arXiv:2601.01324v1 [math.NT] 4 Jan 2026

OP同余子群 $\Gamma_0(2^n$ 的 TIMAL 法雷数列)

NHAT MINH DOAN、SANG-HYUN KIM、MONG LUNG LANG 和 SER PEOW TAN

Abstract. 我们证明 $\Gamma_0(2^n)$ $(n \geq 2)$ 存在一个法雷数列 $\{e_i\}$，使得对于所有 e_i，$e_i \leq 2^{n-1}$。上述上界是最优的，并且存在唯一的 j 使得 $e_j = 2^{n-1}$。对于每个 e_i，存在唯一的 a_i，使得 $\{a_i/e_i\} \cup \{\infty\}$ 是 $\Gamma_0(2^n)$ 的一个基本域的理想顶点集，其边配对给出 $\Gamma_0(2^n)$ 的一组独立生成元。

1. Introduction

1.1. **主要结果**。设

$$T = \{0/1 = a_1/e_1, \ldots\ldots, a_m/e_m = 1/1\} \cup \{\infty\} \tag{1.1}$$

为特殊多边形 P（一种特殊类型的基本域）的尖点（理想顶点）有序集，其中该多边形属于 $\Gamma_0(2^n)$ $(n \geq 2)$。P 的边配对给出 $\Gamma_0(2^n)$ 的一个独立生成元集。我们称分母序列 $\{e_i\}$ 为 $\Gamma_0(2^n)$ 的一个法雷数列。受 Kulkarni [Ku], 的研究启发，我们认为，如果精心构造 P，那么 $\{e_i\}$ 将有助于揭示 $\Gamma_0(2^n)$ 的一些有趣且重要的几何性质和算术性质。在本文中，我们证明:

定理 1.1。（定理 *8.1*）P 可以按如下方式构造，使得 $\{e_i\}$ 满足

$$e_i \leq 2^{n-1} \text{ for all } i \text{ and } e_j = 2^{n-1} \text{ for a unique } j. \tag{1.2}$$

对于每个 e_i，都存在唯一的 a_i，使得 $\{a_i/e_i\} \cup \{\infty\}$ 是 $\Gamma_0(2^n)$的一个特殊多边形的尖点集合。

Th这在第 8.1 小节中得以实现。注意，上界 2^{n-1} 是最优的，这证实了了我们的猜想
在此特殊情形下关于 $\Gamma_0(N)$ 的猜想；参见 [DKLT，猜想 3.16]。

1.2. **较弱的结果**。我们的方法有很大一部分适用于 $\Gamma_0(p^n)$，其中 p 是一个奇素数且$n \geq 2$。然而，在构造的最后一部分，我们无法为 $\{e_i\}$得到最优上界。我们能得到的最好结果如下。

定理 1.2.（定理 *10.1*）设 $p > 2$ 为素数且 $n \geq 2$。那么 Γ_0（p^n）有一个 *Farey*序列$\{e_i\}$，满足

$$e_i \leq (f_{p+1}/2)p^{n-1} + f_p p^{n/2} \text{ for all } i, \tag{1.3}$$

其中 f_m 是第 m 个斐波那契数（$f_1 = f_2 = 1$，$f_m = f_{m-1} + f_{m-2}$ 对所有 $m \in \mathbb{Z}$ 均成立）。

1.3. **前人结果**。构造一种特殊类型的基本域 P for$\Gamma_0(N)$（特殊多边形）的想法可以追溯到 Kulkarni 在 [Ku] 中的工作；在这种基本域中，P的尖点序列是 Farey邻项，且边配对给出 $\Gamma_0(N)$ 的独立生成元集。随后，[CLLT] 进一步发展了这一想法，给出了构造算法，消除了原始构造中的试错歧义。其他人已实现了这一算法，例如 [Mag] 和 [Sag]。然而，该算法不一定能给出分母的最优界。对于 $N = p$ 或p^2, p 为素数的情形，[DKLT]构造了具有最优界的特殊多边形，其对应的 Farey数列为 $\{e_i\}$。

2020 *Mathematics Subject Classification.* 20D08.*Key words and phrases.* 同余子群、特殊多边形、Farey序列。

1.4. **Farey数列**。 在 [CLLT], 中，(1.1) 中 T 的（有序）集合被称为 $\Gamma_0(2^n)$ 的 Farey数列。由于 a_i由 e_i唯一确定（见第 2.3 小节），而我们主要关注 e_i的性质，因此没有必要构造序列 $\{a_i/e_i\}$。所以我们只构造序列 $\{e_i\}$。本文将其称为 $\Gamma_0(2^n)$ 的 Farey数列；更一般地，0 与 1 之间一列 Farey邻项的分母集合称为 Farey数列。同样，依照记号滥用，我们也用 F_r 表示阶为 r 的 Farey数列的有序分母序列。一个显而易见的优点是，诸如 (5.1) 和 (5.5) 这样的表达式会更简洁；若采用旧记法则会显得繁杂（每一项都要写成 $(s+vt)/(a+vb_0p^m)$，而不是 $a+vb_0p^m$）。

1.5. **记号**。 令 $\Gamma := PSL(2,\ \mathbb{Z})$ 通过 Möbius 变换在双曲上半平面 $\mathbb{H}$ 上等距作用。顶点集为 $\{\infty, 0, 1\}$ 的理想三角形在 Γ 作用下的平移像称为 ***Farey* 三角形**，无限直线（∞，0）在 Γ 作用下的平移像称为偶数线。偶数线的理想端点是 ***Farey*邻项**。顶点集为 $\{\infty, 0, e^{i\pi/3}\}$ 的三角形在 Γ 作用下的平移像称为 特殊三角形。注意，每个 Farey 三角形包含 3 个特殊三角形。 $\Gamma_0(N)$ 是 Γ 的子群，由所有 (2，1) 项可被 N 整除的矩阵组成。将 $\Sigma(N)$ 的曲面 $\mathbb{H}/\Gamma_0(N)$ 记为 $\Sigma(N)$。注意， $\Sigma(N)$ 由 Farey 三角形和特殊三角形铺砌而成（如果 $\Sigma(N)$ 具有阶为 3 的轨形点）。 x 的尖点在 $\Sigma(N)$ 中的自然领圈记为 $C(x)$，它是由长度为 2 的 horocycle 所界定、围绕 x 的领圈。注意，不同尖点的自然领圈彼此不相交。从 $\mathbb{H}$ 到 $\Sigma(N)$ 的投影映射记为 π。

设 T 如 (1.1) 所示。一对相邻的成员称为一条边。根据构造，相邻项将是 Farey邻项。用我们的新记号，(e_i，e_{i+1}) 是一条边，而 e_i 是一个尖点（顶点）。然而，将 e_i's 替换为数字时，必须谨慎。例如，取 $\Gamma_0(6)$ 的特殊多边形$\{a_i/e_i\}\cup\{\infty\} = \{0/1, 1/3, 1/2, 2/3, 1/1\}\cup\{\infty\}$。按照我们的约定（第1.4小节）， $F = \{1, 3, 2, 3, 1\}$ 是 $\Gamma_0(6)$ 的法雷数列。这些配对 (1，3)、(3，2)、(2，3) 和 (3，1) 是边。我们也采用约定，用 (1，3) $\in F$ 表示 (1，3) 是 F 的一条边，这不应引起混淆。说 3 是一个尖点（顶点）是不正确的，因为它并不唯一。正确的说法是 (1，3) 中的尖点 3，以及 (3,1) 中的尖点 3。这是两个不同的尖点。在需要时，我们仍将用 x/y 表示一个尖点，用 $[x/y]$ 表示其等价类。

设 (a, b) 是法雷数列 $\{e_i\}$ 的一条边。借鉴法雷构造，

$$a \oplus b \text{ denotes the number } a+b \text{ which we insert into } (a, b). \tag{1.4}$$

1.6. **最优法雷数列的构造 $\{e_i\}$，其中 $\Gamma_0(2^n)$**。 这在第6节中实现，其中构造了 $\{e_i\}$。简而言之，$\{e_i\}$ 是如下给出的并集:

$$\{e_i\} = S_1 \cup \{a \oplus b\ :\ a+b = z2^i,\ i > n/2\} \qquad (\text{see } 1.4), \tag{1.5}$$

其中 S_1 是 F_r、 $r = \lfloor 2^{n/2}\rfloor$ 以及若干条称为 N_e 的链的并集（见 (5.5)）。具体而言， F_r 在第2节中给出，链在 (5.5) 中给出，而 $T\setminus S_1$ 在 (6.1) 中给出。在第4节中，我们构造了一个 Γ_0 (64) 的法雷数列，并说明如何以类似方式处理一般情形。我们约定， $\{e_i\}$ 中的元素按照由 (1.4) 中的运算所产生的法雷构造进行排序（另见第 2.2 小节）。

1.7. **法雷数列的上界（适用于 $N = 2^n$）**。 F_r 顶点的一个上界是$r := \lfloor 2^{n/2}\rfloor$，这基本上是根据定义得出的（见第2节）。 S_1 顶点的一个上界是 2^{n-1}（见引理 7.1）。 $T\setminus S_1$ 顶点的一个上界同样是 2^{n-1} （见定理 8.1）。

1.8. **几何讨论**。我们在此对构造给出一种几何解释，这或许对更偏好几何的读者有所帮助。回想一下，我们希望为曲面 $\Sigma(N) := \mathbb{H}^2/\Gamma_0(N)$构造一种特殊类型的基本域。在我们早先关于 $\Sigma(N)$的最优特殊多边形的研究[DKLT] 中，其中 $N = p$ 或 p^2 (p 素数)，第一个重要观察是，可以选取一个特殊多边形，使其包含顶点为F_r的理想多边形，其中 $r := \lfloor\sqrt{N}\rfloor$。这一点在我们的情形下仍然成立，也是构造的第一步。所用的第二个重要事实是，只需添加彼此孤立的法雷三角形或特殊三角形，就能补全特殊多边形。但在这里情况不再如此（$N = p^n, n > 2$）。主要区别在于，一般而言， $\Sigma(N)$具有中间宽度的尖点（见第3.3节），而对于 $N = p$ 或 p^2，尖点的宽度则只有最小或最大值（1或 N）。回想一下， $\Sigma(N)$的尖点对应于 $\Gamma_0(N)$-轨道中的 $x/y \in \mathbb{Q} \cup \{\infty\}$，且尖点的自然领圈彼此不相交。若 $\Sigma(N)$的两个尖点（不一定互不相同）由一条偶线连接，就称它们为 ***Farey*相邻**。我们将证明结果所需的步骤和观察总结如下（见第3.3小节中的(2)、(3)和(4)）：

(1) 我们可以从 F_r 开始构造 $\Sigma(p^n)$ 的法雷数列 $\{e_i\}$；(2) 尖点 $[0/1]$ 是宽度最大的唯一尖点，并且它与所有尖点（包括自身）Farey相邻；(3) 最小或中间宽度的尖点 $[x/y]$ 仅与尖点 $[0/1]$ Farey相邻；(4) 每个中间宽度尖点的领圈邻域已由 F_r 部分填充。也就是说，尖点集为 F_r 的理想多边形在 $\Sigma(N)$ 上的投影 π 与所有中间宽度尖点的领圈相交；(5) 有一种系统的方法，通过依次插入法雷三角形来填充 $C(x)$ 中间宽度尖点 x 的领圈，同时将分母限制在 p^{n-1} 以内，从而得到 F_r。具体做法是将链 N_ϵ 附加到 F_r，以获得 S_1 （构造 S_1 见第5节，界限见第7节）；(6) 最后，通过填充领圈 $C([0/1])$ 完成构造。在此过程中，根据上述(3)，所有其他尖点也会被填充，于是我们得到 $\Gamma_0(p^n)$ 的法雷数列；(7) 在 $p = 2$ 的情况下，最后一步只需填充孤立的法雷三角形，其分母仍受限于 2^{n-1}。若 $p \neq 2$，则可能需要填充包含至多 $2p - 2$ 个法雷三角形片的块。这就得到了定理 1.2 中的界限。

注记： 在本文中，当我们考虑 $\Gamma_0(p^n)$ 时， $n \geq 3$ 除非另有说明。

致谢。 Nhat Minh Doan 获得新加坡国家研究基金会（NRF）E-146-00-0029-01 项目资助。Sang-hyun Kim 获得韩国政府资助的国家研究基金会通过中坚研究者计划（RS-2023-00278510）提供的支持。Ser Peow Tan 获得新加坡国立大学学术研究项目 A-8000989-00-00 的资助。

2. Constructing Farey sequences

2.1. **法雷数列** F_r。 令 $N > 3$ 且 $r = \lfloor\sqrt{N}\rfloor$。我们主要关注这样的情形：$N = p^n$ 其中 p 是素数（特别是，当 $p = 2$ 时）且 $n \geq 3$。令 F_r 为阶数为 r 的法雷数列中分母的有序序列（分母为 $\leq r$ 的 0 与 1 之间的有理数）。 F_r 中的元素按照法雷数列的***Farey* 构造排序**（见第 2.2 小节）。具体而言， F_r 可按如下方式归纳构造：

(i) 设 $D_1 = \{1, 1\}.$。配对 (1，1) 称为 D_1 的一条边。(ii) 将 $1+1 = 2$ 插入 D_1。由此得到 $D_2 = \{1, 2, 1\}$。相邻对 (1，2) 和 (2，1) 是 D_2 的边。注意，(1，1) 不再是 D_2 的一条边。

(iii) 对于 $k \geq 2$，设 $(a,\ b)$ 是 D_k 的一条边，且 $a+b \leq r$。将 $a+b$ 插入 $(a,\ b)$。由此得到 $D_{k+1} = \{\ldots, a, a+b, b, \ldots\}$。注意，$(a,\ b)$ 不再是 D_{k+1} 的一条边。例如，假设在 D_2 中，$(a,\ b) = (1,\ 2)$。那么 $D_3 = \{1, 3, 2, 1\}$。(iv) 这个过程将在序列 $D_q := F_r$ 中终止；此时，对于 D_q 的所有边 $(a,\ b)$，均有 $a+b > r$。

2.2. **的法雷数列**N。第 2.1 小节中的算法可视为构造 $\Gamma_0(N)$ 的法雷数列（因此也是特殊多边形）的第一步。事实上，若将上述算法中的 (iii) 替换为

(iii′) 对于 $k \geq 2$，取 (a, b) 为 D_k 的一条边，使得 a^2+b^2 和 a^2+ab+b^2 都不是 N 的倍数；对于 D_k 的每条边 (x, y)，$ax+by$ 都不是 N 的倍数；并且在满足这些性质的边 (a, b) 中，$a+b$ 取最小值。将 $a+b$ 插入 (a, b)。由此得到 $D_{k+1} = \{\ldots, a, a+b, b, \ldots\}$。

于是，使用 (i)、(ii) 和 (iii′) 的算法经过有限步后会终止，得到法雷数列 $\{e_i\} := D_s$，对应于 $\Gamma_0(N)$；这是因为 $\Gamma_0(N)$ 在模群 Γ 中具有有限指标（见 [CLLT]）。我们将此算法称为 $(CLLT)$。

DKLT 的首个关键观察是，序列 F_r $(r = \lfloor\sqrt{N}\rfloor)$ 总会作为算法中的中间序列出现，因此实际上，我们可以从序列 F_r 而非 D_1 开始算法，也就是说，将 (i) 替换为 (i′) Set $D_1 = F_r$（第 1.8 节中的步骤 1）。这是由 (iii′) 的极小性条件得出的。事实上，这个极小性条件并非必要；CLLT 中并未采用该条件，即使去掉它，仍然可以得到 $\Gamma_0(N)$ 的法雷数列。

可以根据该序列和配对数据构造带有边配对的特殊多边形。我们先给出一个定义：

定义 2.1。满足 a^2+b^2 是 N 的倍数的 D_s 的边 (a, b) 称为偶边；满足 a^2+ab+b^2 是 N 的倍数的边称为奇数边。偶边和奇数边统称为椭圆边，因为相应的边配对是椭圆型的。满足 $ax+by$ 是 N 的倍数的 D_s 的两条边 (a, b) 和 (x, y) 称为配对边。对于中间序列 D_r，其中 $r < s$，D_r 中未配对的非椭圆边称为自由边。

注： 对于给定的 N，椭圆边的定义适用于任意偶数线的分母；类似地，对于互素整数 a，b 和 x，y，可以讨论 $(a,\ b)$ 与 $(x,\ y)$ 的配对，这对应于一对偶数线的分母。

当过程在 D_s 处终止时，所有边要么是椭圆边，要么已配对，因为没有更多自由边可供插入。存在唯一的理想多边形 P（见第 2.3 小节和注 3.2），其分母序列由 D_s 给出。

2.3. **分数与法雷数列的 Farey 构造**。设 $A_1 = \{0/1, 1/1\}$。$A_1 \cup \{\infty\}$ 是 Farey 三角形的顶点。按照 [CLLT] 中给出的 Farey 构造，从 A_k 出发，通过插入 a/b 与 c/d 的 Farey 和（见 (2.1)）得到 A_{k+1}，其中 $e = (a/b,\ c/d)$ 是 A_k 的一条自由边。注意，A_k 的自由边是指一条非椭圆边，且它未与 A_k 的任何非椭圆边配对。a/b 与 c/d 的 Farey 和定义如下：

$$\frac{a}{b} \oplus \frac{c}{d} = \frac{a+c}{b+d}. \tag{2.1}$$

容易看出，D_1 是第2.1小节中 A_1 的分母；一般而言，D_k 是 A_k的分母集合。以下示例最能说明这一点。

$$A_2 = \{0/1, 1/2, 1/1\},\ D_2 = \{1, 2, 1\},\ A_3 = \{0/1, 1/3, 1/2, 1/1\} \text{ and } D_3 = \{1, 3, 2, 1\}.$$

插入一个 Farey 和等价于附加一个 Farey 三角形。因此， D_k 是一个理想多边形顶点的分母有序集合，该理想多边形由 Farey 三角形组成。以这种方式归纳地得到的数列D_k ，若对插入没有任何限制，则称为法雷数列。以下结论成立（(ii) 和 (iii) 见 [CLLT] ）。

(i) A_k 唯一确定一个法雷数列 D_k ，反之亦然。(ii) 若 $e=(c/a,\ d/b)$ 和 $f=(w/x,\ z/y)$ 是 A_k 的边，且 e 和 f 由 Γ中的元素 M配对，则 M的 (2,1) 项是 N的倍数，因此 $M\in\Gamma_0(N)$。注意， M 的 (2,1) 项是 $ax+by$。(iii) 若 $e=(c/a,\ d/b)$ 是椭圆型，则 e由 $\Gamma_0(N)$中的椭圆型元素 M与自身配对，且该元素的 (2,1) 项是 N的倍数。注意， M的 (2,1) 项为 a^2+b^2或 a^2+ab+b^2。在前一种情况下，该边被视为两条互相配对的半无限边；在后一种情况下，在该边上附加一个特殊三角形，并将由此产生的半无限边互相配对。

3. Farey sequences of $\Gamma_0(p^n)$ and cusps of $\Sigma(p^n)$

3.1. ()的法雷数列。第 2.2 小节中的构造最终得到一个法雷数列 D_s ，适用于 $\Gamma_0(p^n)$（当 $N=p^n$时），并具有以下性质：

(i) D_s 有 $1+\lfloor[\Gamma:\ \Gamma_0(p^n)]/3\rfloor$ 个成员（由指数 $[\Gamma:\ \Gamma_0(p^n)]$可得）。(ii) 对于 D_s的每一条非椭圆边 $s=(a,\ b)$，存在唯一一条 D_s的边 $s^*=(x,\ y)$，使得 s 与 s^* 配对，也就是说， $ax+by$ 是 p^n的倍数。（参见 [Ku] 和 [CLLT]）。

定义 3.1。称法雷数列 F 为 $\Gamma_0(p^n)$ 的法雷数列，如果 $F_r\subseteq F$ 和 F 满足上述 *(i)* 和 *(ii)*。称法雷数列 S 为 $\Gamma_0(p^n)$ 的子数列，如果 $F_r\subseteq S$，并且 S 是 $\Gamma_0(p^n)$的法雷数列 F 的子数列。

根据定义，利用 Farey 构造，可以将 Farey 子序列 S 扩展为 $\Gamma_0(p^n)$ 的法雷数列 F 。此外，在第 2.2 小节中使用 (i′)、(ii)、(iii′) 的算法所得到的中间序列 D_r （其中 $r<s$ ）也是 $\Gamma_0(p^n)$ 的 Farey 子序列。

注 3.2. 序列 $D_s=\{e_i\}$ 确定了 $\Gamma_0(p^n)$ 的一个特殊多边形（参见第 1.3 小节和第 2.3 小节）。对于每个 e_i，都存在唯一的 a_i ，使得 $\{a_i/e_i\}$ 是 $\Gamma_0(p^n)$ 的某个特殊多边形（基本域）的尖点集合。特殊三角形附着在理想多边形的奇数边上，这些边在有限顶点处相交并配对。一条偶数边通过绕其上平移后的 $\sqrt{-1}$ 进行 π 旋转而与自身配对。配对边的两侧彼此配对。

注 3.3. 第 2.2 小节的算法将 $a+b$ 插入到 $\Gamma_0(p^n)$ 的 Farey 子序列的一条自由边 $s=(a,\ b)$ 上，并选择使 $a+b$ 在所有可能的自由边中最小的那条，从而得到 $\Gamma_0(p^n)$ 的一个新 Farey 子序列。该过程经过有限步后会终止，得到 $\Gamma_0(p^n)$ 的一个 Farey 数列，因为指数 $[\Gamma:\ \Gamma_0(p^n)]<\infty$。如果不加入 $a+b$为最小值这一条件，该过程仍会终止于 $\Gamma_0(p^n)$ 的一个 Farey 数列（可能不同）。

3.2. 法雷数列 $F_{[\sqrt{8}]}$ 和 $F_{\sqrt{16}}$ 以及 $\Gamma_0(8)$ 和$-\Gamma_0(16)$。容易看出， $F_{[\sqrt{8}]}=\{1,2,1\}$ 和 $F_{\sqrt{16}}=\{1,4,3,2,3,4,1\}$.。此外，简单验证可知，以下分别是 $\Gamma_0(8)$ 和 $\Gamma_0(16)$ 的法雷数列：

$$\{1,4,3,2,1\},\ \{1,4,3,8,5,2,3,4,1\}. \tag{3.1}$$

3.3. () 的尖点。 回顾一下，一般而言， $\Sigma(N) := \mathbb{H}/\Gamma_0(N)$ 有 $\sum_{d|N} \phi(\gcd((d,\ N/d))$ 个不等价尖点。这些尖点对应于 $\Gamma_0(N)$ 在 $\mathbb{Q} \cup \{\infty\}$ 上的作用轨道，因此我们也用等价类 $[x/y]$ 表示 $\Sigma(N)$ 的一个尖点。尖点的一个重要不变量是：

定义 3.2. 设 $[x/y]$ 是 $\Sigma(N)$ 的一个尖点，且设 $A \in PSL(2,\mathbb{Z})$ 是一个将 ∞ 映到 x/y 的矩阵。 $[x/y]$ 的宽度是满足下式的最小正整数 $w := w([x/y])$

$$A \begin{pmatrix} 1 & w \\ 0 & 1 \end{pmatrix} A^{-1} \in \Gamma_0(N). \tag{3.2}$$

几何上， $w([x/y])$ 是与领圈 $C([x/y])$ 相交的偶数线的数量。注意， $w([\infty]) = 1$。我们用记号 $w(x/y)$ 简记 $w([x/y])$。关于 $\Sigma(N)$ 的尖点，以下事实将会有用（见 [Sh] 第 25 页）：

引理 3.3. 考虑 $\Gamma_0(N)$ 及其对应的曲面 $\Sigma(N)$。

(a) 对于 N 的每个正因子 d ，当且仅当 $x - y$ 是 $gcd(d, N/d)$ 的倍数时， x/d 和 y/d （既约形式）彼此等价。(b) x/y （既约形式）等价于某个 x' 对应的 $x'/gcd\,(y, N)$。

此外，如果 $N = p^n$，则有：

引理 3.4. 考虑 $\Gamma_0(p^n)$ 及其对应的曲面 $\Sigma(p^n)$，其中 p 是素数。设 $x = a/bp^i$（为既约形式），其中最大公因数 $(ab, p) = 1$，且 $0 \le i \le n$。

(i) 若 $i \ge n/2$ ，则 $w(x) = 1$ ；若 $i \le n/2$，则 $w(x) = p^{n-2i}$ 。特别地，当且仅当 $[x] = [0/1]$ 时， $w(x) = p^n$ 。宽度为 p^{n-2i} 且满足 $0 < i < n/2$ 的尖点称为中间宽度尖点。*(ii)* 按照 F_r 的构造（见第 *2.1* 小节），并由引理 *3.3(b)* 可知，若 $i \le n/2$，则 $x = a/bp^i$ 等价于 F_r 的一个顶点。*(iii)* 每个尖点 $[x/y] \ne [0/1]$ 仅与 $[0/1]$ *Farey*相邻；反过来， $[0/1]$ 与所有尖点 *Farey* 相邻。*(iv)* 假设 $[x_1] = [1/1], [x_2] = [1/2], \ldots, [x_{p^n}] = [1/p^n]$ 是按循环顺序与 $[0/1]$ *Farey*相邻的尖点，则 $[x_i]$ 具有中间宽度或最小宽度，当且仅当 p 整除 i。此外，如果 x_i 的宽度为 *1* 且 $n \ge 3$，那么 $w(x_{i-p}) > 1$ ，且 $w(x_{i+p}) > 1$。*(v)* 假设 $N = 2^n \ge 4$。设 $c = x/y2^{n-1}$，其中最大公因数 $(xy, 2) = 1.$ 。由上可知， c 的宽度为 *1*，且 $\Sigma(2^n)$ 有唯一一个这种形式的尖点。

4. $\Gamma_0(64)$ 和 $\Gamma_0(2n)$ 的法雷数列)

我们构造了一个 $\Gamma_0(64)$的法雷数列，并说明可以用同样的方法构造 $\Gamma_0(2^n)$的法雷数列（见第 4.5 小节）。希望这种非正式的处理能让我们在第5节和第6.1小节中的阐述更加通俗易读。因此，可以肯定地说， $\Gamma_0(64)$情形至关重要（另见猜想 10.1）。首先注意到

$$F_{\sqrt{64}} = F_8 = \{1, 8, 7, 6, 5, 4, 7, 3, 8, 5, 7, 2, 7, 5, 8, 3, 7, 4, 5, 6, 7, 8, 1\}. \tag{4.1}$$

4.1. 第一个观察。 边 (1，8) 与 (8，7) 配对。一般而言，若 $N = p^{2m}$， F_r 的边 $(a,\ p^m)$ 与 $F_r\,(r = m)$ 的边 $(p^m,\ p^m - a)$ 配对。

4.2. 构造链。 现在来看边 $e_1 = (7,6)$。注意，第二个数是 2 的倍数。可以验证 (7,6) 是自由的，我们可以在 $(7, 6)$ 中插入尖点。每一步中，只要可行，我们就在 6 旁边插入一个尖点。由此得到以下链：

$$\{7, 13, 6\},\ P = \{7, 13, 19, 6\},\ N' = \{7, 7+6, 7+2\cdot 6, 7+3\cdot 6, 6\} = \{7, 13, 19, 25, 6\}. \tag{4.2}$$

链在 N' 处停止，因为 (25, 6) 与 (6, 7) 配对 $\in F_{\sqrt{64}}$（这里 $25\cdot 6+6\cdot 7=192$ 是 64 的倍数）。N' 的最大成员是 25，这相当大，但仍小于 $2^5=32$。我们也可以从另一侧由右向左部分填充，并以平衡的方式进行，从而减小最大元素。这里我们将链 N' 替换为

$$\{7,13,19,6\}\cup\{6,13,7\}, \tag{4.3}$$

其中 (19,6) 与 (6,13) 配对。

一般而言，对于 $N=p^n$，在 F_r 的自由边上处理形如 $e=(a,bp^m)$ 的边，并首先构造链

$$N'_e=\{a,a+bp^m,a+2bp^m,\dots,a+vbp^m,bp^m\} \tag{4.4}$$

其中 v 是使 $(a+vbp^n,bp^m)$ 与 F_r 的某条边 (x,y) 配对的最小正整数。由于尖点宽度有限，这样的整数总是存在。事实上，v 的一个直接上界是 $w-1$，其中 w 是尖点宽度。我们在小节 7.1 中证明 $a+vbp^m<p^{n-1}$。

随后可将其替换为更优的链

$$N_e=\{a,a+bp^m,a+2bp^m,\dots,a+v_1bp^m,bp^m\}\cup\{x,v_2x+y,\dots,2x+y,x+y,y\} \tag{4.5}$$

其中，若 v 为偶数，则为 $v_1=v_2$；若 v 为奇数，则为 $v_1=v_2+1$。边 $(a+v_1bp^m,bp^m)$ 与 (x,v_2x+y) 配对。

几何上，我们通过向对应于 F_r 的部分基本域添加法雷三角形，填补中间宽度尖点环带中的间隙。每个间隙都对应 F_r 的形如 $e=(a,\ bp^m)$ 和 $e=(xp^m,\ y)$ 的自由边，它们是该间隙的左右边界。因此，在添加了所有链之后，我们就填补了中间宽度尖点环带中的所有间隙。还需注意，根据引理 3.4(iii)，链 N_e 的填补彼此独立。我们以均衡的方式填补间隙，以减小所得分母的大小；这对于得到 $\Gamma_0(2^n)$的最优界至关重要。

4.3. 法雷序列 S_1 和 T。 令 S_1 为 $F_{\sqrt{64}}$ 与 N_{e_i} 的并集，其中 $e_i\in\{e_1=(7,\ 6)\ e_2=(5,\ 4)\ e_3=(7,\ 2)\ e_4=(7,\ 4)\ e_5=(5,\ 6)\}$（当 b 为偶数时，F_8 的自由边 $(a,\ b)$）。在这里，我们将链的中间尖点插入 F_r 的对应边中。注意，

$N_{e_2}=\{5,9,4\}\cup\{4,7\}$，$N_{e_3}=\{7,9,2\}\cup\{6,5\}$，$N_{e_4}=\{7,11,4\}\cup\{4,5\}$，$N_{e_5}=\{5,11,6\}\cup\{2,7\}$，其中 (9，4) 与 (4，7) 配对，(9，2) 与 (6，5) 配对，(11，4) 与 (4，5) 配对，(11，6) 与 (2，7) 配对。简而言之，

$$S_1=\{1,8,7,13,19,6,5,9,4,7,3,8,5,7,9,2,7,5,8,3,7,11,4,5,11,6,13,7,8,1\}. \tag{4.6}$$

一般而言，S_1 是 F_r 与所有 N_e的并集（将 N_e的中间尖点插入到 F_r对应的边中），其中 e 是一条自由边，其形式为 $(a,\ bp^m)$，$m\geq 1$。详情请见第5节。

4.4. 的边的（非）自由性。 注意，S_1 中形式为 $(a,\ b)$ 且 ab 是2的倍数的所有边都不是自由边。换言之，对于 S_1的任意自由边 $(a,\ b)$，2都不整除 ab。这由第4.1小节以及第4.2小节的几何解释可知。现在我们考察式 (4.4) 中给出的 N_{e_1} 里的边 (7，13)。这不是一条自由边。下面我们将给出两个证明来说明这一点：一个较差的证明，以及一个能提供一些见解的较好证明。

(B) 一个错误证明。 (7，13) 不是自由的，因为它与 (7，11) 配对 $\in S_1$。

(G) 正确证明。 假设 (7，13) 是自由的。我们可以将 $7+13=20$ 插入 (7，13) 中。然而，20 对应于一个中间宽度为 $w=2^{6-4}=4$ 的尖点（引理3.4(i)），但所有中间宽度的尖点都已由 S_1 填入，这就产生了矛盾。

根据同样的推理，如果 $(a,\ b)$ 是 S_1 的一条边，使得 $a+b=z2^i$、z 为奇数，$i<6/2$，那么 $(a,\ b)$ 不是一条自由边。剩下的（自由）边只有

$$(13,19)\in N_{e_1},\,(7,9))\in N_{e_3},\,(5,11))\in N_{e_5}.$$

注意，$13+19$、$7+9$、$5+11$ 是 $\sqrt{64}$的倍数，并且(13，32) 与 (32，19) 配对，(7，16) 与 (16，9) 配对，(5，16) 与 (16，11) 配对。插入$13\oplus 19$、$7\oplus 9$、$5\oplus 11$后，就没有更多自由边了。因此

$$T=S_1\cup\{13\oplus 19,7\oplus 9,5\oplus 11\} \tag{4.7}$$

没有自由边。
符号约定见第1.4小节。因此，T 是 Γ_0(64)的法雷数列。

4.5. 一般情形。令 S_1 为 F_r 与所有 N_e的并集，其中 e是形如（a，$b2^m$）$m\geq 1$的自由边。如前所述，S_1 中形如（a，$b2^m$）或（$x2^p$，y）（bx 为奇数）的边不是自由边，而 S_1 中可能的自由边只能形如（a，b），其中 a和 b 都是奇数。与 Γ_0(64)情形类似，若（a，b）是一条满足 $a+b=z2^i$的边，其中 $i<n/2$（z 为奇数），则（a，b）不是自由边。在 $a+b=z2^i$、$i\geq n/2$ 的情形下，同样与 Γ_0(64)情形类似，（a，$a+b$）与（$a+b$，b）配对。总之，

$$T=S_1\cup\{a\oplus b:\,a+b=z2^i,i\geq n/2\}\text{ has no free sides.} \tag{4.8}$$

因此，T 是 $\Gamma_0(2^n)$的法雷数列。详情见第6.1小节，界限见第7.2小节。

5. The Farey sequence S_1

本节的主题是证明，由 F_r 构造的法雷数列 S_1 是 $\Sigma(p^n)$的 Farey 子序列，正如第4.3小节所述。我们考虑 $N=p^n$、p 素数、$n\geq 3$和 $r=\lfloor\sqrt{N}\rfloor$，因为这适用于一般的素数 p。

5.1. **链** N_e。设 $e=(a,\ b_0p^m)=(a,\ b)$ 是 F_r的一条自由边，其中 a和 b_0分别与 p 和 $m\geq 1$互素。考虑这条链

$$\{a,a+b_0p^m,a+2b_0p^m,\ldots,a+vb_0p^m,\ldots,b_0p^m\}. \tag{5.1}$$

由于 $w(b_0p^m)=p^{n-2m}$ (引理3.4(i))，存在最小的 $0<v<p^{n-2m}$，使得 $(a+vb_0p^m,\ b_0p^m)$ 与 F_r的一条边 $(x,\ y)$ 配对。等价地，

$$(a+vb_0p^m)x+b_0p^my=kp^n. \tag{5.2}$$

回顾一下，$b=b_0p^m$。因此，(5.2) 可写成以下更简单的形式

$$(a+vb)x+by=kp^n. \tag{5.3}$$

注意，x 必须具有 x_0p^m的形式，其中 x_0 与 p互素。令 $v=v_1+v_2$，当v 为偶数时 $v_1=v_2$，当 v 为奇数时 $v_1=v_2+1$。方程 (5.3) 可写为

$$(a+v_1b)x+b(y+v_2x)=kp^n. \tag{5.4}$$

Equ式 (5.4) 对我们更有用，因为它给出了更小的顶点（$a+v_1b<a+vb$）。因此我们将 u se (5.4) 并将 (5.1) 替换为

$$N_e=\{a,a+b,a+2b,\ldots,a+v_1b,b\}\cup\{x,y+v_2x,\ldots,y+x,y\}, \tag{5.5}$$

其中 $(a+v_1b,b)$ 与 $(x,y+v_2x)$ 配对。这给出：

引理 5.1。对于上述的自由边 $e=(a,b_0p^m)$，N_e中的内部顶点的形式为 $a+k_1b$ 或 $y+k_2x$，其中 $k_i\leq v_i$、$v_1+v_2\leq p^{n-m/2}-1$，且当 v_1+v_2 为偶数时 $v_1=v_2$，否则为 $v_1=v_2+1$。

命题 5.2。 同余子群 $\Gamma_0(p^n)$ 拥有一个 ***Farey*** 子序列 S_1，满足(i) $S_1 = F_r \cup N_e$，其中 N_e 是引理 ***5.1*** 中给出的自由边 $e = (a, b_0p^m)$ 的链（此并集表示通过 ***(1.4)*** 将 N_e 的内部顶点插入 F_r）。(ii) S_1 所有自由边 (σ, τ) 的顶点都与 p 互素。

证明。 (i) 设 $E = \{e_1, e_2, \dots, e_k\}$ 是 F_r 的自由边集合，其中的边如引理 5.1 所述，具有 (a, b_0p^m) 的形式。我们可以自由地将 N_{e_1} 插入 F_r。根据构造， $L_1 = F_r \cup N_{e_1}$ 是 $\Gamma_0(p^n)$ 的一个法雷数列的子序列，因为在添加链 N_{e_1} 时，我们只向自由边中插入。这里的关键观察是，插入链 N_{e_1} 时，除了一对边 $(a + v_1b, b)$ 和 $(x, v_2y + x)$ 外，其他引入的边都具有 (u, v) 的形式，其中 p 不整除 uv。这些边无法与 E 中剩余的自由边配对，因为 e_j 只能与具有 (xp^m, y) 形式的边配对。因此， $e_2, \dots, e_k$ 仍然是自由的。接着，我们考察 F_r 的第二条自由边 $e_2 \in E$（它在 L_1 中是自由的），其形式为 (c, dp^m)（对应的 m 可能与 e_1 的不同），并将 N_{e_2} 插入 L_1。根据同样的观察，插入 N_{e_1} 时引入的 (u, v) 形式的边不会影响 N_{e_2} 的插入。再次根据同样的观察， $e_3, \dots, e_k$ 在 L_2 中仍然是自由的。我们继续这一构造，得到法雷数列 $S_1 = F_r \cup \bigcup_{e_i \in E} N_{e_i}$。于是，根据构造， S_1 是 $\Gamma_0(p^n)$ 的一个法雷数列的子序列。

(ii) 根据构造， S_1 不再具有形如（a, bp^m）的自由边。类似地，S_1 也不含形如（xp^m, y）的自由边，因为当我们尝试通过依次在以 xp^m 为左顶点的边上插入元素，将 Farey 子序列扩展为$\Gamma_0(p^n)$ 的 Farey 数列时，这意味着必须包含形如（a, bp^m）的自由边。因此， S_1 的任何自由边都具有所需的形式。□

5.2. **填充链的几何意义**。 注意，根据引理3.4(i)和(ii)，如果 x 等价于一个形如 a/bp^i 且满足 $gcd(ab, p) = 1$和 $i \le n/2$的尖点，那么 F_r 到 $\Sigma(p^n)$的投影与 $C(x)$相交。 $C(x)$中不在像内的间隙，左侧由形如（a, b_0p^m）的 F_r 自由边界定，右侧由形如（x_0p^m, y）的自由边界定；插入链 N_e 对应于通过向 F_r插入法雷三角形来填充这些间隙。根据引理 3.4(iii)，每个插入的三角形只有一个顶点位于中间宽度尖点的领圈内，另外两个顶点则位于 $[0/1]$的领圈内； $[0/1]$是宽度最大的唯一尖点。因此，在中间宽度尖点处填充每个间隙不会影响这些尖点的其余间隙，各条链可以彼此独立地添加。注意，在 S_1 到$\Sigma(p^n)$的投影中，与 a/bp^i、 $i \le n/2$等价的尖点的领圈内不再有间隙。

6. Farey sequence $\{e_i\}$ of $\Gamma_0(p^n)$

6.1. **情形** $p = 2$。 **</style}设 如命题 5.2 所述，且 (,** b) 是 S_1的一条自由边。按照我们的构造， a 和 b 都与 $p = 2$ 互素（见命题 5.2 的 (ii)）。因此，$a + b = 2^i z$ 为偶数（z 为奇数）。由于所有与 $2^m z$ 等价的尖点都已通过 S_1的投影填入 $m \le n/2$中，故 $i > n/2$。由此，$(a, a + b)$ 与 $(a + b, b)$ 互相配对。总之，

$$T = S_1 \cup \{a \oplus b : a + b = z2^i, i > n/2\} \text{ has no free sides.} \tag{6.1}$$

因此， T 是 $\Gamma_0(2^n)$ 的法雷数列。

6.2. **一般情形**。 在这里，仅将 Farey 三角形插入 S_1 的每条自由边，可能不足以得到 T。一般而言，需要将法雷三角形块插入这些自由边。详情见附录 11。

7. Upper bounds

7.1. 中顶点的上界 N_e。设 $(a,b) = (a, b_0p^m) \in F_r$ 是一条自由边，其中 ab_0 与 p 互素，且 $1 \le m \le n/2$。那么 $m < n/2$，因为对于 $m = n/2$，端点处对应的分母为 b_0p^m 的尖点宽度为 1，且它的两条关联边已在 F_r 内配对，因此它们都不可能是自由边。令 $X = b$ 和 $Y = p^{n-m} - a > 0$ ($a \le p^{n/2}$, $m < n/2$)。那么$aX + bY = b_0p^n$。令 $\gcd(X,Y) = d$。由于 Y 与 p 互素， d 是 b_0 的因数。特别地，$b_0/d \in \mathbb{N}$。我们考虑

$$a(X/d) + b(Y/d) = (b_0/d)p^n. \tag{7.1}$$

这意味着 F_r 的自由边（a, b）与（X/d, Y/d）配对。由于 $X/d = b/d < p^{n/2}$ 且 $\gcd(X/d,\ Y/d) = 1$, 必有 $Y/d > p^{n/2}$（否则，（X/d, Y/d）$\in F_r$，这与（a, b）是自由边这一事实矛盾）。由于 $X/d = b/d < p^{n/2}$，存在唯一的 $w \in \mathbb{N}$ 使得

$$0 < Y/d - w(X/d) \le p^{n/2} < Y/d - (w-1)(X/d). \tag{7.2}$$

这意味着

$$(X/d, Y/d - wX/d) \in F_r \text{ and } (a+wb)(X/d) + b(Y/d - wX/d) = (b_0/d)p^n. \tag{7.3}$$

回忆一下， $w > 0$。由（7.3）以及 $X = b = b_0p^m$ 这一事实可得

$$a + wb = p^{n-m} - (Y - wX) < p^{n-m}. \tag{7.4}$$

引理 7.1。设 $(a + v_1b)x + b(y + v_2x) = kp^n$ 和 w 如（*5.4*）和（*7.2*）中所给。则

$$a + v_1b \le a + vb < p^{n-1}, \qquad y + v_2x \le y + vx < p^{n-1}. \tag{7.5}$$

证明。设 $U = X/d, V = Y/d - wX/d$和 $\tau = b_0/d$如 (7.3) 中所述。则 $(a+wb)U + bV = \tau p^n$。由于 v是使得 ($a + vb, b$) 与 F_r的一条边配对的最小值，而 $(U,V) \in F_r$, $v \le w$。因此 $a + v_1b \le a + vb \le a + wb < p^{n-m}$，最后一个不等式由 (7.4) 得出。第二个不等式的证明思路类似，留给读者完成。□

7.2. 中的顶点上界 $T \setminus S_1$。设 E 为 S_1的自由边集合。根据我们在第 4.5 小节中的结果（详见第 11 节），通过在 E 的每条边 (s,t) 上至多插入 $p-1$ 个顶点，可以得到一个法雷数列 T。能够得到的最大顶点对应于在一条自由边上进行 $p-1$ 次插入，且这些插入遵循如下斐波那契模式 ($f_1 = f_2 = 1$, $f_m = f_{m-1} + f_{m-2}$)：

$$\{s, s+t, \ldots\ldots f_{p-1}s + f_pt, \ldots\ldots, s+2t, t\}. \tag{7.6}$$

为了得到所有可能自由边的上界，我们首先假设 $a+(v_1-1)b = s < t = a+v_1b$（见 (5.5)）。容易证明，最大的顶点是

$$f_{p-1}s + f_pt = f_{p-1}(a + (v_1-1)b) + f_p(a + v_1b) \le (f_{p+1}/2)p^{n-1} + f_pp^{n/2}. \tag{7.7}$$

注意，(7.7) 可由 (7.5) 以及如下事实得到： $v_1 \le (v+1)/2$，因为当 v 为偶数时 $2v_1 = v$，当 v 为奇数时 $2v_1 - 1 = v$。将 $(s,t) \in N_e$ 替换为 $(u,v) \in F_r$，并重复我们的构造。由于 u, $v \le p^{n/2}$，显然可知 $f_{p-1}u + f_pv \le (f_{p+1}/2)p^{n-1} + f_pp^{n/2}$.。总之，我们有：

命题 7.2。 T 可以选择为使得 T 的顶点上界为

$$(f_{p+1}/2)p^{n-1} + f_pp^{n/2}. \tag{7.8}$$

8. The main result

在本节中， $p = 2$ 和 $n \geq 2$。首先回顾一下，当$n \geq 2$时， $\Gamma_0(2^n)$没有椭圆元素。因此， $\Gamma_0(2^n)$的法雷数列不具有椭圆边。

定理 8.1。 *(主定理)*。 $\Gamma_0(2^n)$ 具有一个法雷数列 $T = \{e_i\}$ ，使得

$$e_i \leq 2^{n-1}. \tag{8.1}$$

证明。 设 $T = \{e_i\}$ 如 (6.1) 所示。由于 (7.8) 给出的上界显然大于 (7.5) 给出的上界，我们可以假设最大的顶点来自 $T \setminus S_1$。根据 (6.1)，最大的顶点形式为 $e_j = 2^i z$。此外，(7.8) 表明

$$2^i z < 2^{n-1} + 2^{n/2}. \text{ Equivalently, } z < 2^{n-i-1} + 2^{n/2-i}. \tag{8.2}$$

由于 $n/2 - i < 0$，因此有 $z \leq 2^{n-i-1}$。由此可得， $e_j = 2^i z \leq 2^{n-1}$。 □

8.1. 上界 2^{n-1} 是最优的。 根据引理 3.3 和 3.4，存在唯一的 $e_j \in T$，使得 $e_j = z2^{n-1}$。根据定理 8.1， $z = 1$。因此， T 的上界 2^{n-1} 是最优的，并且在此 e_j处取到。

8.2. 独立生成元。 T 的所有边配对构成了 $\Gamma_0(2^n)$的一组独立生成元 $\{g_i\}$ 。根据定理 8.1， $e_i \leq 2^{n-1}$。 g_i 的 (2,1) 项具有$ax + by$的形式，其中 (a, b) 和 (x, y) 是 T的边（见 [CLLT]）。因此， g_i的 (2,1) 项的上界为 $2 \cdot 2^{2n-2} = 2^{2n-1}$.

8.3. 的自由边 。 以下引理有助于求得 $\Gamma_0(2^n)$的法雷数列。

引理 8.2。 设 $n \geq 3$ ，且(c, d) 是 S_1的一条自由边。那么 c 和 d 是链上的相邻顶点

$$N_e = \{a, a + b, a + 2b, \ldots, a + v_1 b, b\} \cup \{x, y + v_2 x, \ldots, y + x, y\}, \tag{8.3}$$

其中 $e = (a, b) = (a, b_0 2^m) \in F_r\,(ab_0\ odd)$ 且$(x, y) = (x_0 2^m, y) \in F_r\,(yx_0\ odd)$。此外， $m = 1$。特别是，如果 $m \geq 2$，那么所有来自 N_e 的边(c, d) 都不是 S_1的自由边。

证明。 我们首先注意到，如果 (a, b) 是 S_1 的一条边，同时也是 F_r 的一条边，那么 (a, b) 不可能是自由边，因此 S_1 的任意自由边都是某个 e 的一条边。设

$$c = a + kb_0 2^m,\ d = a + (k + 1)b_0 2^m. \text{ Then } c + d = 2a + (2k + 1)b_0 2^m. \tag{8.4}$$

根据第6.1小节中的结果， $c + d = 2^i z$、 $i > n/2 \geq 3/2$。注意， a 是奇数。因此 $m = 1$。情形 $c = y + (k + 1)x_0 2^m$， $d = y + kx_0 2^m$ 可以类似地处理。□

9. Algorithm [DKLT] for $\Gamma_0(2^n)$

下面给出用于确定 T 的算法。

(i) 构造 F_r，其中 $r = \lfloor 2^{n/2} \rfloor$。(ii) 检查每一条这样的边 $(a, b2^i)$ 是否自由（ab 为奇数，$i \geq 1$）。注意，只有当 $(a, b2^i)$ 与形如 $(x2^i, y)$ 的边配对时，它才不是自由边。(iii) 将 (ii) 中的自由边列为 $s_1, s_2, \ldots, s_k$。我们可以选择这样的排序，使得 $s_1, s_2, \ldots, s_r, r < k$ 是形如 $(a_i, b_i 2)$ 的边，其中 $a_i b_i$ 为奇数。依次构造 N_{s_i} （见 (5.5)）。(iv) 列出所有由插入 N_{s_i} $(i \leq r)$ 得到的边 (a, b)，其中 ab 为奇数。注意，引理 8.2 表明， S_1 可能存在的自由边必须来自 $N_{s_i}, i \leq r$。

(v) 设 $s=(a,\ b)$ 是 (iv) 中的一条边。若 $a+b$ 是某个 $i\geq n/2$ 的倍数，则将 $a\oplus b$ 插入 $(a,\ b)$。(vi) 由于经过 ((vi) 中所述的插入后已没有剩余的自由边（见第6.1小节），上述所有顶点组成的集合给出了 $\Gamma_0(2^n)$ 的法雷数列。

定理 9.1。 本节中的算法 *[DKLT]* 给出了一个法雷数列 T，其上界 2^{n-1} 对于 $\Gamma_0(2^n)$是最优的。

证明。 应用定理 8.1 和第 8.1 小节。 □

10. A simple conjecture

10.1. 我们在第 9 节中给出的算法可以修改，从而为许多$\Gamma_0(p^n)$的例子构造出一个良好的法雷数列，这促使我们猜想

猜想 10.1。 如果 $n\geq 3$，那么 $\Gamma_0(p^n)$ 有一个法雷数列 $\{e_i\}$，使得 $e_i\leq p^{n-1}$。

这个猜想是我们针对 $\Gamma_0(N)$ 提出的更一般猜想的特例；参见 [DKLT，猜想 3.16]。为了证明这个猜想，我们可能需要找到一个虽小却至关重要的例子。当 $p=2$ ($\Gamma_0(64)$ for $\Gamma_0(2^n)$) 时，我们有这样一个例子。遗憾的是，当 p 为奇数时，我们没有这样的例子。

11. Appendix

本节将说明，为了得到 $\Gamma_0(p^n)$ 的法雷数列，每条 S_1 的自由边上至多需要插入 $p-1$ 个顶点。我们回顾如下 $\Gamma_0(p^n)$ 的尖点分类：

(1) $c=[1/0]=[1/p^n]$；该尖点的宽度为 1；(2) 对每个满足 $\gcd(a,p)=1$ 的整数 $1\leq a<p^i$，以及每个整数 $1\leq i\leq n/2$，都有 $c=[a/p^i]$；该尖点的宽度为 p^{n-2i}；(3) 对每个满足 $\gcd(a,p)=1$ 的整数 $1\leq a<p^{n-i}$，以及每个整数 $n/2<i<n$，都有 $c=[a/p^i]$；该尖点的宽度为 1；(4) 对每个满足 $\gcd(b,p)=1$ 的既约分数 a/b，都有 $c=[0/1]=[a/b]$；该尖点的宽度为 p^n。

根据前面各节的讨论，从 S_1 到 $\Sigma(p^n)$ 的投影覆盖了类型 (1) 和 (2) 尖点的尖点环带，在类型 (3) 的尖点环带上为空，并部分覆盖了类型 (4) 的环带 ($c=[0/1]$)。我们需要仔细分析尖点 $c=[0/1]$ 周围的 Farey 三角形族的结构。

11.1. 尖点周围的三角形 $[0/1]$. 将尖点 $[0/1]$ 周围的 Farey 三角形族提升为以下一族连续的 p^n 个 Farey 三角形会很方便；这些三角形在 $\mathbb{H}$ 上的 $0/1$ 处有一个顶点：

$$\Delta:=\left\{\left(\frac{0}{1},\frac{1}{0},\frac{1}{1}\right),\left(\frac{0}{1},\frac{1}{1},\frac{1}{2}\right),\ldots,\left(\frac{0}{1},\frac{1}{p^n-1},\frac{1}{p^n}\right)\right\},$$

in w其中每组三个元素构成相应三角形的三个顶点。为简单起见，我们记 te

$$\Delta=\{[0,1],[1,2],\ldots,[p^n-1,p^n]\},$$

并且隐含地将 Δ 中的每个元素 $[a,b]$ 视为一个顶点为 $0\,1,\ \frac{1}{a}$和 $\frac{1}{b}$ 的 Farey 三角形。根据引理 3.4(i)(iii)，Δ 中的两个不同元素 $[a,a+1]$ 和 $[b,b+1]$ 是 $\Gamma_0(p^n)$-等价的；若存在一个元素 $\gamma\in\Gamma_0(p^n)$ 将三角形 $\left(\frac{0}{1},\frac{1}{a},\frac{1}{a+1}\right)$映射为三角形 $\left(\frac{0}{1},\frac{1}{b},\frac{1}{b+1}\right)$，且映射方式如下之一，则记作 ── $[a,a+1]\sim[b,b\mp1]$: ──

- $\gamma\left(\frac{0}{1}\right)=\frac{1}{b+1}, \gamma\left(\frac{1}{a}\right)=\frac{0}{1}, \gamma\left(\frac{1}{a+1}\right)=\frac{1}{b}$.
- $\gamma\left(\frac{0}{1}\right)=\frac{1}{b}, \gamma\left(\frac{1}{a}\right)=\frac{1}{b+1}, \gamma\left(\frac{1}{a+1}\right)=\frac{0}{1}$.

我们有以下性质。

引理 11.1。 Δ 中的两个不同元素 $[a,a+1]$ 和 $[b,b+1]$ 等价，当且仅当$a(b+1)+1$ 或 $b(a+1)+1$ 可被 p^n 整除。特别地，$[a-1,a]\sim[a,a+1]$ 当且仅当 $a^2\equiv 0$ 或 $a^2\equiv -1$ 模 p^n。

证明。应用矩阵 $\begin{bmatrix} a & -1 \\ a & b+1 \end{bmatrix}$ 或 $\begin{bmatrix} a+1 & -1 \\ b & a+1 \end{bmatrix}$。

□

将 $N([a,a+1])$ 记为 Δ 中与 $[a,a+1]\in\Delta$ $\Gamma_0(p^n)$ 等价的不同元素的个数。

引理 11.2。 对于每个 $[a,a+1]\in\Delta$，我们有 $N([a,a+1])\in\{1,2,3\}$，并且

- $N([a,a+1])=3$ 当且仅当 最大公因数$(a(a+1),p)=1$，并且 $a(a+1)\not\equiv -1$ (模 p^n)，
- $N([a,a+1])=2$ 当且仅当 最大公因数$(a(a+1),p)=p$，
- $N([a,a+1])=1$ 当且仅当 $a(a+1)\equiv -1$ (模 p^n)。

Proof. 该结果可由两个简单的事实推得:

- 尖点 $[0/1]$ 的宽度为 p^n,
- 上半平面 Δ 中的三角形有三个顶点，其中至少两个与尖点 $[0/1]$(p^n)-等价。

□

11.2. 至多插入 $p-1$ 个顶点。在 Δ 中，每个三角形都属于以下两个互不相交的子集之一:

$$U_L=\left\{[kp^i-1,kp^i]\,\middle|\,1\le i\le n/2,\ 1\le k\le p^{n-i},\ \text{and}\ \gcd(k,p)=1\ \text{if}\ k\ne p^{n-i}\right\},$$
$$U_R=\left\{[kp^i,kp^i+1]\,\middle|\,1\le i\le n/2,\ 0\le k<p^{n-i},\ \text{and}\ \gcd(k,p)=1\ \text{if}\ k\ne 0\right\},$$

与理想多边形中顶点集为 S_1 的三角形 Γ_0(p^n)-等价，因为每个这样的三角形都至少有一个顶点代表上述分类中类型 (1) 或类型 (2) 的尖点。更准确地说，若 $\pi:\mathbb{H}\to\Sigma$(p^n) 表示投影，则 $U_L\cup U_R$ 中所有三角形的像都位于 π(S_1) 中。

Δ 中 $\{[x,x+1],\dots,[x+k-1,x+k]\}$ 个连续元素组成的集合称为 Δ 中长度为 k 的间隙，其中 $k\ge 1$。根据上述讨论，我们得到以下两个引理。我们稍微滥用了记号，也用 S_1 表示 Δ 中由与某个关联于 S_1 的三角形等价的三角形组成的子集。

引理 11.3。 $\Delta\setminus S_1$ 是长度至多为 $2p-2$ 的间隙集合。

$\Delta\setminus S_1$ 的间隙 $\{[x,x+1],\dots,[x+k-1,x+k]\}$ 若其两侧 $[x-1,x]$ 和 $[x+k,x+k+1]$ 均不在 $\Delta\setminus S_1$ 中，则称为极大 间隙。

引理 11.4。 如果 $\{[x,x+1],\dots,[x+k-1,x+k]\}$ 是 $\Delta\setminus S_1$ 的极大间隙，那么两条边（0，$\frac{1}{x}$）和（0，$\frac{1}{x+k}$）分别与 S_1 中的两条自由边 Γ_0（p^n）等价。

我们的目标是以合理且系统的方式填补 $\Delta\setminus S_1$ 的所有间隙。记 b y

$$F(S_1)=\{(a_1,b_1),(a_2,b_2),\dots,(a_u,b_u)\}$$

S_1的自由边集合。

步骤1: 我们按如下方式构造 S_2 :

1. 将 $a_1 + b_1$ 插入(a_1, b_1)，得到

$$S_1^1 = \{(a_1, a_1 + b_1), (a_1 + b_1, b_1), (a_2, b_2), \ldots, (a_u, b_u)\}.$$

2. 考虑下一条边（a_2，b_2），有两种可能：
i. 如果（a_2, b_2）仍是 S_1^1中的一条自由边，则将 $a_2 + b_2$ 插入（a_2, b_2），得到$S_1^2 = \{$（$a_1, a_1 + b_1$），（$a_1 + b_1, b_1$），（$a_2, a_2 + b_2$），（$a_2 + b_2, b_2$），（a_3, b_3）.....，（a_u, b_u）$\}$ii. 如果（a_2, b_2）不是S_1^1中的一条自由边，则考虑下一条边（a_3, b_3），而不是（a_2，b_2）.
3. 一般而言，S_1^{i+1}由 S_1^i 通过将 $a + b$ 插入 S_1^i的一条自由边（a，b）得到，且需满足额外条件（a，b）$\in S_1$。注意，（a，b）不再是 S_1^{i+1}中的一条边。4. 当构造结束时，我们得到集合 S_2。注意，在 S_2中，S_1 的每条自由边（a_i，b_i）要么已配对，要么被配对（a_i，$a_i + b_i$）和（$a_i + b_i$，b_i）所取代。

根据 S_2的构造，我们有以下引理：

引理 11.5. $\Delta \setminus S_2$ 是长度至多为 $2p - 4$的间隙的集合。

证明。设 $\{[x, x + 1], \ldots, [x + k - 1, x + k]\}$ 是 $\Delta \setminus S_1$的一个极大间隙。由引理 11.3，$1 \leq k \leq 2p - 2$。由引理 11.4，$\left(\begin{smallmatrix} 0 & 1 \\ x & \end{smallmatrix}\right)$与$S_1$中的一条自由边（即$(a_i, b_i)$）在 $\Gamma_0(p^n)$意义下等价。根据上述构造，(a_i, b_i)不再是 S_2中的自由边；因此，三角形 $[x, x + 1]$ 不再是 $\Delta \setminus S_2$中的元素。同理，$[x + k - 1, x + k]$ 也不再是 $\Delta \setminus S_2$中的元素。因此，若 $\Delta \setminus S_1$ 的一个极大间隙长度大于1，则在 $\Delta \setminus S_2$中，其长度至少减少2。结论得证。□

步骤2：完成步骤1后，如果 S_2 仍有自由边，我们就对 S_2 应用步骤1并得到 S_3。一般而言，如果S_i 仍有自由边，我们就按照步骤1从 S_i构造 S_{i+1}。由于以下引理，该构造至多经过 $p - 1$ 步便会停止：

引理 11.6。 $\Delta \setminus S_i$ 是由长度至多为 $2p - 2 - 2i$的间隙构成的集合。

证明。 证明与引理 11.5 的证明类似。 □

这就完成了定理 1.2 中关于法雷数列 $\{e_i\}$ 的 Γ_0（p^n）的 e_i 上界的证明。

References

[CLLT] *Special polygons for subgroups of the modular group and applications* 4 1993 11 34
S. P. Chan、M. L. Lang、C. H. Lim、S. P. Tan，《国际数学杂志》（）-。[DKLT] N.M. Doan、S. Kim、M.L. Lang 和 S.P. Tan， *Optimal special polygons for the congruence subgroups* Γ_0（p）*and* Γ_0（pq），《几何分析杂志》35，文章编号 216（2025）。[Ku] R.S. Kulkarni,
An arithmetic-Geometric method in the study of subgroups of the modular group，《美国数学杂志》113（1991），1053-1134。[Mag] 数学学院计算代数组和悉尼大学。统计学、法雷符号和基本域，Magma 手册，https://magma.maths.usyd.edu.au/。[Sag] SageMath 项目， $PSL(2, \mathbb{Z})$ 的算术子群的法雷符号，Sage 10.1 参考手册，https://doc.sagemath.org/。[Sh] G. Shimura， *Introduction to the arithmetic theory of automorphic functions*，岩波书店、出版社和普林斯顿大学出版社，1971。

Department of Mathematics, National University of Singapore, Singapore & Institute of Mathemat-ics, Vietnam Academy of Science and Technology, Vietnam*Email address*: minh.dn@nus.edu.sg, dnminh@math.ac.vn

School of Mathematics、 Korea Institute for Advanced Study (KIAS)、 Korea
Email address: kimsh@kias.re.kr

Singapore*Email address*:
lang2to46@gmail.com

Department of Mathematics, National University of Singapore, Singapore
Email address: mattansp@nus.edu.sg