arXiv:2602.09135v1 [math.GR] 9 Feb 2026

模函数与魔群指数

JOHN F. R. DUNCAN 和 HOLLY SWISHER

Abstract. 我们提出一种基于模函数的方法，用以解释在阶为.....的有限单群怪兽群的阶的素数分解中出现的指数（针对大于 3 的素数）。

1. Introduction

令人信服的证据表明，一个新的有限单群——群论中的“友善巨人” [24], ，其阶为

$$\#\mathbb{M} = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71, \tag{1.1}$$

这一发现由 Fischer 和 Griess 于 1973年11 月独立作出（见 [24, § 15]）。Conway 将其称为 怪兽群 ，并有人推测（见 [10, § 1]和 [25]），它应当有一个维数为 $196883 = 47 \cdot 59 \cdot 71$ 的不可约表示。基于此，Fischer、Livingstone 和 Thorne 计算出了怪兽群的完整特征标表（见 [9] ，另见 [24, § 15]）。

随后，在1978年11月（参见 [32, 序言]），McKay注意到 $196884 = 1 + 196883$ 是 j函数的 q 展开中 q 的系数，并向Thompson提出这或许意义重大。在进一步发现了更多类似的巧合 [37] *之后，Thompson提出（参见 [36]和 [10, § 1]），应当存在一个无限维分次 $\mathbb{M}$模 $V = \bigoplus_{n\geq -1} V_n$ 来解释这些现象。*McKay–Thompson*级数

$$T_g(\tau) := \sum_{n\geq -1} \mathrm{tr}(g|V_n) q^n \tag{1.2}$$

Conway和Norton的怪兽月光 猜想 [10]完全规定了猜想中的怪兽模 V 的（此处 $q = e^{2\pi i \tau}$ 对应 $\tau \in \mathbb{H}$） T_g 。最引人注目的是，他们预言每个 T_g 都应是某个特定群 $\Gamma_g \subseteq \mathrm{SL}_2(\mathbb{R})$的正规化Hauptmodul，且该群为零亏格。

到了1980年1月（参见 [23] 和 [24, § 1]），Griess通过将 $\mathbb{M}$构造为一个196884维（交换但非结合）代数的自同构，确立了它的存在。到了1983年11月，Frenkel、Lepowsky和Meurman宣布了 [20] （另见[19, 21]），构造出一个分次 $\mathbb{M}$模 $V^\natural = \bigoplus_{n\geq -1} V^\natural_n$，使得

$$T^\natural_g(\tau) := \sum_{n\geq -1} \mathrm{tr}(g|V^\natural_n) q^n \tag{1.3}$$

与 (1.2) 中的 $T_g(\tau)$ 对各种 g 相吻合，特别是对 $g = e$ 恒等元。随后，在1992年，Borcherds [2] 巧妙地证明了 $T^\natural_g = T_g$对所有 $g \in \mathbb{M}$ 成立，从而解决了魔群月光猜想。

近年来，月光的研究已扩展到其他有限单群以及其他类型的模对象，包括雅可比形式 [5, 18], 斜全纯雅可比形式

MSC2020: 11F03，20C34，20D08。

*McKay 在其 CRM-Fields奖讲座（见 [29]）中提到，是 Bernd Fischer 的女儿（作者不知其名）最先研究将 j 的系数与怪兽群联系起来，而不只是 q 的系数。

[13, 26], 西格尔模形式 [4, 38], 和模拟模形式 [6, 12, 22]。此外，有限群的分次表示与算术几何不变量之间的联系也已出现[1, 7, 8, 15, 14, 27]。

然而，我们希望重新审视一种更早出现的几何观点；在提出任何与 j 系数相关的联系之前，这种观点就已存在：1975年1月，Ogg 注意到，整除 $\#\mathbb{M}$ 的素数p，恰好也是那些使特征-p 的超奇异 j 不变量全部定义在 $\mathbb{F}_p$ 上，而不只是定义在 $\mathbb{F}_{p^2}$ 上的素数。这为出现在 (1.1) 中的素数提供了几何刻画。受这一观点或许还能带来更多发现的可能性所启发，我们在本文中探讨以下问题。

问题。能否　　刻画出哪些素数整除 $\#\mathbb{M}$，并且确定它们的重数?　　?

对于大于 3 的素数，我们给出这一问题的两种答案。两种答案都受到 Deligne 关于 j 函数的 p-进刚性定理的启发（见 [17, 28]）。一种答案以素数幂水平的模函数来表述，另一种则完全以超奇异椭圆曲线来表述（或者完全以 j 来表述，见注释 1.4）。我们的方法并不完全适用于 $p = 2, 3$ 的情形。这些例外素数留待今后研究。

为陈述我们的结果，若 $\Gamma_0(N)$为零亏格，则定义 J_N 为 $\Gamma_0(N)$的正规化Hauptmodul，否则令 $J_N := 0$。对 $\Gamma_0(N)^+$类似地定义 J_{N+}。进一步，定义 $\mathfrak{S}_p$ 为特征 p中超奇异椭圆曲线的 j-不变量之集，并记

$$\mathfrak{S}_p = \mathfrak{S}_p^1 \sqcup \mathfrak{S}_p^2 \tag{1.4}$$

表示将 $\mathfrak{S}_p$ 分解为位于 $\mathbb{F}_p$中的那些 j-不变量（$\mathfrak{S}_p^1$），以及位于 $\mathbb{F}_{p^2}$ 中但不在 $\mathbb{F}_p$中的那些（$\mathfrak{S}_p^2$）。又定义 m_p 为特征 p中一条超奇异椭圆曲线的自同构群的最小阶，

$$m_p := \min\{\#\operatorname{Aut}(E) \mid E/K \text{ supersingular, } \operatorname{char}(K) = p\}. \tag{1.5}$$

关于$\#\mathfrak{S}_p^2 = 0$情形下 m_p 的值，见(4.2)。当 $\mathfrak{S}_p^2$ 非空时，我们有 $m_p = 2$。

记 $v_p(x)$为 x的 p-进赋值。对于具有整系数的 q-级数 f，$v_p(f)$表示 f的系数的最小 p-进赋值。我们证明 $v_p(\#\mathbb{M})$的如下两个刻画，其中 $p > 3$。

定理1.1。设 p 是一个大于3的素数。那么我们有

$$v_p(\#\mathbb{M}) = v_p(J_1 - J_{p+}) + v_p(J_1 - J_p) + v_p(J_1 - J_{p^2}). \tag{1.6}$$

定理 1.2。设 p 是一个大于3的素数。那么我们有

$$v_p(\#\mathbb{M}) = \begin{cases} \frac{3}{2}m_p & \text{if } \#\mathfrak{S}_p^1 = 1 \text{ and } \#\mathfrak{S}_p^2 = 0, \\ \frac{1}{2}m_p & \text{if } \#\mathfrak{S}_p^1 > 1 \text{ and } \#\mathfrak{S}_p^2 = 0, \\ 0 & \text{if } \#\mathfrak{S}_p^2 > 0. \end{cases} \tag{1.7}$$

注 1.3。我们在§ 4中计算所有 p对应的(1.6)右端，因此可以详细说明 $p = 2,3$时(1.6-1.7)中的差异：对于 $p = 2$，(1.6-1.7)的右端均为36，而$v_2(\#\mathbb{M}) = 46$；对于 $p = 3$，(1.6-1.7)的右端均为18，而$v_3(\#\mathbb{M}) = 20$。特别地，对于所有 p，(1.6-1.7)的右端都相等。

注 1.4。我们也可以完全用 j-函数来表述定理 1.2，因为事实证明，对于所有 p 素数，$m_p = v_p($ $j|V_p - \Phi_p(j))$，其中 Φ_p 是第 p个法贝尔多项式。

注记 1.5。Ogg [30] 证明了，当且仅当 $\mathfrak{S}_p^2$ 为空时，$\Gamma_0(p)^+$ 才是零亏格。由此可得（见命题 4.1 和定理 1.2 的证明），对于这样的 p，我们有

$$v_p(J_1 - J_{p+}) = \frac{1}{2}m_p = \left\lceil \frac{12}{p-1} \right\rceil. \tag{1.8}$$

类似地， $\Gamma_0(p)$恰在 $\mathfrak{S}_p$ 为单元素集时具有零亏格，而这又恰在$p-1$ 整除 12 时成立。对于这样的 p ，我们证明（见命题 4.1）：

$$v_p(J_1 - J_p) = \frac{12}{p-1} + \left\lceil \frac{12}{p+1} \right\rceil . \tag{1.9}$$

我们也可以类似地处理 (1.6) 中的最后一项：群 $\Gamma_0(p^2)$ 仅当 p^2-1 整除 24 时才具有零亏格，而对于这些素数（见命题 4.2），我们有

$$v_p(J_1 - J_{p^2}) = \frac{24}{p^2-1}. \tag{1.10}$$

其余内容安排如下。我们在第 2 节证明关于模函数和 Hauptmodul 的引理，为后续分析奠定基础。在第 3 节，我们利用 Deligne 的一项结果确定 $J_1|U_p$ 的 p 可整除性。在第 4 节，我们证明定理 1.1 和 1.2。我们在此承认，我们提出的许多论证都可以用穷举计算代替。我们更倾向于采用一种更自然且自成一体的方法，部分原因是这能免去读者繁重的计算工作，同时也因为我们致力于这一宏大挑战：解释怪兽群如何从更自然的数学对象中产生。我们或许还不知道哪些论证能够实现这一目标，但可以预期，更一般的论证会让我们更接近目标。

Acknowledgement

J.D. 谨此感谢中央研究院（AS-IA-113-M03）和台湾国家科学及技术委员会（112-2115-M-001-006-MY3）提供的资助。H.S. 获得了美国国家科学基金会资助，项目编号 DMS-2101906。

2. Preparations

2.1. 群与函数。 我们首先回顾，模群 $\Gamma_0(1) := SL_2(\mathbb{Z})$ 由 $W_1 := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ 和 $T := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ 生成。接着，对于 N 个正整数，我们定义 $V_N := \frac{1}{\sqrt{N}} \left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)$，并定义 ***Fricke*** 对合

$$W_N := W_1 V_N = V_N^{-1} W_1 = \frac{1}{\sqrt{N}} \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right). \tag{2.1}$$

N 次 ***Hecke*** 同余子群 为 $\Gamma_0(N) := \Gamma_0(1) \cap V_N^{-1}\Gamma_0(1)V_N$。我们还使用 $\Gamma_0(N)^+ := \langle \Gamma_0(N),\ W_N \rangle = \Gamma_0(N) \cup \Gamma_0(N)W_N$。

对于 $\Gamma = \Gamma_0(N)$ 或 $\Gamma = \Gamma_0(N)^+$， Γ 的尖点 是 Γ 在 $\mathbb{Q} \cup \{\infty\}$ 上的轨道。每个尖点由一个有理数 $\frac{a}{b}$ 表示，其中 $\gcd(a, b) = 1$ 且 $b|N$。此外，当且仅当 $b = b'$ 和 $a \equiv a'$ 模 $\gcd(b, \frac{N}{b})$ 时，$\frac{a}{b}$ 和 $\frac{a'}{b'}$ 定义 $\Gamma_0(N)$ 的同一个尖点（例如参见 [11, 命题 2.2.3]）。W_N 的作用会将由 $\frac{a}{b}$ 和 $\frac{-ab}{N}$ 表示的尖点合并。无穷尖点 由 ∞ 以及 $\frac{1}{N}$ 表示。

给定 p 素数且 b 与 p 互素，选取 b' 使得 $bb' \equiv 1$ 模 p，并令

$$X_p^b = V_p^{-1} T^b W_1 T^{b'} V_p. \tag{2.2}$$

于是 $\Gamma_0(p^2)X_p^b$ 与 b 的选取无关，且 b' 模 p，我们有如下

引理 2.1. 对于 p 素数且与 p互素的 b， $\Gamma_0(p^2)$ 的无穷尖点经 X_p^b 映射到 $\frac{b}{p}$，而 $0 < b < p$ 的 $\Gamma_0(p^2)X_p^b$ 是 $\Gamma_0(p^2)$ 在 $\Gamma_0(p)$ 中的非平凡右陪集。

令 $\mathbb{H}$ 表示复上半平面。对于 $\Gamma = \Gamma_0(N)$ 或 $\Gamma = \Gamma_0(N)^+$，Γ的尖点自然地将轨道空间 $\Gamma\backslash\mathbb{H}$上的黎曼曲面结构紧化（例如参见 [33, § 1.3]）。Γ 的亏格 即为此曲面的亏格。例如，利用 [33,命题 1.40, 1.43], 可以证明

$$\text{genus}(\Gamma_0(p^v)) = \begin{cases} 0 & \text{if } v \le 2 \text{ and } p \in \{2,3\}, \\ \frac{p-a}{12} & \text{if } v = 1 \text{ and } p \equiv a \bmod 12 \text{ for } a \in \{-1,5,7,13\}, \\ \frac{p-a}{12} + \frac{(p-5)(p-1)}{12} & \text{if } v = 2 \text{ and } p \equiv a \bmod 12 \text{ for } a \in \{-1,5,7,13\}. \end{cases} \tag{2.3}$$

本文中，模函数 是定义在 $\mathbb{H}$ 上的全纯函数，且对某个 $M > 0$ 而言具有 $\Gamma_0(M)$-不变性。给定一个模函数 f，令 $c_n(f)$ 表示 f 的 q-展开中 q^n 的系数，使得 $f(\tau) = \sum_n c_n(f) q^n$。这里，对于 $\tau \in \mathbb{H}$，$q = e(\tau)$，其中 $e(x) := e^{2\pi i x}$。算子 U_N 定义为

$$f|U_N = \frac{1}{N} \sum_{b=0}^{N-1} f|V_N^{-1} T^b, \tag{2.4}$$

并且满足 $c_n(f|U_N) = c_{nN}(f)$。

戴德金 η 函数 为 $\eta(\tau) := q^{\frac{1}{24}} \prod_{n>0}(1-q^n)$。固定一个整数 $N > 1$，令 $d = d_N$ 为满足以下两个条件的最小正整数： $d(N-1) \equiv 0$ 模 24，且 N^d 是一个平方数。于是

$$t_N(\tau) := \frac{\eta(\tau)^d}{\eta(N\tau)^d} \tag{2.5}$$

是 $\Gamma_0(N)$ 的模函数（参见例如 [31, 定理 1.64]），且 t_N 的 q-展开具有如下形式

$$t_N(\tau) = q^{-n} \left(1 - dq + \frac{d(d-3)}{2} q^2 + dq^N + \mathcal{O}(q^3)\right), \tag{2.6}$$

其中 $d = d_N$ 和 $n = n_N := \frac{d(N-1)}{24}$。

根据 (2.6)，函数 t_N 仅当满足 $N-1$ 整除 24 的 N时，才在 $\Gamma_0(N)$ 的无穷尖点处有一个简单极点，即

$$N \in \{2,3,4,5,7,9,13,25\}. \tag{2.7}$$

关于 t_N 在非无穷尖点附近的行为，我们有如下结论。

引理 2.2. 对于 $N > 1$，函数 t_N 在 $\Gamma_0(N)$ 的无穷尖点之外有界，当且仅当 N 是素数或素数的平方。

证明。令 b 为 N 的一个因子，并令 a 为一个与 b互素的整数。利用 [31, 定理 1.65]，我们得到 t_N 在由 $\frac{a}{b}$ 表示的尖点处的 q展开的消失阶为

$$\frac{d_N}{24 \gcd(b, \frac{N}{b})} \left(\frac{N}{b} - b\right). \tag{2.8}$$

特别地， t_N 在由 $\frac{a}{b}$ 表示的尖点附近有界，当且仅当 $b \le \frac{N}{b}$。结论由以下观察立即得出：对于 N 的每个真因子 b， $b^2 \le N$ 当且仅当 N 是素数或素数的平方。□

由 (2.6) 和引理 2.2 可知， $n_N = 1$，且 t_N 是 $\Gamma_0(N)$ 的主模函数；特别地，当 $N-1$ 整除 24 时， $\Gamma_0(N)$ 的亏格为零。利用 (2.3)，我们得到如下结果。

引理 2.3。 对于 p 素数，若 $N = p$ 或 $N = p^2$，则 Γ_0（N）是零亏格，当且仅当 $N-1$整除24。

$\Gamma_0(1)$的正规化Hauptmodul为

$$J_1(\tau) = j(\tau) - 744 = q^{-1} + 196884q + \mathcal{O}(q^2), \tag{2.9}$$

而对于满足 $N-1$ 整除 24 的 N， $\Gamma_0(N)$ 的正规化Hauptmodul为

$$J_N = t_N - c_0(t_N) = t_N + d_N, \tag{2.10}$$

其中 $d_N = \frac{24}{N-1}$。由 (2.6) 和 (2.9-2.10) 可推得

$$c_1(J_1 - J_N) = \begin{cases} 196884 - \frac{d(d-1)}{2} & \text{for } N = 2, \\ 196884 - \frac{d(d-3)}{2} & \text{for } N = 3, 4, 5, 7, 9, 13, 25, \end{cases} \tag{2.11}$$

其中 $d = d_N$。为便于日后查阅，我们将满足 $n_N = 1$ 的 $N > 1$ 对应的 d_N，以及相应 $c_1(J_1 - J_N)$ 的素数分解列于表 1。

TABLE 1. $N > 1$ 满足 $n_N = 1$ 时的 d_N 和 $c_1(J_1 - J_N)$。

N	2	3	5	7	13
d_N	24	12	6	4	2
$c_1(J_1 - J_N)$	$2^{16} \cdot 3$	$2 \cdot 3^9 \cdot 5$	$3^2 \cdot 5^5 \cdot 7$	$2 \cdot 7^4 \cdot 41$	$5 \cdot 13^2 \cdot 233$

N	2^2	3^2	5^2
d_N	8	3	1
$c_1(J_1 - J_N)$	$2^8 \cdot 769$	$2^2 \cdot 3^3 \cdot 1823$	$5 \cdot 13^2 \cdot 233$

由 (2.1)、(2.6) 以及公式 $\eta(W_1\tau) = \sqrt{-i\tau}\eta(\tau)$ 可得

$$s_N(\tau) := (t_N|W_N)(\tau) = N^{\frac{d}{2}} t_N(\tau)^{-1} = N^{\frac{d}{2}} q^n + \mathcal{O}(q^{n+1}), \tag{2.12}$$

其中 $d = d_N$ 且 $n = n_N$。因此， $t_{N+} := t_N + s_N$ 是 $\Gamma_0(N)^+$ 的模函数，在无穷尖点处有一个 n_N 阶极点。特别地，

$$J_{N+} = t_N - c_0(t_N) + N^{\frac{d}{2}} t_N^{-1} = J_N + N^{\frac{d}{2}} t_N^{-1} \tag{2.13}$$

是 $\Gamma_0(N)^+$ 的正规化Hauptmodul，其中 $d = d_N$（参见 (2.10)）。

2.2. **降级**。本节中我们定义并应用一些降级算子。我们的第一个结果展示了 U_N (2.4) 的降级性质。

引理 2.4。对于 N 为正整数，若 f 是 $\Gamma_0(N^2)$ 的模形式，则 $f|U_N$ 是 $\Gamma_0(N)$ 的模形式 .

证明。首先注意，若 $A = \left(\begin{smallmatrix} a & b \\ * & * \end{smallmatrix}\right) \in \Gamma_0(N)$，则 $T^{-ab}A \in \Gamma_0(N, N) := V_N\Gamma_0(N^2)V_N^{-1}$。因此，由于 $f|U_N$ 是 T-不变的，只需证明 $f|U_N$ 是 $\Gamma_0(N, N)$-不变的。接下来注意，对于 $A = \left(\begin{smallmatrix} * & * \\ * & d \end{smallmatrix}\right) \in \Gamma_0(N, N)$ 以及任意的 b，有 $B_b := V_N^{-1}T^bAT^{-bd^2}V_N \in \Gamma_0(N^2)$。利用这一点，我们计算得

$$Nf|U_NA = \sum_{b \bmod N} f|V_N^{-1}T^bA = \sum_{b \bmod N} f|B_bV_N^{-1}T^{bd^2} = \sum_{b \bmod N} f|V_N^{-1}T^b, \tag{2.14}$$

其中，(2.14) 中最后一个等式成立，是因为 $B_b \in \Gamma_0(N^2)$ 且 $d \equiv 1$ 模 N。由 (2.4) 可得 $f|U_NA = f|U_N$。□

注记 2.5。类似于 (2.14) 的计算表明，若 $f \in \Gamma_0(MN^2)$，则 $f|U_N \in \Gamma_0(MN)$，对于任意正整数 M 和 N。

回顾 X_p^b 由 (2.2) 得。对于 p 素数以及 f 一个关于 $\Gamma_0(p^2)$ 的模函数，我们现在定义 e

$$f|X_p := f + \sum_{0<b<p} f|X_p^b. \tag{2.15}$$

于是引理 2.1 表明 $f|X_p$ 是良定义的，并且还证明了以下结论。

Lemma 2.6. 对于素数 p，若 f 是 $\Gamma_0(p^2)$ 的模形式，则 $f|X_p$ 是 $\Gamma_0(p$的模形式).

接下来我们同时使用 U_p 和 W_p，将水平从 $\Gamma_0(p)$降到 $\Gamma_0(1)$。

引理 2.7. 若 f是 $\Gamma_0(p)$ 的模形式，则 $pf|U_p + f|W_p$是 $\Gamma_0(1)$的模形式。

证明. 令 $h := pf|U_p + f|W_p$。于是 h是 T不变的，因为 W_p正规化 $\Gamma_0(p)$。为证明h是 W_1不变的，我们记 $h = h_1 + h_2$，其中 $h_1 = \sum_{0<b<p} f|V_p^{-1}T^b$且 $h_2 = f|V_p^{-1} + f|W_p$。

现在， h_2 是 W_1不变的，因为 $W_p = V_p^{-1}W_1$ （参见（2.1））。对于 h_1，我们有

$$h_1|W_1 = \sum_{0<b<p} f|V_p^{-1}T^bW_1 = \sum_{0<b<p} f|X_p^bV_p^{-1}T^{-b'} = \sum_{0<b<p} f|V_p^{-1}T^{-b'} \tag{2.16}$$

（参见（2.2））。我们得出 $h_1|W_1 = h_1$，因为赋值 $b \mapsto -b'$ 在 $\mathbb{Z}$模 p的非零元素上定义了一个双射。□

注 2.8. 与（2.16）类似的计算表明，若 M 是一个与 p互素的正整数，且 $f \in \Gamma_0(Mp)$，并且 W_p 取为 $\Gamma_0(Mp)$的一个恰当选取的阿特金–莱纳对合，则$pf|U_p + f|W_p$属于 $\Gamma_0(M)$。

下一个结果本质上是 [16, 引理 2.1]。也可见于 [10, 第 318] 页

引理 2.9. 对于满足 $\Gamma_0(p)^+$ 亏格为零的 p 素数， $J_1 - J_{p+} = pJ_{p+}|U_p$。

证明。 由引理 2.7 可知， $pJ_{p+}|U_p + J_{p+}|W_p$ 在 $\Gamma_0(1)$下不变，因此是J_1的多项式。由于 $J_{p+}|U_p = \mathcal{O}(q)$和 $J_{p+}|W_p = J_{p+} = q^{-1} + \mathcal{O}(q)$，我们有 $pJ_{p+}|U_p + J_{p+} = J_1$。□

引理 2.9 有如下推论。

引理 2.10。证 明 $k \geq 0$，以及 p素数，使得 $\Gamma_0(p)^+$亏格为零， $v_p(J_1|U_p^k) = v_p(J_{p+}|U_p^k)$

证明。 由引理 2.9，我们有 $J_1|U_p^k = J_{p+}|U_p^k + pJ_{p+}|U_p^{k+1}$。该断言成立，这是因为当 $v_p(a) < v_p(b)$ 时， $v_p(a+b) = v_p(a)$，并且对于任意模函数 f， $v_p(f) < v_p(pf|U_p)$。□

以下两个引理将用于约束 J_{p^2}。

引理 2.11. 对于使得 $\Gamma_0(p)$ 为零亏格的 p 素数，若 m 满足 $0 < mn_{p^2} < p$，则$pt_{p^2}^m|U_p$ 为常数。

证明. 令 $f := pt_{p^2}^m|U_p$。则根据引理 2.4， f 对 $\Gamma_0(p)$ 是模形式，并且根据关于 m 的条件在无穷尖点附近有界（见 (2.6)）。由引理 2.3， s_p （见 (2.12)）是 $\Gamma_0(p)$ 的主模函数。由于 s_p 在无穷尖点附近有界，故对某个多项式 $P(x)$ 有 $f = P(s_p)$。考虑 $f|W_p$。一方面 $f|W_p = P(s_p)|W_p = P(t_p)$，因此由于$n_p = 1$， $P(x)$ 的次数是 $f|W_p$ 的 q-展开中极点的阶。另一方面

$$f|W_p = t_{p^2}^m|V_p^{-1}W_p + \sum_{0<b<p} t_{p^2}^m|V_p^{-1}T^bW_p = s_{p^2}^m + \sum_{0<b<p} t_{p^2}^m|X_p^bV_p^{-1}T^{-b'}V_p \tag{2.17}$$

（参见 (2.2) 和 (2.4)，并比较 (2.16)）。现在， $t_{p^2}^m|X_p^b$ 对于 $0 < b < p$ 而言，是根据引理 2.1 在 $\Gamma_0(p^2)$ 的一个非无穷尖点处对 $t_{p^2}^m$ 的展开，因此根据引理 2.2， $t_{p^2}^m|X_p^b$ 在无穷尖点附近有界。由于 $q|V_p^{-1}T^{-b'}V_p$ 只是 q 乘以一个 p 次单位根，(2.17) 中没有任何一项在其 q 展开中有极点。因此， $P(x)$ 的次数为 0，且 f 是常数。□

引理 2.12。 对于 $p=2$ 和 $p=3$，我们有 $c_n(J_{p^2}) = 0$，除非 $n \equiv -1$模 p。

证明。 为简化记号，令 $c_n^* = c_n(J_{p^2})$。于是由 (2.10) 可得 $c_n^* = c_n(t_{p^2})$，其中 $n>0$。由于 $n_{p^2}=1$，我们可以在 $0<m<p$ 的条件下应用引理 2.11。取 $m=1$，得到 $c_n^*=0$，其中 $n \equiv 0$ 模 p。这就证明了 $p=2$ 的情形。对于 $p=3$，我们还需证明：对于满足$n \equiv 1$ 模 3 的 $n>0$，有 $c_n^*=0$。由于 $d_9=3$（见表 1），我们有 $J_9^2 = t_9^2+6t_9+9$。因此，在$m=1$和 $m=2$的条件下应用引理 2.11，得到 $c_{3n}(J_9^2) = 0$，其中 $n>0$。由此可得

$$2c_{3n+1}^* = -\sum_{k=0}^{n-1}\left(c_{3k+1}^* c_{3(n-k-1)+2}^* + c_{3k+2}^* c_{3(n-k-1)+1}^*\right) \tag{2.18}$$

对于 $n>0$。由 (2.6) 可得 $c_1^*=0$。现在利用 (2.18)，对 n 作归纳法，即可推出：对于满足 $n \equiv 1$ 模 3 的 $n>0$， c_n^* 消失。□

本节其余结果用于计算 $v_p(J_1-J_p)$（见命题 4.1）和 $v_p(J_1-J_{p^2})$（见命题 4.2）。我们注意到，只需利用模函数的前几个系数，就可以确定其 p 可除性的上界。如 §1 中所述，我们更倾向于采用一种能够凸显这些对象内在结构的方法，并着眼于构建更一般的理论。

命题 2.13。 对于使 $\Gamma_0(p)$ 具有零亏格的 p 素数， $v_p(J_1-J_p) = v_p(c_1(J_1-J_p))$。

证明。 根据定义，我们有 $v_p(J_1-J_p) \le v_p(c_1(J_1-J_p))$。对于反向不等式，首先注意到 J_1-J_p 在 $\Gamma_0(p)$ 的无穷尖点附近有界，因此，与引理 2.11 的证明一样，存在一个常数项为零的多项式 $P(x)$，使得 $J_1-J_p = P(s_p)$。记作

$$(J_1-J_p)|W_p = P(t_p) = q^{-p} - d_p + \mathcal{O}(q) \tag{2.19}$$

我们得到 $P(x)+d_p$ 是关于 t_p 的第 p 个 法贝尔多项式 （例如参见 [3, § 3]），由此得出 $P(x)$ 具有整系数。

现在写作 $P(x) = a_1x + P_*(x)x^2$，其中 $P_*(x) \in \mathbb{Z}[x]$。那么， $v_p(J_1-J_p) = v_p(P(s_p))$ 的下界是 $v_p(a_1s_p)$ 和 $v_p(P_*(s_p)s_p^2)$ 中的较小值。应用 (2.12)，我们得到 $v_p(c_1(J_1-J_p)) = v_p(c_1(a_1s_p)) = v_p(a_1s_p)$，并且还有 $v_p(P_*(s_p)s_p^2) \ge v_p(s_p^2) = d_p$。因此， $v_p(J_1-J_p)$ 的下界是 $v_p(c_1(J_1-J_p))$ 和 d_p 中的较小值。利用表 1，我们验证 $d_p \ge v_p(c_1(J_1-J_p))$。□

命题 2.14. 对于使 $\Gamma_0(p^2)$ 具有零亏格的 p 素数， $v_p(J_p - J_{p^2}) = d_{p^2}$。

证明。 根据引理 2.3，我们有 $p \in \{2,3,5\}$。对于 $p=5$，我们有 $d_{p^2}=1$；由（2.5）、（2.10）以及 $(1-x)^5 \equiv 1-x^5$ 模 5 这一事实，即可得出结论。对于 $p \in \{2,3\}$，我们考虑$h = t_{p^2}|X_p$ （见（2.15））；根据引理 2.6，它是 $\Gamma_0(p)$ 上的模形式。由引理 2.1 可知， h是 $q^{-1}+\mathcal{O}(1)$，并且是 $\Gamma_0(p)$ 的主模函数，因此 $h = J_p + c_0(h)$。接下来注意到

$$X_p^b = T^{\frac{b}{p}} W_{p^2} T^{\frac{b'}{p}} \tag{2.20}$$

（见（2.2）），其中 $T^x := \left(\begin{smallmatrix}1 & x\\ 0 & 1\end{smallmatrix}\right)$。在本证明余下部分中，令 $d = d_{p^2}$。由（2.10）和引理 2.12 可知

$$t_{p^2}|T^{\frac{b}{p}} = e(-\tfrac{b}{p})t_{p^2} + (e(-\tfrac{b}{p})-1)d. \tag{2.21}$$

此外， $b^2 \equiv 1$ 模 p 对 $p \in \{2,3\}$成立，因此我们可以假设在（2.20）中有 $b'=b$。于是我们得到

$$t_{p^2}|X_p^b = e(-\tfrac{b}{p})p^d t_{p^2}^{-1}|T^{\frac{b}{p}} + (e(-\tfrac{b}{p})-1)d. \tag{2.22}$$

在 $p=2$ 的情况下，我们由 (2.22) 推得

$$h = t_4 + t_4|X_2^1 = J_4 - 3d + 2^d\sum_{n>0}(-1)^{n+1}c_n(t_4^{-1})q^n. \tag{2.23}$$

利用 $h = J_2 + c_0(h)$，我们得到 $J_2 - J_4 = 2^d \sum_{n>0}(-1)^{n+1} c_n(t_4^{-1}) q^n$。特别地，该结论对 $p = 2$ 成立。

在 $p = 3$ 的情形下，由 (2.22) 可推得

$$h = t_9 + t_9|X_3^1 + t_9|X_3^2 = J_9 - 4d + 3^d \sum_{n>0} 2\Re(e(\tfrac{n-1}{3})) c_n(t_9^{-1}) q^n. \tag{2.24}$$

利用 $h = J_3 + c_0(h)$，现在得到 $J_3 - J_9 = 3^d \sum_{n>0} 2\Re(e(\frac{n-1}{3})) c_n(t_9^{-1}) q^n$，且该结论对$p = 3$成立。
□

3. Application of Deligne's Theorem

为方便起见，本节重新定义 $\mathfrak{S}_p \subset \mathbb{F}_{p^2}$ （参见 (1.4)），将其定义为特征 p 下的超奇异J_1-值集合。也就是说， $\mathfrak{S}_p$ 表示对于特征为 p 的超奇异椭圆曲线，作为 $J_1(E) = j(E) - 744$ 出现的那些值。假设 $\Gamma_0(p)^+$ 的亏格为零。由 [30]可知 $\mathfrak{S}_p \subset \mathbb{F}_p$，因此我们可以对每个 $\alpha \in \mathfrak{S}_p$ 选取一个整数 $\hat{\alpha}$，使得 $\hat{\alpha} \equiv \alpha$ 模 p。下述结果利用了 Deligne 的一个定理，具体描述见 Dwork [17] 和 Koike [28]。

命题 3.1。对于满足 $\Gamma_0(p)^+$ 具有零亏格的 p 素数，存在整数$\hat{\alpha} \equiv \alpha$ 模 p，对每个 $\alpha \in \mathfrak{S}_p$，使得

$$pJ_1|U_p = -\sum_{\alpha \in \mathfrak{S}_p} \sum_{n \geq 1} A_n(\hat{\alpha})(J_1 - \hat{\alpha})^{-n}, \tag{3.1}$$

其中 $A_n(\hat{\alpha})$ 是满足以下条件的整数:

$$v_p(A_n(\hat{\alpha})) \geq \begin{cases} \frac{3np+1}{p+1} & \text{if } \alpha \equiv -744 \bmod p, \\ \frac{2np+1}{p+1} & \text{if } \alpha \equiv 984 \bmod p, \\ \frac{np+1}{p+1} & \text{else.} \end{cases} \tag{3.2}$$

此外，若 $p > 3$，则对于 $n = 1$，*(3.2)* 中的界是最优的。

证明。令 Φ_p 表示 J_1的第 p 个法贝尔多项式，它是满足$\Phi_p(J_1) = q^{-p} + \mathcal{O}(q)$的唯一多项式（例如参见 [3, § 3]），并注意到 $\Phi_p(J_1) = j_p$，其中 j_p 如 [35]中所述。于是根据 [17, § 7] 的结果（另见 [28, (36-37)]）以及 [35, 定理 1.1], ，我们得到

$$J_1|V_p = \Phi_p(J_1) + \sum_{\alpha \in \mathfrak{S}_p} \sum_{n \geq 1} A_n(\hat{\alpha})(J_1 - \hat{\alpha})^{-n}, \tag{3.3}$$

其中 $A_n(\hat{\alpha})$ 如 (3.2) 中所述。（注意，对于 $p \in \{2, 3\}$，可以得到更强的界。参见 [17, 第 89] 页和[28, (38)]。此外，在 [17, § 7]中， $A_n(\hat{\alpha})$ 记作 $A_n^{(i)}$。）将引理 2.7 应用于 J_1，可得 $J_1|W_p + pJ_1|U_p = J_1|V_p + pJ_1|U_p$ 是 $\Gamma_0(1)$ 不变的，因此是 J_1的一个多项式。此函数也满足 $q^{-p} + \mathcal{O}(q)$，故有 $J_1|V_p + pJ_1|U_p = \Phi_p(J_1)$。这就证明了 (3.1-3.2)。

关于尖锐性结论， [17] 的定理 8.2 告诉我们，当 $p > 3$ 且$\alpha \not\equiv -744,984 \bmod p$ 时， $v_p(A_1(\hat{\alpha})) = 1$。正如 [17, § 7.e], 开头所述，通过注意到 $J_1 + 744$ 在 $J_1 = -744$ 附近的表现类似于 $(\lambda - \lambda_0)^3$，而 $J_1 - 984$ 在 $J_1 = 984$ 附近的表现类似于 $(\lambda - \lambda_0)^2$，即可得到针对 $\alpha \equiv -744,984 \bmod p$ 的定理 8.2 的对应结论，其中 λ 表示由勒让德标准形定义的模数（见 [17, § 4]）。结果是，当 $\alpha \equiv -744 \bmod p$ 时， $v_p(A_1(\hat{\alpha})) = 3$；当 $\alpha \equiv 984 \bmod p$ 时， $v_p(A_1(\hat{\alpha})) = 2$。证明至此完成。□

我们在表 2 中明确列出使 $\Gamma_0(p)^+$ 具有零亏格的 $\mathfrak{S}_p$ 集合（对应 p ）。由关于 $j(E)$ 的等价结果可知， $-744 = 0 - 744$ 属于 $\mathfrak{S}_p$ 当且仅当 $p \equiv 2$ 模 3，且 $984 = 1728 - 744$ 属于 $\mathfrak{S}_p$ 当且仅当 $p \equiv 3$ 模 4。表 2 中给出了范围 $0 \leq \hat{\alpha} < p$ 内各值 $\alpha \in \mathfrak{S}_p$ 对应的代表元 $\hat{\alpha}$；第一列和第二列分别表示 $\hat{\alpha} \equiv -744$ 模 p 和 $\hat{\alpha} \equiv 984$ 模 p。

TABLE 2. 超奇异 J_1-值的代表元，其中 p 满足 $\mathfrak{S}_p \subset \mathbb{F}_{p^2}$.

p	-744	984	其他超奇异 J_1-值
2	0	0	-
3	0	0	-
5	1	-	-
7	-	4	-
11	4	5	-
13	-	-	2
17	4	-	12
19	-	15	4
23	15	18	11
29	10	-	6, 12
31	-	23	2, 4
41	35	-	22, 26, 38
47	8	44	5, 17, 18
59	23	40	11, 12, 38, 51
71	37	61	6, 7, 14, 32, 54

取一个使 $\Gamma_0(p)^+$ 具有零亏格的素数 p。对于 $\ell = \ell_p \geq 0$，令 $\alpha_1, \ldots, \alpha_\ell$ 表示不属于 $\{-744, 984\}$ 的超奇异 J_1 值；令 β_0 和 β_1 分别表示超奇异 J_1 值 -744 和 984。请注意，对于给定的素数 p，这些值不一定都存在。由命题 3.1 中关于 $v_p(A_n(\hat{\alpha}))$ 的界可知

$$pJ_1|U_p \equiv \sum_{i=1}^{\ell} \frac{A_1(\hat{\alpha}_i)}{J_1 - \hat{\alpha}_i} \bmod p^2, \tag{3.4}$$

对每个 i，有 $v_p(A_1(\hat{\alpha}_i)) = 1$，此外还满足

$$pJ_1|U_p \equiv \frac{A_1(\hat{\beta}_1)}{J_1 - \hat{\beta}_1} + \sum_{i=1}^{\ell} \left(\frac{A_1(\hat{\alpha}_i)}{J_1 - \hat{\alpha}_i} + \frac{A_2(\hat{\alpha}_i)}{(J_1 - \hat{\alpha}_i)^2} \right) \bmod p^3, \tag{3.5}$$

其中，右侧 (3.5) 中的第一项在 β_1 不存在时约定为 0（参见表 2），而对 i 的求和在 $\ell = \ell_p = 0$时约定为 0。

由表 2 可知 β_1 存在，且对于 $p = 11$，有 $\ell_p = 0$。结合 (3.2) 和 (3.5)，我们可以直接推得以下结论。

命题 3.2。对于 $p = 11$，有 $v_p(pJ_1|U_p) = 2$。

接下来我们利用 (3.5) 求出 $p \geq 13$ 的 $v_p(pJ_1|U_p)$。

命题 3.3. 对于满足 $\Gamma_0(p)^+$ 具有零亏格的 $p \geq 13$ 素数，$v_p(pJ_1|U_p) = 1$。

证明。从表 2 可知 $\ell = \ell_p > 0$。在 $\mathbb{Z}[[q]]$ 中进行计算，写作

$$\frac{1}{J_1 - \hat{\alpha}_i} = \frac{J_1^{-1}}{1 - \hat{\alpha}_i J_1^{-1}} = J_1^{-1} \sum_{n \geq 0} (\hat{\alpha}_i J_1^{-1})^n. \tag{3.6}$$

由于 $J_1^{-n} = q^n + \mathcal{O}(q^{n+1})$，由式 (3.4) 得

$$\begin{aligned} pJ_1|U_p &\equiv \sum_{n\geq 1}\sum_{i=1}^{\ell} A_1(\hat{\alpha}_i)\hat{\alpha}_i^{n-1}J_1^{-n} \bmod p^2 \\ &\equiv \left[\sum_{i=1}^{\ell} A_1(\hat{\alpha}_i)\hat{\alpha}_i^0\right](q+\cdots) + \left[\sum_{i=1}^{\ell} A_1(\hat{\alpha}_i)\hat{\alpha}_i^1\right](q^2+\cdots) + \cdots \bmod p^2. \end{aligned} \tag{3.7}$$

若 $J_1|U_p \equiv 0 \bmod p$ 成立，则可推出

$$\sum_{i=1}^{\ell} A_1(\hat{\alpha}_i) \equiv \sum_{i=1}^{\ell} A_1(\hat{\alpha}_i)\hat{\alpha}_i \equiv \sum_{i=1}^{\ell} A_1(\hat{\alpha}_i)\hat{\alpha}_i^2 \equiv \cdots \equiv 0 \bmod p^2. \tag{3.8}$$

然而，

$$M = \begin{bmatrix} \hat{\alpha}_1^0 & \hat{\alpha}_1^1 & \cdots & \hat{\alpha}_1^{\ell-1} \\ \vdots & \vdots & \vdots & \vdots \\ \hat{\alpha}_1^0 & \hat{\alpha}_\ell^1 & \cdots & \hat{\alpha}_\ell^{\ell-1} \end{bmatrix} \tag{3.9}$$

是一个范德蒙德矩阵，且 $\hat{\alpha}_1$、.....、$\hat{\alpha}_\ell$ 互不相同，因此 M 可逆。若 (3.8) 成立，则 $(A_1(\hat{\alpha}_1)\ \cdots,\ A_1(\hat{\alpha}_\ell))^T$ 将属于 M^T 模 p^2 的核，这与对每个 i 都有 $v_p(A_1(\hat{\alpha}_i)) = 1$ 这一事实矛盾。因此，$v_p(pJ_1|U_p) = 1$，证毕。□

4. Proofs of Theorems 1.1 and 1.2

本节首先给出若干命题，用以确定 $\Gamma_0(p)$ 亏格为零时的 $v_p(J_1 - J_p)$ 和 $v_p(J_1 - J_{p+})$，并确定 $\Gamma_0(p^2)$ 亏格为零时的 $v_p(J_1 - J_{p^2})$。

命题 4.1. 设 p 为素数，且 $\Gamma_0(p)$ 的亏格为零。则 *(1.8)* 和 *(1.9)* 均成立。

证明. 根据引理 2.3，涉及的素数是满足 $p-1$ 整除 12 的那些 p。利用表 1，我们检验可知，对于这些素数，$v_p(c_1(J_1 - J_p))$ 与 (1.9) 右侧一致。于是由命题 2.13 得出 (1.9)。特别地，我们有

$$v_p(J_1 - J_p) = v_p(c_1(J_1 - J_p)) > \tfrac{12}{p-1}. \tag{4.1}$$

令 $d = d_p$。那么，为证明 (1.8)，我们需要检验 $v_p(J_1 - J_{p+}) = \frac{d}{2}$。根据 (2.13)，由于 $J_{p+} \equiv J_p$ 模 $p^{\frac{d}{2}}$，由 (4.1) 可得 $v_p(J_1 - J_{p+}) \geq \frac{d}{2}$。对于反向不等式，我们再次应用 (2.13)，得到 $c_1(J_1 - J_{p+}) = c_1(J_1 - J_p) - p^{\frac{d}{2}}$，并利用 (4.1)（参见引理 2.10）推出 $v_p(c_1(J_1 - J_{p+})) = \frac{d}{2}$。根据定义，$v_p(J_1 - J_{p+}) \leq v_p(c_1(J_1 - J_{p+}))$，因此结论成立。□

命题 4.2. 设 p 为素数，且 $\Gamma_0(p^2)$ 的亏格为零。则 *(1.10)* 成立。

证明. 引理 2.3 告诉我们 $p \in \{2, 3, 5\}$，特别是 $p^2 - 1$ 整除 24。因此 $d_{p^2} = \frac{24}{p^2-1}$，我们需要证明 $v_p(J_1 - J_{p^2}) = d_{p^2}$（参见 (2.5)）。这可由 v_p 的性质推出（参见引理 2.10），因为命题 4.1 给出 $v_p(J_1 - J_p) > d_{p^2}$，而命题 2.14 告诉我们 $v_p(J_p - J_{p^2}) = d_{p^2}$。□

现在我们可以证明主要结果了。

定理*1.1*的证明. 首先，假设 $\Gamma_0(p)^+$ 具有正亏格。那么，按照我们的约定，J_p、J_{p+} 和 J_{p^2} 都为零，因此右侧 (1.6) 中的每一项均为 $v_p(J_1) = 0$。这就证明了对于满足 p 且 $\Gamma_0(p)^+$ 不具有零亏格的情形，定理1.1成立。

接下来考虑 $\Gamma_0(p)^+$ 具有零亏格、但 $\Gamma_0(p)$具有正亏格的情形。也就是说，p 整除 $\#\mathbb{M}$ (1.1)，并且 $p = 11$ 或 $p > 13$ （参见引理 2.3）。于是，(1.6) 的右端化简为

$v_p(J_1 - J_{p+})$，根据引理 2.9 和引理 2.10，这就是 $v_p(pJ_1|U_p)$。命题 3.2 给出，对于 $p = 11$，有$v_p(pJ_1|U_p) = v_p(\#\mathbb{M})$，而命题 3.3 处理 $p > 13$。

尚需考虑那些素数 $p > 3$，使得 $\Gamma_0(p)$ 具有零亏格，即 $p \in \{5, 7, 13\}$（参见引理 2.3）。对于 $p \in \{7, 13\}$，群 $\Gamma_0(p^2)$ 具有正亏格（参见引理 2.3），且 (1.6) 的右端化为 $v_p(J_1 - J_{p+}) + v_p(J_1 - J_p)$。所需等式随即由命题 4.1 推出。命题 4.1–4.2 处理 $p = 5$。至此证明完成。□

定理 *1.2* 的证明。根据 Ogg 的工作 [30]，，群 $\Gamma_0(p)^+$ 恰在 $\mathfrak{S}_p^2$ 非空时具有正亏格。$\Gamma_0(p)^+$ 具有零亏格而 $\Gamma_0(p)$ 具有正亏格的情形，恰好就是 $\#\mathfrak{S}_p = \#\mathfrak{S}_p^1 > 1$ 的情形，且 $\Gamma_0(p)$ 恰在 $\#\mathfrak{S}_p = \#\mathfrak{S}_p^1 = 1$ 时具有零亏格。因此，对于使得 $\Gamma_0(p)^+$ 具有正亏格的素数 p，(1.7) 正确地取值为 0。此外，由表 2 与[34, III. 定理 10.1]，我们有

$$m_p = \begin{cases} 2 & \text{if } p \in \{13, 17, 19, 23, 29, 31, 41, 47, 59, 71\}, \\ 4 & \text{if } p \in \{7, 11\}, \\ 6 & \text{if } p = 5, \\ 12 & \text{if } p = 3, \\ 24 & \text{if } p = 2. \end{cases} \tag{4.2}$$

因此，$v_p(\#\mathbb{M}) = \frac{1}{2}m_p$ 对于素数 $p > 3$，使得 $\Gamma_0(p)^+$ 具有零亏格且 $\Gamma_0(p)$ 具有正亏格，而 $v_p(\#\mathbb{M}) = \frac{3}{2}m_p$ 对于素数 $p > 3$，使得 $\Gamma_0(p)$ 具有零亏格，如所欲证。□

References

[1] L. Beneish. 拟模月光与算术联系。 *Trans. Amer. Math. Soc.*, 372 8813, 2019 12 8793( ): – .[2] R. Borcherds. 怪兽月光与怪兽李超代数。 *Invent. Math.*, 109(2):405–444, 1992. [3] S. Carnahan. 广义月光，II：Borcherds 乘积。 *Duke Math. J.*, 161(5):893–950, 2012. [4] M. Cheng 和 J. Duncan. 最大 Mathieu 群与（拟）自守形式。载于 *String-Math 2011*，第 *Proc. Sympos. Pure Math.* 卷，第 53–82 页。美国数学会，普罗维登斯，罗得岛州，2012年。[5] M. Cheng、J. Duncan 和 J. Harvey. 影子月光。 *Commun. Number Theory Phys.*, 8(2):101–242, 2014. [6] M. Cheng、J. Duncan 和 J. Harvey. 影子月光与 Niemeier 格。 *Res. Math. Sci.*, 1 3, 81, 2014 :Art. . [7] M. Cheng、J. Duncan 和 M. Mertens. 类数、循环单群与算术。 *J. Lond. Math.* , ( ): – . [8] *Soc. (2)* 108 1 238 272, 2023
M. Cheng、J. Duncan 和 M. Mertens. 类数、合同数与影子月光。
J. Number , : – . [9] J. *Theory* 277 201 235, 2025
Conway、R. Curtis、S. Norton、R. Parker 和 R. Wilson. $\mathbb{ATLAS}$ *of finite groups*。牛津大学出版社，Eynsham，1985年。单群的极大子群与普通特征标，计算工作由 J. G. Thackray 协助。[10] J. Conway 和 S. Norton. 怪兽月光。 *Bull. London Math. Soc.*, 11(3):308–339, 1979年。[11] J. Cremona. *Algorithms for modular elliptic curves*。剑桥大学出版社，剑桥，第二版，1997年。[12] J. Duncan、M. Griffin 和 K. Ono. 影子月光猜想的证明。 *Res. Math. Sci.*, 2 26, 47, 2015 :Art. .[13] J. Duncan、J. Harvey 和 B. Rayhaun. 半影月光概述。 *To appear in Communications in Number Theory and Physics* 。[14] J. Duncan、M. Mertens 和 K. Ono. O'Nan 月光与算术。 *Amer. J. Math.*, 143(4):1115–1159, 2021年。[15] J. Duncan、M. Mertens 和 K. Ono. 散群月光。 *Nature Communications*, 8:670, 2017年9月。[16] J. Duncan 和 K. Ono. Jack Daniels 问题。 *J. Number Theory*, 161:230–239, 2016年。[17] B. Dwork. p进循环。 *Inst. Hautes Études Sci. Publ. Math.*, (37):27–115, 1969年。[18] T. Eguchi、H. Ooguri 和 Y. Tachikawa. 关于 $K3$ 曲面与 Mathieu 群 M_{24}的札记。 *Exp. Math.*, 20 1 91 96, 2011 ( ): – . [19] I. Frenkel、J. Lepowsky 和 A. Meurman. Fischer-Griess 怪兽群的一个自然表示，其特征标为模函数 J。 *Proc. Nat. Acad. Sci. U.S.A.*, 81(10, Phys. Sci.):3256–3260, 1984年。

[20] I. Frenkel、J. Lepowsky 和 A. Meurman. 怪兽群的一个月光模块。载于 *Vertex operators in mathematics and physics (Berkeley, Calif., 1983)* 3 *Math. Sci. Res. Inst. Publ.* 231 273 ，第 卷，页码 – 。施普林格，纽约，1985年。[21] I. Frenkel、J. Lepowsky 和 A. Meurman. *Vertex operator algebras and the Monster* 134 *Pure and Applied Mathematics* ，第 卷。学术出版社公司，波士顿，马萨诸塞州，1988。[22] T. Gannon. 关于 Mathieu 的诸多讨论。 *Adv. Math.*, 301:322–358, 2016年。[23] R. Griess, Jr. 将 F_1 196, 883 *Proc. Nat. Acad. Sci. U.S.A.* 78 2, 1 686 691, 1981 构造为一个 维代数的自同构。 , (部分): – . [24] R. Griess, Jr. 友善巨人。 *Invent. Math.*, 69(1):1–102, 1982年。[25] R. Griess, Jr. “怪兽”单群的结构。载于 *Proceedings of the Conference on Finite Groups (Univ. Utah, Park City, Utah, 1975)* 113 118 1976 ，页码 – 。学术出版社公司，纽约，。[26] J. Harvey 和 B. Rayhaun. 奇异模数的迹与汤普森群的月光。 *Commun. Number* , ( ): – . [27] M. Khaqan. *Theory Phys.* 10 1 23 62, 2016 椭圆曲线与汤普森散在单群。 *J. Number Theory*, 224:274–306, 2021年。[28] M. Koike. 模形式与模函数之间的同余及其在 Atkin 猜想中的应用。 *J.* , : – . [29] J. McKay，CRM菲尔兹奖讲座，2004年3月。[30] A. Ogg. 模曲线的自同构。载于 *Séminaire Delange-Pisot-Poitou (16e année: 1974/75), Théorie des nombres* 7, 8 ´ 1975 ， *Fasc. 1*，第 Exp. No. 页。数学秘书处，巴黎，。[31] K. Ono. *The web of modularity: arithmetic of the coefficients of modular forms and q-series*, *CBMS Regional Conference Series in Mathematics*第 102 卷。由数学科学会议委员会出版，华盛顿特区，2004年。[32] M. Ronan. *Symmetry and the monster*。牛津大学出版社，牛津，2006年。[33] G. Shimura. *Introduction to the arithmetic theory of automorphic functions* 11 *Publications of the Mathematical Society of Japan* ，第 卷。普林斯顿大学出版社，普林斯顿，新泽西州。原著重印本，《Kanô 纪念讲座》第 1 卷。[34] J. Silverman. *The arithmetic of elliptic curves*, *Graduate Texts in Mathematics*第 106 卷。施普林格，多德雷赫特，第二版，2009年。[35] H. Swisher. 关于黑克算子以及 Dwork 和 Koike 定理的一条注记。 *Illinois J. Math.*, 48 356, 2004 1 353( ): – .[36] J. Thompson. 有限群与模函数。 *Bull. London Math. Soc.*, 11(3):347–351, 1979年。[37] J. Thompson. Fischer-Griess 怪兽群与椭圆模函数之间的一些数字关系。 *Bull.* , ( ): – . [38] H. Wang 和 B. Williams. 马蒂厄月光与 Borcherds 乘积。 *Commun. Number Theory Phys.*, 19 1 135 168, 2025 ( ): – .

Institute of Mathematics, Academia Sinica, Taipei, Taiwan
Email address: jduncan@as.edu.tw

Department of Mathematics, Oregon State University, Corvallis, Oregon, U.S.A.
Email address: swisherh@oregonstate.edu