}^{(k-1)/2} \big((2j-1)p + \mathbf{or}(p)\big)\right),$$

我们有

$$\Big(\prod_{\mathbf{er}(K)} r\Big)^2 \equiv \Big(\prod_{\mathbf{er}(p)} r\Big)^2\Big(\prod_{\mathbf{r}(p)} r\Big)^{k-1} \equiv (-1)^{\frac{p-1}{4}}\Big(\prod_{\mathbf{r}(p)} r\Big)\cdot 1 \equiv (-1)^{1+\frac{p-1}{4}} \pmod p. \tag{16.6}$$

然后，类似于我们对$\mathbf{er}(K)$ 的处理，将$\mathbf{e}(K)$ 展开，我们有

$$\prod_{\mathbf{e}(K)} e \equiv \Big(\prod_{\mathbf{e}(p)} e\Big)\Big(\prod_{\mathbf{e}(p)} e \prod_{\mathbf{o}(p)} o\Big)^{\frac{k-1}{2}} \equiv (-1)^{\frac{k-1}{2}}\Big(\prod_{\mathbf{e}(p)} e\Big) \equiv (-1)^{\frac{k-1}{2}} 2^{\frac{p-1}{2}} (\tfrac{p-1}{2})! \pmod p,$$

并且，利用（16.1），我们可推出

$$\prod_{\mathbf{e}(K)} e \equiv (-1)^{\frac{k-1}{2}+\frac{p-1}{4}+\varepsilon}\cdot i \pmod p. \tag{16.7}$$

回到（16.5）并对 p 取模，我们注意到 $h^{(p-1)/2} \equiv -1$ （模 p），并应用（16.6）和（16.7），得出

$$h^{\frac{p-1}{4}}(-1)^{\frac{k-1}{2}}(-1)^{1+\frac{p-1}{4}} \equiv (-1)^{\tau_{\mathbf{er}}(h,K)}(-1)^{\frac{k-1}{2}+\frac{p-1}{4}+\varepsilon}\cdot i \pmod p,$$

$$(-1)^{1+\varepsilon}(\bar{g}h)^{\frac{p-1}{4}} \equiv (-1)^{\tau_{\mathbf{er}}(h,K)} \pmod p,$$

由此即可得到结论。 ■

引理 16.1 和16.2，我们得到了表格中的以下条目 1.

		$\tau_*(h,\ K)$（模 2）			
		er	**es 或 os**		
$h \equiv g^{4\eta+*}(p)$	0	0	0		
	1	$1+\varepsilon$			
	2	1	1		
	3	ε			

引理16.3处理es列中的其余两项，而引理 16.4表明，or列和os列分别由er列和es列确定。

引理 16.3。固定 $p \equiv 1$ （模 4），令 $K = kp$ 为奇数，并令 $(h, K) = 1$。若 h 是一个非二次剩余 （模 p），则

$$\tau_{\mathbf{er}}(h, K) + \tau_{\mathbf{es}}(h, K) \equiv 1 \pmod 2.$$

证明。 首先，我们得到

$$h^{\frac{k(p-1)}{2}} \Big(\prod_{\mathbf{er}(K)} r \Big) \equiv h^{\frac{k(p-1)}{4}} (-1)^{\tau_{\mathbf{er}}(h,K)} \Big(\prod_{\mathbf{es}(K)} s \Big) \equiv (-1)^{\tau_{\mathbf{er}}(h,K)+\tau_{\mathbf{es}}(h,K)} \Big(\prod_{\mathbf{er}(K)} r \Big) \pmod K,$$

从而

$$h^{\frac{k(p-1)}{2}} \equiv (-1)^{\tau_{\mathbf{er}}(h,K)+\tau_{\mathbf{es}}(h,K)} \pmod K.$$

根据假设， $h^{(p-1)/2} \equiv -1$ （模 p），因此可得

$$(-1)^{\tau_{\mathbf{er}}(h,K)+\tau_{\mathbf{es}}(h,K)} \equiv (-1)^k \equiv -1 \pmod p,$$

这立即给出结论。 ■

引理 16.4。 固定 $p \equiv 1$ （模 4），令 $K = kp$ 为奇数，并令 $(h、 K) = 1$。则有

$$\tau_{\mathbf{os}}(h, K) \equiv \frac{p-1}{4} + \tau_{\mathbf{es}}(h, K) \pmod 2, \tag{16.8a}$$

and

$$\tau_{\mathbf{or}}(h, K) \equiv \frac{p-1}{4} + \tau_{\mathbf{er}}(h, K) \pmod 2. \tag{16.8b}$$

证明。 回顾方程（13.8），其指出

$$\sum_{\substack{\mu \,(K) \\ (\mu, 2p)=1}} \Big(\frac{\chi_\mu - 1}{2} \Big) \Big[\frac{h\mu}{K} \Big] \equiv \frac{(h-1)(p-1)}{4} + \sum_{\substack{\mu \,(K) \\ (\mu, 2p)=2}} \Big(\frac{\chi_\mu - 1}{2} \Big) \Big[\frac{h\mu}{K} \Big] \pmod 2, \tag{16.9}$$

其中 $[x]$ 表示 x的整数部分。再次令 $[x] = x - \{x\}$，并注意到对于奇数 μ，我们有

$$K[h\mu/K] \equiv h\mu + K\{h\mu/K\} \equiv h + \{h\mu\}_K \pmod 2,$$

在（16.9）的左边，我们有

$$\sum_{\substack{\mu \,(K) \\ (\mu, 2p)=1}} \Big(\frac{\chi_\mu - 1}{2} \Big) \Big[\frac{h\mu}{K} \Big] \equiv h \sum_{\substack{\mu \,(K) \\ (\mu, 2p)=1}} \Big(\frac{\chi_\mu - 1}{2} \Big) + \tau_{\mathbf{os}}(h, K)$$

$$\equiv h|\mathbf{os}(K)| + \tau_{\mathbf{os}}(h, K) \equiv \frac{hk(p-1)}{4} + \tau_{\mathbf{os}}(h, K) \pmod 2.$$

在（16.9）的右边，我们有

$$\frac{(h-1)(p-1)}{4} + \sum_{\substack{\mu \,(K) \\ (\mu, 2p)=2}} \Big(\frac{\chi_\mu - 1}{2} \Big) \Big[\frac{h\mu}{K} \Big] \equiv \frac{(h-1)(p-1)}{4} + \tau_{\mathbf{es}}(h, K) \pmod 2,$$

由此可得

$$\tau_{\mathbf{os}}(h, K) \equiv (hk + h - 1)\frac{p-1}{4} + \tau_{\mathbf{es}}(h, K) \equiv \frac{p-1}{4} + \tau_{\mathbf{es}}(h, K) \pmod 2.$$

这就是（16.8a），同样的论证给出（16.8b）。 ■

参考文献

[1] G. E. Andrews，《分拆理论》，剑桥数学文库，剑桥大学出版社，剑桥，1998年。1976年原版的重印。[2] B. C. Berndt，论带特征的艾森斯坦级数与狄利克雷 L函数的值，《算术学报》28（1975/76），第3期，299–320。[3] B. C. Berndt，戴德金和及其推广的互反定理，《数学进展》23（1977），第3期，285–316。[4] B. C. Berndt与L. Schoenfeld，欧拉-麦克劳林公式与泊松求和公式的周期类似及其在数论中的应用，《算术学报》28（1975/76），第1期，23–68。[5] B. C. Berndt与L. Schoenfeld，对论文的勘误：“欧拉-麦克劳林公式与泊松求和公式的周期类似及其在数论中的应用”/《算术学报》28（1975/76），第1期，23–68；MR 52 #*5586f*,《算术学报》38（1980/81），第3期，323。[6] T.Daniels，与勒让德符号加权分拆相关的两个 q级数中的消失系数，《数论研究》10（2024），第4期，论文第81号，12页。[7] T. Daniels，勒让德符号分拆数，《数学分析与应用杂志》542（2025），第1期，论文第128717号，43页。[8] H. Davenport，《乘法数论》，第二版，数学研究生教材，第74卷，施普林格出版社，纽约-柏林，1980年。由Hugh L. Montgomery修订。[9] P. Hagis Jr.，关于素数模数 $p \geq 3$的分拆问题，《美国数学会汇刊》102（1962），30–62。[10] P. Hagis Jr.，论一类具有互异加数的分拆，《美国数学会汇刊》112（1964），401–415。[11] G. H. Hardy与S. Ramanujan，组合分析中的渐近公式，《伦敦数学会会刊》（2）17（1918），75–115。[12] D. H. Lehmer，论分拆函数的级数，《美国数学会汇刊》43（1938），第2期，271–295。[13] J. Lehner，与模数五相关的一个分拆函数，《杜克数学杂志》8（1941），631–655。[14] H. L. Montgomery、I. Niven与H. S. Zuckerman，《数论导引》，第五版，约翰·威立父子公司，纽约，1991年。[15] H. L. Montgomery与R. C. Vaughan，《乘法数论。I. 经典理论》，剑桥高级数学研究丛书，第97卷，剑桥大学出版社，剑桥，2007年。[16] I. Niven，论特定分拆函数，《美国数学杂志》62（1940），第1期，353–364。[17] H. Rademacher，一个算术求和公式，《数学与物理月刊》39（1932），第1期，221–228。[18] H. Rademacher，论分拆函数p(n)，《伦敦数学会会刊》（2）43（1937），第4期，241–254。[19] H. Rademacher与E. Grosswald，《戴德金和》，卡鲁斯数学专著，第16号，美国数学协会，华盛顿哥伦比亚特区，1972年。[20] H. Rademacher与A. Whiteman，戴德金和定理，《美国数学杂志》63（1941），377–407。[21] H. Salié，论整模形式傅里叶系数的估计，《数学杂志》36（1933），第1期，263–278。[22] G. N. Watson，《贝塞尔函数理论》，大学出版社，英国剑桥，1922年。

数学系，普渡大学，印第安纳州西拉法叶 47907电子邮件地址：
daniel84@purdue.edu