非同余子群上的模形式数据库

DAVID BERGHAUS、HARTMUT MONIEN 和 DANYLO RADCHENKO

Abstract. 我们展示了一个数据库，其中收录了指数为 ≤ 17 的非同余子群上、权不超过六（包括权六）的数百个模形式。此外，我们的数据库还包含零属子群的贝利映射表达式、亏格为一的子群所对应的椭圆曲线方程，以及精度达到 1500 位的非同余艾森斯坦级数数值近似。

arXiv:2301.02135v1 [math.NT] 5 Jan 2023

1. Introduction

非同余子群上的模形式理论仍未得到充分理解（关于近期进展，参见 [6, 7]）。在这项工作中，我们提供了大量计算实例，希望这些实例能够促成新的观察和猜想。构建非同余子群上的模形式数据库，已被列为 AIM 研讨会 非同余模形式与模性 [17]提出的未来研究目标之一。Atkin 和 Swinnerton-Dyer [1] 已经证明了计算机生成数据对于研究非同余子群上的模形式具有实用价值；他们仅依据少数几个计算实例，就提出了关键猜想。尽管如此，目前计算出的非同余子群上的模形式仍然极少。已知实例通常局限于非同余特征群 [12, 15] ，或指数非常低的非同余子群 [13] ，以及少数几个指数较大的零属情形 [19]。

在本文中，我们应用 [3] 的算法，建立一个非同余子群上的模形式数据库。这补充了现有的相关数据库，例如同余子群上的经典模形式数据库 [5], 、希尔伯特模形式数据库 [11], 以及贝利映射数据库 [20]。

2. Background and Notation

2.1. 模形式。 令 SL(2,Z) 为行列式为 1 的 2×2 整数矩阵群，并令 G 为 SL(2,Z) 的有限指数子群。群 G 的权为 k 的模形式，是定义在上半平面 $\mathcal{H} := \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$ 上且满足以下变换律的全纯函数

$$f(\gamma(\tau)) = (c\tau + d)^k f(\tau)\,, \qquad \text{for all } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G\,, \tag{2.1}$$

其中

$$\gamma(\tau) := \frac{a\tau + b}{c\tau + d}\,, \tag{2.2}$$

并且 $(c\tau + d)^{-k} f(\gamma(\tau))$ 在 $\mathrm{Im}(\tau) \to \infty$时有界，对所有 $\gamma \in$SL(2,Z) 均成立。本文将限于不存在乘子系、且 k 为偶整数的情形。并且不失一般性，我们可以改为考虑商群 PSL(2,Z) :=SL(2,Z)/$\{\pm 1\}$，记作 Γ ，并将 G 视为 Γ的有限指数子群。关于经典模形式的广博理论，读者可参阅 Cohen 和 Str¨omberg 的著作 [8]、Diamond 和 Shurman 的著作 [10] ，以及 Zagier 的讲义 [26]。本文的框架和记号沿用 [3]中的用法。

子群 $\Gamma(N) \leqslant \Gamma$ 定义如下：

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \quad \text{and} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \right\}, \tag{2.3}$$

称为层 N 的主合同子群。若有限指数子群 $G \leqslant \Gamma$ 不包含任意 $N \geq 1$对应的 $\Gamma(N)$，则称其为非同余子群。

设 G 是 Γ 的任意有限指数子群，且 f 是权为 $k \in 2\mathbb{Z}_{>0}$的模形式。那么 f 具有傅里叶展开

$$f(\tau) = \sum_{n=0}^{\infty} a_n q_h^n, \tag{2.4}$$

其中 $q_h := \exp(2\pi i \tau / h)$，而 h 表示 ∞处尖点的宽度。可以为非同余子群上的模形式空间选取基，使其傅里叶系数定义在有理数域 $\mathbb{Q}$ 上；此外，这些系数还可以写成如下形式（见 [1,21]）

$$a_n = u^n b_n, \tag{2.5}$$

其中 b_n 和 u^h 属于某个数域 K。我们固定 v，使其成为 K 在有理数域 $\mathbb{Q}$ 上的生成元（即 $K = \mathbb{Q}(v)$，其中 v 为代数数）。我们还将包含所有 a_n 的数域记为 $L = \mathbb{Q}(w)$。

2.2. **Belyi 映射**。

定义 2.1（贝利映射）。设 X 是一个紧黎曼曲面。一个全纯函数

$$f : X \to \mathbb{P}^1(\mathbb{C}), \tag{2.6}$$

若它在三个点之外均无分歧，则称为一个贝利映射 。

覆盖映射

$$R : X(G) \to X(\Gamma) \overset{j}{\cong} \mathbb{P}^1(\mathbb{C}), \tag{2.7}$$

是一个贝利映射，其中 $X(G) = \overline{G \backslash \mathcal{H}}$ 是 G 的模曲线。如果 G 是一个零属子群，那么覆盖映射 $R(j_G)$ 是主模函数 j_G 的有理函数，其分歧点位于椭圆点和尖点的像上。请注意，该贝利映射可以定义在与上文相同的域 K 上。

2.3. **特征与护照**。

定义 2.2（签名）。我们将 $G \leqslant \Gamma$ 的签名 定义为元组 $(\mu, g, n(c)\ n(e_2)\ n(e_3))$，其中 μ 表示 G 在 Γ 中的指数，g 表示基本域 $\mathcal{F}(G)$ 的亏格，$n(c)$ 表示 G 的尖点数，$n(e_2)$ 和 $n(e_3)$ 分别表示二阶和三阶椭圆点的数量。

签名可用于区分不同类型的子群。还可以利用护照这一概念作进一步区分：

定义 2.3（护照）。给定一组签名相同的子群，根据 Millington 定理 [18],，它们对应于元组 $(\sigma_S, \sigma_R, \sigma_T)$，这些元组是 S_μ 共轭类的代表。若两个子群的单值群（即由 σ_S 和 σ_R 生成的置换群）在 S_μ 中共轭，则称它们属于同一护照。

了解护照很有用，因为绝对伽罗瓦群对贝利映射的作用会保持护照不变，因此护照的大小（即护照中元素的数量）为数域 K 的次数提供了一个上界。

3. Numerical Computation of Elliptic Curves

在 [3] 中，我们展示了如何以高精度数值计算非同余子群上模形式的傅里叶展开。本节将说明如何据此计算出与亏格一非同余子群对应的椭圆曲线方程。我们采用的方法与 Cremona [9,第二章]所述方法类似。令$f \in S_2(G)$表示亏格一群的一个非平凡权二尖点形式 G （注意，对于亏格一群，$\dim(S_2) = 1$，这意味着 f 在规范化意义下唯一）。通过应用 [3]的算法，可以数值计算 f 在所有尖点处的傅里叶展开。然后我们定义积分

$$I_f(\alpha,\beta) := \int_\alpha^\beta 2\pi i f(\tau)d\tau\,, \tag{3.1}$$

其中 α，$\beta \in \overline{\mathcal{H}}$ 和

$$I_f(\tau_0) := I_f(\tau_0, i\infty) = \int_{\tau_0}^{i\infty} 2\pi i f(\tau)d\tau = -\sum_{n=1} \frac{a_n}{n}\exp(2\pi i n\tau_0/h)\,, \tag{3.2}$$

其中 h 表示尖点宽度。于是，周期映射 P_f 定义为

$$P_f(\gamma) := I_f(\tau_0, \gamma(\tau_0)) = I_f(\tau_0) - I_f(\gamma(\tau_0))\,, \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G\,, \tag{3.3}$$

它与基点 τ_0 的选取无关，并定义了从 G 到周期格 $\Lambda_f = \mathbf{Z}w_1 + \mathbf{Z}w_2$的同态，其中 w_1，$w_2 \in \mathbf{C}$（见 [9]）。

3.1. 计算 $P_f(\gamma)$。 由于我们进行数值计算，基点 τ_0 的选取应使计算 $P_f(\gamma)$时的精度最大化。为此，应使 τ_0 和 $\gamma(\tau_0)$的虚部中的较小值最大化。如果 G 只有一个尖点，我们选择

$$\tau_0 = -\frac{d}{c} + \frac{1}{c}i \in \mathcal{H}\,, \tag{3.4}$$

对于 $c > 0$ （若 $c = 0$ 则 $P_f(\gamma) = 0$ 且若 $c < 0$ 则我们只需选择 γ 在 $\mathrm{PSL}(2,\mathbf{Z})$ 中的另一个代表元）。注意，对于这一选择的 τ_0，我们有 $\gamma(\tau_0) = a/c + i/c$，这意味着 τ_0 和 $\gamma(\tau_0)$ 的虚部相等。

如果 G 有多个尖点，我们将与尖点 p 相关联的尖点正规化子记为 A_p （采用约定 $A_p(i\infty) = p$），并将 p 处的尖点展开记为 $f_p = f|_2 A_p$。于是我们得到

$$P_f(\gamma) = I_{f_p}(\tau_{0,p}) - I_{f_p}((A_p^{-1}\gamma A_p)(\tau_{0,p}))\,. \tag{3.5}$$

令 $\gamma_p := A_p^{-1}\gamma A_p = \begin{pmatrix} a_p & b_p \\ c_p & d_p \end{pmatrix}$。那么我们选择

$$\tau_{0,p} = -\frac{d_p}{c_p} + \frac{1}{c_p}i \in \mathcal{H}\,, \tag{3.6}$$

并使用尖点 p 处的展开来计算 $P_f(\gamma)$，其中取使 $c_p \cdot h_p$ 最小的尖点（这里 h_p 表示尖点 p 的尖点宽度）。

3.2. 计算 Λ_f。 数值计算周期格 Λ_f 的方法可概述如下：

(1) 计算集合 $S = \{P_f(\gamma_1)\ P_f(\gamma_2)\ \ldots\}$，其中 γ_j 表示 G的一组生成元。(2) 从集合 S 中移除（近似）零元素（它们显然位于格上）以及（近似）重复元素。(3) 任取两个线性无关元素 w_1，$w_2 \in S$，作为 Λ_f的一组基的初步猜测。

(4) 通过求解，将其余元素表示为有理数域 $\mathbb{Q}[w_1, w_2]$ 中的元素

$$\begin{pmatrix} \mathrm{Re}(w_1) & \mathrm{Re}(w_2) \\ \mathrm{Im}(w_1) & \mathrm{Im}(w_2) \end{pmatrix} \cdot \begin{pmatrix} r_j \\ s_j \end{pmatrix} = \begin{pmatrix} \mathrm{Re}(P_f(\gamma_j)) \\ \mathrm{Im}(P_f(\gamma_j)) \end{pmatrix}, \tag{3.7}$$

得到 $P_f(\gamma_j) = r_j w_1 + s_j w_2$ 其中 $r_j,\ s_j \in$ 有理数域。

（5）求最小公分母 λ，使得对所有 j，$\lambda r_j,\ \lambda s_j \in \mathbb{Z}$。

（6）通过计算厄米特标准形，求由 $\lambda \cdot (r_j,\ s_j)$ 张成的 $\mathbb{Z}^2$-子模的基矩阵 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$。

（7）切换到格基

$$w_1, w_2 \mapsto \frac{a w_1 + b w_2}{\lambda}, \frac{c w_1 + d w_2}{\lambda}. \tag{3.8}$$

（8）计算 $\tau := w_1/w_2$，使 $\mathrm{Im}(\tau) > 0$（如有必要则交换 w_1 和 w_2），并将 τ 变换到 Γ 的基本域中，从而得到与 Λ_f等价的格 $\mathbb{Z} + \mathbb{Z}\tau$。

注记 3.1。元素 $S = \{P_f(\gamma_1)\ P_f(\gamma_2)\ ...\}$ 的精度取决于生成元代表的选择（我们使用 Sage 计算这些代表）。据我们所知，目前还没有任何算法能够生成在以下意义上最优的生成元：τ_0 的虚部可能达到最大值，参见第3.1节。因此，我们对 G 施以 $\sigma = (1\ j)$ 共轭，其中$j = 2,\ .....,\ \mu$（以 G的置换群表示计），并选择使 τ_0 的高度达到最大的代表。尽管这种选择可能并不理想，因为 τ_0 的高度可能低于基本域的高度，即 $\mathrm{Im}(\mathcal{F}(G)) = \sqrt{3}/(2h_{\max})$, 其中 $h_{\max}$ 表示最大的尖点宽度（这意味着我们无法以完整精度计算 $P_f(\gamma)$），但在实践中，精度始终足以确定椭圆曲线。

3.3. **椭圆曲线的计算**。得到周期格 Λ_f 后，椭圆曲线的计算就变得直接明了。我们首先计算椭圆不变量

$$g_2(\tau) = 60 G_4(\tau) = 60 \sum_{(m,n)\neq(0,0)} (m + n\tau)^{-4}, \tag{3.9}$$

其中 $G_4(\tau) = (\pi^4/45) E_4(\tau)$，并且

$$g_3(\tau) = 140 G_6(\tau) = 140 \sum_{(m,n)\neq(0,0)} (m + n\tau)^{-6}, \tag{3.10}$$

wh其中 $G_6(\tau) = (2\pi^6/945) E_6(\tau)$，使用 Arb [14]。然后，$j$-不变量由下式给出

$$j(\tau) = 1728 \frac{g_2^3}{g_2^3 - 27 g_3^2}. \tag{3.11}$$

之后，我们将 $j(\tau)$ 识别为有理数域 K 中的一个代数数（使用 LLL算法 [16]），并使用 Sage [22] 求出椭圆曲线的方程。

例 3.2。考虑非合同子群 G，其单值群为 $\mathrm{PSL}_2(\mathbb{F}_8)$，签名为 (9，1，1，1，0)，对应于可容许置换对 $(\sigma_S,\ \sigma_R)$，其中$\sigma_S = (1)(2\ 5)(3\ 7)(4\ 8)(6\ 9)$，且 $\sigma_R = (1\ 2\ 6)(3\ 8\ 5)(4\ 9\ 7)$。我们发现 $\tau = 0.332234... + 0.744371... i$，且 j-不变量的值为 $\approx -1159088625/2097152$，由此得到椭圆曲线

$$E\colon y^2 + xy + y = x^3 - x^2 - 95x - 697 \tag{3.12}$$

其导子为 162。我们可以通过计算 $S_6(G)$ 的三个权 6 尖点形式（此处记作 x，y，z）来验证这一结果，并观察到它们满足关系

$$-xy^2+(-2w)y^3+x^2z+(-w)xyz+(19w^2)y^2z+(-3w^3)yz^2+(15w^4)z^3=0, \tag{3.13}$$

对于 $w=(-27/256)^{1/9}$。代入 $x\mapsto xw$, $z\mapsto z/w$ 并除以 w，我们得到三次方程

$$-xy^2-2y^3+x^2z-xyz+19y^2z-3yz^2+15z^3=0\,, \tag{3.14}$$

定义在有理数域 Q 上，由此我们利用 Sage 得到关于 E 的相同方程。

4. 数据库结构

Str¨omberg[24] 已计算出指数为 $\mu\le 17$ 的非同余子群数据库，可在 [23] 获取。我们以此为基础构建了自己的数据库。

注记 4.1。 我们开发了一种算法，可以列出指数高于 [23, 24] 中已计算出的子群。借助该算法，我们能够生成所有指数为 $\mu\le 30$ 的子群。不过，后来我们发现了 Vidal 的一篇论文 [25]，其中介绍了一种用于完成同一任务、效率高得多且基本上最优的算法。我们计划在可预见的未来将更高指数的子群加入数据库。

4.1. **数据库标签**。 每个数据库条目都以护照中所含元素的签名作为标签，后接护照的 id，以及用于标记伽罗瓦轨道的字母。

例 4.2。 考虑签名为 (15，1，2，1，0)、单值群为 S_{15} 的护照。该护照包含三个元素（这是数据库中具有此签名的第四个护照[23]，因此我们将其 id 设为 3）。此护照分解为两个伽罗瓦轨道：第一个轨道的标签为 $15\,1\,2\,1\,0\,3\,a$，其中 $K=\mathbb{Q}(v)$，而 $v^2-v-1=0$；第二个轨道的标签为 $15\,1\,2\,1\,0\,3\,b$，其中 $K=\mathbb{Q}$。

4.2. **置换三元组规范化**。 每个数据库条目在置换三元组规范化（即在 $\mathrm{SL}_2(\mathbb{Z})$ 中共轭）意义下都是唯一的。我们通常将 σ_T 规范化，使循环类型按降序排列，标签按升序排列。这意味着最大的尖点位于无穷远处。虽然这会使数域 L 的次数更高（因此运算速度更慢），但 u 和 v 中的因式分解表达式通常包含较小的因子，因此更易读。

例4.3。 考虑置换 (1 2 34)(5 6 7)(89)，其循环类型为按降序排列的 (4，3，2)。

上述策略有三个例外。第一种情况是子群 G 有多个宽度相同的尖点。将其中一个尖点置于无穷远处，可能会因对称性被破坏而使 K 的次数增大。因此，在这种情况下，我们将 σ_T 规范化，使宽度唯一且最大的尖点位于无穷远处。第二种例外是 G 有一个宽度为 1 的（唯一）尖点。在这种情况下，我们将宽度为 1 的尖点置于无穷远处，因为这样 $K=L$会更方便。第三种例外适用于亏格为一的子群：如果另一种规范化方式能在计算椭圆曲线时获得更高精度（见第3节），我们就不将 σ_T 的标签按升序排列。

4.3. **针对每个数据库元素计算的数据**。对于每个数据库元素，我们都计算了曲线（零属子群对应贝利映射，亏格为一的子群对应椭圆曲线），以及主模函数、尖点形式和模形式的傅里叶展开，权数最高至 6（包括 6）。对于零属子群，我们通过应用 [3, Section 5] 中的算法，在一个数

域 L 上实现了这一点。对于高亏格子群，我们使用 [3, Section 4.3.2] 中的方法，计算了对应傅里叶展开的数值近似，精度达到 1500 位，并由此利用 LLL算法猜测其闭式解。值得一提的是，出于效率考虑，并不需要从头开始计算所有形式。相反，我们通过计算尖点形式与模形式的乘积来生成（部分）高权形式。此外，我们还使用 [4] 中描述的一种算法，计算了将 M_k 映射到 E_k 的基因子的数值近似，精度达到 1500 位。有趣的是，我们未能在这些表达式之间找到任何代数依赖。

4.4. 一个完整示例。 举一个具体的例子，让我们来看看数据库条目15 1 2 1 0 2 a。

- G：子群 G 对应于由以下元素生成的置换群：

$$\sigma_S = (1\,15)(2\,12)(3\,7)(4\,9)(5\,13)(6\,10)(8\,14)(11)\,,$$
$$\sigma_R = (1\,11\,12)(2\,13\,6)(3\,8\,15)(4\,10\,7)(5\,14\,9)\,,$$
$$\sigma_T = (1\,3\,4\,5\,6\,7\,8\,9\,10\,2)(11\,12\,13\,14\,15)\,.$$

- 单值群：$(C_3 \times C_3 \times C_3 \times C_3) : (C_2 \times A_5)$。
- K：$v = 1$（即，K =有理数域）。
- 嵌入：$v = 1$。
- u：$(-3125/14348907)^{1/10}$，带有一个嵌入 $-0.409269... - 0.132979... \cdot i$。
- L：$w^8 - 5/27w^6 + 25/729w^4 - 125/19683w^2 + 625/531441$，带有 $w = -0.409269... - 0.132979... \cdot i$。

- 曲线：$y^2 + xy + y = x^3 - x^2 + 7x - 103$。
- 傅里叶展开（最多 ~ 700 项）：– M_2:

  * $m_0 = 1 + 48/5u^2q_{10}^2 - 528/5u^3q_{10}^3 - 2448/25u^4q_{10}^4 - 3096/25u^5q_{10}^5 + ...$。
  * $m_1 = q_{10} + uq_{10}^2 - 21/5u^2q_{10}^3 + 101/5u^3q_{10}^4 + 816/25u^4q_{10}^5 + ...$。– S_2:

  * $s_0 = q_{10} + uq_{10}^2 - 21/5u^2q_{10}^3 + 101/5u^3q_{10}^4 + 816/25u^4q_{10}^5 + ...$（在此情形下，这与 m_1 相同）。– E_2:

  * e_0：我们给出艾森斯坦基底矩阵 $[1, 0.356085... + 0.115699... \cdot i]$（至多 1500 项），这意味着 $e_0 = m_0 +$（$0.356085... + 0.115699... \cdot i$）$m_1$。请注意，此基已经过典范归一化。– M_4:

    * $m_0 = 1 - 688747536/625u^{10}q_{10}^{10} + ...$（这是来自 Γ 的一个旧形式，即 SL(2,Z) 的权 4 Eisenstein 级数）。
    * $m_1 = q_{10} - 70111/110u^4q_{10}^5 + ...$。
    * $m_2 = q_{10}^2 - 621/22u^3q_{10}^5 + ...$。
    * $m_3 = q_{10}^3 + 237/22u^2q_{10}^5 + ...$。
  * $m_4 = q_{10}^4 - 115/22uq_{10}^5 + ...$。– S_4:

    * $s_0 = q_{10} - 65u^3q_{10}^4 - 1488/5u^4q_{10}^5 + ...$。
    * $s_1 = q_{10}^2 - 27/5u^2q_{10}^4 + ...$。
  * $s_2 = q_{10}^3 - uq_{10}^4 + 16u^2q_{10}^5 + ...$。– E_4:

    * $e_0 = m_0$。
    * $e_1 = m_1 + (12.068314... + 3.921233... \cdot i)m_2 + (106.205344... + 77.162699... \cdot i)m_3 + (-61.318023... - 84.397019... \cdot i)m_4$.
    * $e_{0,\text{可以}}$：对于典范归一化，我们得到$e_{0,\text{可以}} = e_0 + (-0.014977... - 0.004866... \cdot i)e_1$。

亏格 / 指数	0	1
7	3/3	0
8	1/1	0
9	9/9	1/1
10	9/9	1/1
11	6/6	0
12	23/27	2/3
13	22/23	1/1
14	21/29	1/2
15	54/62	7/9
16	36/65	7/9
17	16/35	1/2
总计	200/269	21/28

TABLE 1. 目前数据库中计算得到的护照数量。（请注意，不存在满足 $\mu \leq 17$ 和 $g > 1$的非同余子群。）

$$* \ e_{1,\mathrm{can}} = (0.059909... + 0.019465... \cdot i)e_1.$$

（数据库中也给出了权为六的空间，但此处未列出。）

4.5. 数据库状态。 当前版本中计算得到的护照数量见表 1。目前，数据库压缩后的大小为 ~ 6GB，未压缩时为 ~ 16GB。总计使用了约 25000 小时的 CPU时间，在 `Intel Xeon E5-2680 v4 @ 2.40GHz` 上计算这些数据。

4.6. 结果的可靠性。 对于零属，所有系数均使用数域上的严格算术或严格区间算术计算得出。唯一的例外是艾森斯坦级数，其精度只能通过启发式方法估计。对于高属，系数并非严格计算得出（但有极具说服力的数值证据支持），因为这些系数是通过 LLL算法猜测得到的。作为额外验证，我们还将严格表达式和艾森斯坦级数的数值与使用不同 horocycle高度通过 Hejhal方法进行的计算结果进行了比较，以确认结果至少在 10 位精度上吻合。

4.7. 如何访问数据库。 目前，数据库以 GITHUB存储库的形式提供，地址为 [2] ，并计划很快发布到 LMFDB。运行 SAGE 脚本即可加载数据库条目；脚本会返回一个包含结果的 PYTHON 字典。与将结果存储为序列化对象相比，这样能更好地兼容不同版本。此外，我们还以字符串形式将结果打印在 JSON文件中。为节省存储空间，我们没有保存傅里叶系数的数值近似。出于同样的原因，我们也没有显式存储数域L 上的表达式，而是在加载 SAGE 脚本时，通过代入 v 和 w的值来生成这些表达式。

5. SOME NOTABLE EXAMPLES

5.1.的最高次数 K。 K 的最高次数出现在护照16 0 3 2 1 11 a 中，此时得到 $K = \mathbb{Q}(v)$，其中$v = 1.531805... + 0.185685...i$ 是以下多项式的一个根

$$0 = v^{24} - 6v^{23} + 21v^{22} - 60v^{21} + 184v^{20} - 478v^{19} + 651v^{18} - 1220v^{17} + 2230v^{16} + 1226v^{15} - 947v^{14} + 804v^{13} - 7092v^{12} - 6862v^{11} + 3971v^{10} - 15340v^9 + 7975v^8 + 36044v^7 + 7134v^6$$

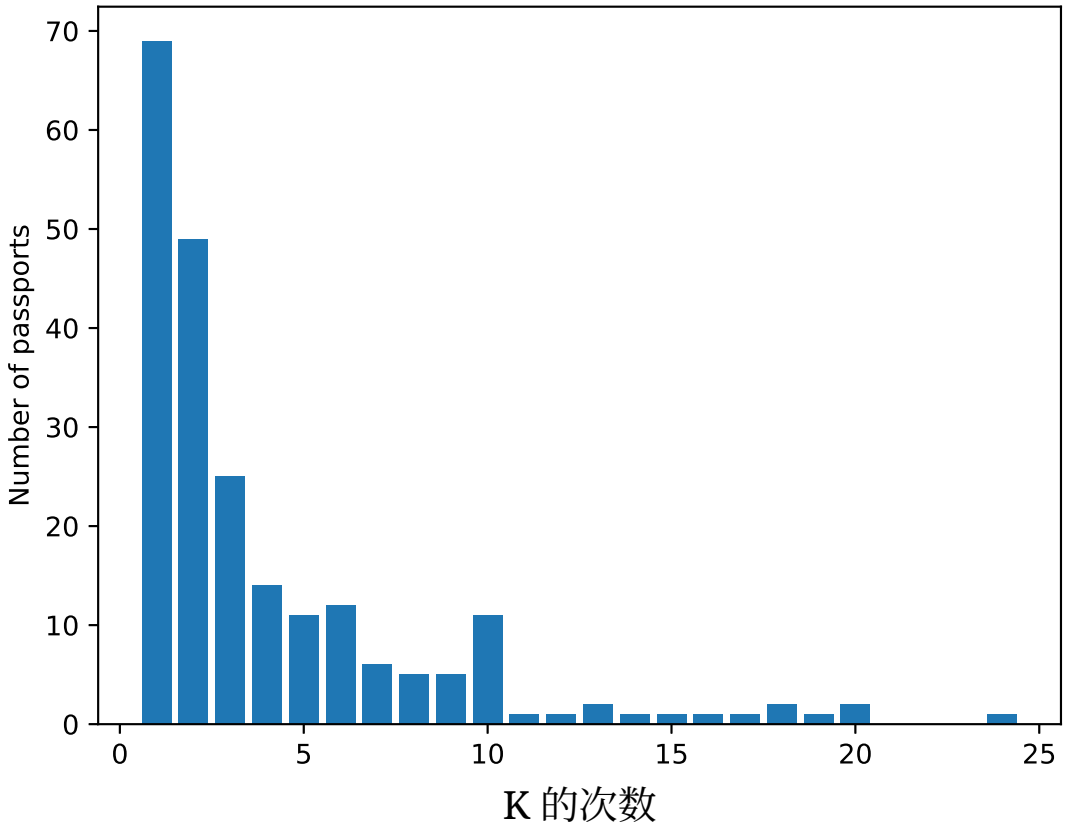


FIGURE 1. 数据库中 K 的次数分布。

$$+ 14896v^5 + 13928v^4 - 2372v^3 + 3970v^2 - 584v + 22\,,$$

其判别式为 $2^{52}3^{15}5^{10}7^{4}13^{4}$，伽罗瓦群为 S_{24}。尽管确实可以使用 [3, 第 5 节1] 的方法来计算更高数域次数下的贝利映射（例如参见 [19]），但计算数量不小的傅里叶系数将变得不可行，这也是这些大型护照未被纳入数据库的原因。为了说明所涉及系数的规模，我们指出，主模函数的第一个非平凡系数以

$$1803514480033338560116570995593169475394856903323733848361806547555555703 7...$$
$$...39589674217818100366320241631582723746983523118064516837 04v^{23} + ...\,,$$

它有 132 位十进制数字，并分解为

$$2^3 \cdot 3^4 \cdot 7^2 \cdot 13^3 \cdot 179 \cdot 1178062360621513$$
$$\cdot 151568799572553565849217592 1 \cdot 157310389634738553599688992620 03$$
$$\cdot 514197500928774955284304452843050396002488377491\,.$$

K 的次数分布见图 1。

5.2. 最多的傅里叶展开项。 数据库中计算出的傅里叶展开系数最多的情形对应于护照 $9\ 1\ 1\ 1\ 0\ 0\ a$，我们列出了 1459 个系数。图 2 给出了傅里叶展开项数量的分布。对于零属子群，我们根据一些启发式估计来选择项数，这些估计取决于 L 的次数，以确保计算

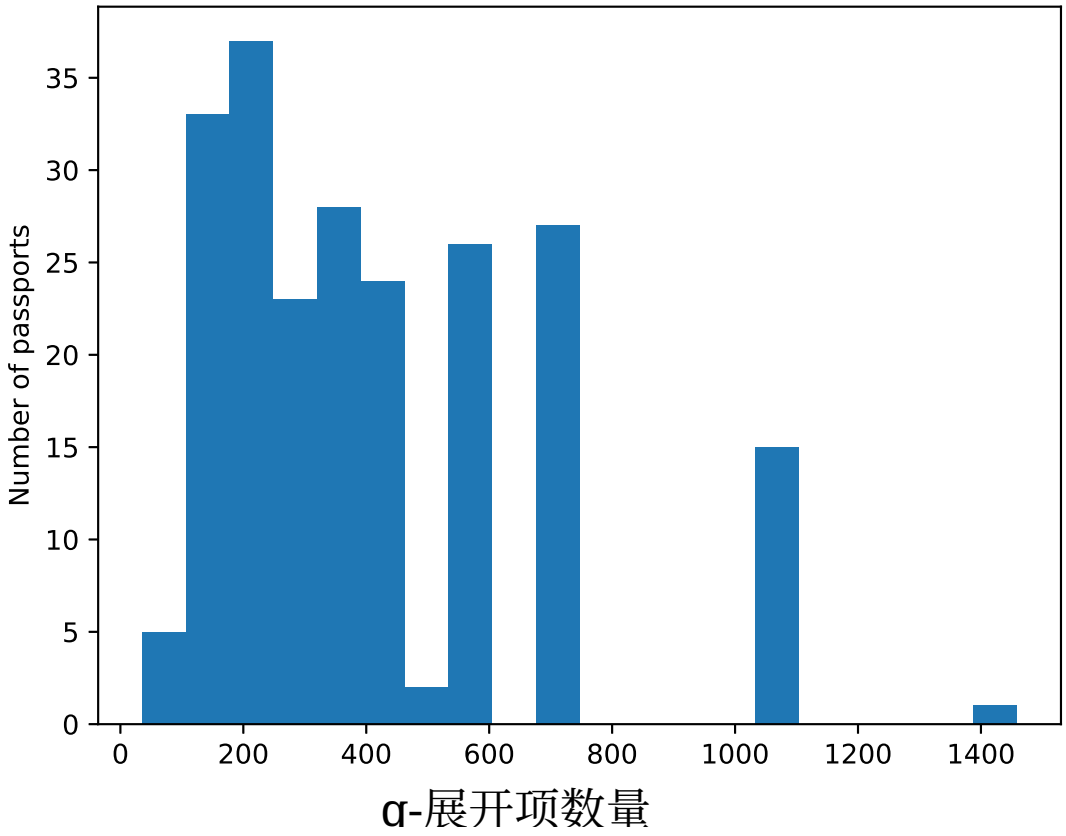


FIGURE 2. 数据库中傅里叶展开项数的分布。

护照标签	椭圆曲线	导子
9_1_1_1_0_0_a	$y^2+xy+y=x^3-x^2-95x-697$	162
10_1_1_0_1_0_a	$y^2+xy+y=x^3+x^2-110x-880$	15
15_1_2_1_0_2_a	$y^2+xy+y=x^3-x^2+7x-103$	270
15_1_2_1_0_3_b	$y^2+xy=x^3-x^2-41370x+2022196$	2970

TABLE 2. 与有理数域 Q 上椭圆曲线对应的非同余子群。

不会持续超过几天。对于高亏格子群，我们纳入了 LLL算法 根据数值近似能够可靠确定的尽可能多的项。对于某些护照，为满足最大 GITHUB 文件大小限制 100MB，我们还不得不减少系数的数量。

5.3. **定义在有理数域 Q 上的椭圆曲线**。表 2 列出了数据库中所有亏格为 1、与有理数域 Q 上的椭圆曲线对应的非同余子群实例，以及它们的定义方程和导子。

REFERENCES

[1] A. O. L. Atkin 和 H. P. F. Swinnerton-Dyer. 非同余子群上的模形式。载于组合学（《纯粹数学专题讨论会论文集》第 *XIX* 卷，加利福尼亚大学洛杉矶分校，洛杉矶，加利福尼亚州，*1968*），第 1–25 页，1971 年。[2] D. Berghaus、H. Monien 和 D. Radchenko. psl(2,zz) 非同余子群的模形式数据库。https://github.com/David-Berghaus/noncong_database，2022 年。 [在线；访问于 10 月 11 日 2022]。

[3] D. Berghaus、H. Monien 和 D. Radchenko. 关于非同余子群上模形式的计算，2022 年。[4] D. Berghaus 和 D. Radchenko. 关于非同余子群上艾森斯坦级数的计算，即将发布。[5] A. J. Best、J. Bober、A. R. Booker、E. Costa、J. E. Cremona、M. Derickx、M. Lee、D. Lowry-Duda、D. Roe、A. V. Sutherland 和 J. Voight. 经典模形式的计算。载于 J. S. Balakrishnan、N. Elkies、B. Hassett、B. Poonen、A. V. Sutherland 和 J. Voight 编，《算术几何、数论与计算》，第 131–213 页，沙姆，2021 年。施普林格国际出版公司。[6] F. Calegari、V. Dimitrov 和 Y. Tang. 无界分母猜想，2021 年。[7] W. Y. Chen. 非同余模曲线的模空间解释。《数学年刊》，371(1-2):41–126，2018 年。[8] H. Cohen 和 F. Str¨omberg.《模形式：一种经典方法》。数学研究生教程 179。美国数学学会，2017 年。[9] J. E. Cremona.《模椭圆曲线的算法》。剑桥大学出版社，剑桥，第二版，1997 年。[10] F. Diamond 和 J. Shurman.《模形式初级教程》。数学研究生教材。施普林格纽约，2006 年。[11] S. Donnelly 和 J. Voight. 希尔伯特模形式数据库。载于 J. S. Balakrishnan、N. Elkies、B. Hassett、B. Poonen、A. V. Sutherland 和 J. Voight 编，《算术几何、数论与计算》，第 365–373 页，沙姆，2021 年。施普林格国际出版公司。[12] L. Fang、J. W. Hoffman、B. Linowitz、A. Rupinski 和 H. Verrill. 非同余子群上的模形式与 Atkin-Swinnerton-Dyer 关系。《实验数学》，19(1):1–27，2010 年。[13] A. Fiori 和 C. Franc. 指标 7 的非同余子群的无界分母猜想。《数论杂志》，2022 年。[14] F. Johansson. Arb：高效的任意精度中点—半径区间算术。《IEEE 计算机汇刊》，66:1281–1292，2017 年。[15] C. A. Kurth 和 L. Long. 关于若干 $SL_2(Z)$ 非同余子群的模形式。《数论杂志》，128(7):1989–2009，2008 年。[16] A. K. Lenstra、H. W. Lenstra, Jr. 和 L. Lov´asz. 有理系数多项式的因式分解。《数学年刊》，261(4):515–534，1982 年。[17] W. Li、T. Liu、L. Long、R. Ramakrishna 等. 非同余模形式与模性。https://aimath.org/pastworkshops/noncongruence.html，2009 年。 [在线；访问于 3 月 22 日 2022]。[18] M. H. Millington.《经典模群的子群》。《伦敦数学会杂志》，s2-1(1):351–357，1969 年 1 月。[19] H. Monien. 偶散群 co3、主模函数与贝利映射，2018 年。[20] M. Musty、S. Schiavone、J. Sijsling 和 J. Voight. 贝利映射数据库。载于《第十三届算法数论研讨会论文集》，Open Book Ser. 第 2 卷，第 375–392 页。Math. Sci. Publ.，伯克利，加利福尼亚州，2019 年。[21] A. J. Scholl. 非同余子群上的模形式。载于 S´eminaire de Th´eorie des Nombres，巴黎 1985–86，Progr. Math. 第 71 卷，第 199–206 页。Birkh¨auser Boston，波士顿，马萨诸塞州，1987 年。[22] W. A. Stein 等. Sage 数学软件（9.2 版）。https://www.sagemath.org/，2021 年。 [在线；访问于 3 月 22 日 2022]。[23]F. Str¨omberg. 非同余子群与 Maass 波形。https://github.com/fredstro/ noncongruence，2018 年。 [在线；访问于 3 月 22 日 2022]。[24] F. Str¨omberg. 非同余子群与 Maass 波形。《数论杂志》，199:436–493，2019 年。[25] S. A. Vidal. 生成有根三价图和有根三角映射的最优算法。《理论计算机科学》，411(31-33):2945–2967，2010 年。[26] D. Zagier. 椭圆模形式及其应用。载于 K. Ranestad 编，《模形式的 1-2-3：挪威诺德菲约尔德暑期学校讲座》，第 1–103 页。施普林格柏林海德堡，柏林，海德堡，2008 年。

Bethe Center, University of Bonn, Nussallee 12, 53115 Bonn, Germany
电子邮件地址：berghaus@th.physik.uni-bonn.de

Bethe Center, University of Bonn, Nussallee 12, 53115 Bonn, Germany
电子邮件地址：hmonien@uni-bonn.de

Laboratoire Paul Painlevé, University of Lille, F-59655 Villeneuve d'Ascq, France电子邮件地址：danradchenko@gmail.com