arXiv:2302.00920v1 [math.NT] 2 Feb 2023

某些对角方程与素数长度的冲突避免码

LIANG-CHUNG HSIA、HUA-CHIEH LI 和 WEI-LIANG SUN

摘要。我们从数论的角度研究最优冲突避免码（CAC）的构造。素数长度 p、重量 3 的最优冲突避免码的大小，可表述为有限域 $\mathbb{F}_p$ 上某些形如 $g^2X^\ell + gY^\ell + 1 = 0$ 的扭曲费马方程的可解性问题，其中 g 是模 p 的某个原根。我们通过允许基域为 $\mathbb{F}_p$. 的任意有限扩张 $\mathbb{F}_q$，在更一般的情形下研究扭曲费马方程的求解问题。我们证明，当 q 大于阶数量级 $O(\ell^2)$ 的某个下界时，存在 $\mathbb{F}_q^\times$ 的生成元 g，使得所讨论的方程在 $\mathbb{F}_q$. 上可解。利用我们的结果，我们为素数长度、重量 3 的最优冲突避免码的构造取得了新的成果。

关键词：二进制协议序列、冲突避免码、对角方程、Hasse-Weil 界、拉马努金和、斐波那契本原根。

1. 引言

在信息论中，用于在无反馈的多址碰撞信道上传输数据包的二进制协议序列集合称为冲突避免码（CAC）。数十年前， [Mat90、NGM92、GV93、TR02、LT05、Lev07] 已对其进行研究。长度为 n、（汉明）重量为 w 的 CAC 的数学模型如下。设 $\mathbb{Z}/n\mathbb{Z}$ 为整数环 $\mathbb{Z}$ 模 n 的加法群。对于 $\mathbb{Z}/n\mathbb{Z}$ 的一个 w 元子集 $x = \{x1, \ldots, x_w\}$，令 $\Delta(x) = \{x_i - x_j \mid i \neq j\}$。长度为 n、重量为 w 的 CAC 是由 $\mathbb{Z}/n\mathbb{Z}$ 的 w 元子集组成的集合 $\mathscr{C}$，满足对于任意不同的 x、$y \in \mathscr{C}$，都有 $\Delta(x) \cap \Delta(y) = \varnothing$。$\mathscr{C}$ 的每个 w 元子集 x 都称为一个码字。若 CAC $\mathscr{C}$ 的大小在所有长度和重量相同的 CAC 中达到最大，则称其为最优 CAC。重量为 1 或 2 时，求出最优大小并不困难。然而，对于重量大于 2 的情形，寻找最优 CAC 并确定其大小仍是一个未解决的问题。首先面临的挑战是重量 3 的情形。本文的目的之一是从数论的角度研究寻找最优 CAC 的问题，并为重量 3 的最优 CAC 构造提供新的结果。因此，我们所研究的所有 CAC 都是重量 3 的。

对于偶数长度且重量为 3 的情形，关于构造最优 CAC 的问题已有完整答案，相关成果见 [LT05, JMJ+07, MFU09, FLM10]。相比之下，奇数长度的情形尚未解决。令 $o_m(2)$ 表示 2 模正奇整数 m 的乘法阶。对于奇数长度 n 的 CAC，我们记 $n = n_1 n_2$，使得对 n_1 的所有素因子 p，$o_p(2)$ 都是 4 的倍数；而对所有

n_2. 的素因子 p，o_2. (2) 都不能被 4 整除。在 $n_2 = 1$ 时， [LT05, Lev07] 构造了一个最优 CAC。若 $n_2 \neq 1$，则 [FLS14] 证明，可以由长度为 n_2 的最优 CAC 构造出长度为 n 的最优 CAC。 [FLS14] 还证明，若已知如何构造素数长度的最优 CAC，且所讨论的素数 p 是非 Wieferich 素数，则可以构造素数幂长度的最优 CAC。关于其他奇数长度或紧致／等差 CAC 的构造，参见 [Mom07, WF13, LMSJ14, MM17, HLS] 。事实证明，素数长度的 CAC 是需要构造的基本情形。这自然引导我们研究素数长度、重量为 3 的 CAC。

设 p 为奇素数，并用 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ 表示含 p 个元素的有限域。回顾一下，形如 $\{0, a, 2a\}$ 的码字称为等差码字。在论文 [LT05], 中，作者证明，当 $4 \mid o_p(2)$ 时，存在一个由 p_4^{-1} 个等差码字组成的最优冲突避免码。相反，若 $4 \nmid o_p(2)$，则仅由等差码字组成的冲突避免码通常不是最优的。通过分析非等差码字， [FLS14] 给出了奇数长度最优冲突避免码大小的一个上界。现在回顾一下他们关于素数长度冲突避免码的结果。令

$$\mathscr{O}(p) = \begin{cases} \frac{p-1}{2o_p(2)} & \text{if } o_p(2) \text{ is odd}, \\ \frac{p-1}{o_p(2)} & \text{if } o_p(2) \equiv 2 \pmod 4, \\ 0 & \text{if } 4 \mid o_p(2) \end{cases}$$

并令 M(p) 表示长度为 p 的最优冲突避免码的大小。那么，根据 [FLS14， 3] 引理可得

$$\frac{p-1-2\mathscr{O}(p)}{4} \leq M(p) \leq \frac{p-1-2\mathscr{O}(p)}{4} + \left\lfloor \frac{\mathscr{O}(p)}{3} \right\rfloor. \tag{1}$$

注意，在 $\mathscr{O}(p) \leq 2$ 的情况下，不等式 (1) 已经给出 $M(p) = \frac{p-1-2\mathscr{O}(p)}{4}$。对于 $\mathscr{O}(p) \geq 3$，作者提供了一种构造非等差冲突避免码的算法，并猜想该算法生成的冲突避免码由 $\frac{p-1-2\mathscr{O}(p)}{4}$ 个等差码字和 $\left\lfloor \frac{\mathscr{O}(p)}{3} \right\rfloor$ 个非等差码字组成。换言之，式 (1) 中的上界可以达到，因此他们的算法所得到的冲突避免码实际上是最优冲突避免码。该算法得以奏效所需的关键性质如下文的猜想 A 所述。为便于讨论，我们将他们的猜想改写为关于乘法群 $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$ 中由 -1 和 2 生成的子群的陪集的表述，其中 $\mathbb{F}_p$。

猜想 A ([FLS14， 猜想 1])。设 p 是一个非 Wieferich 素数。那么子群 -1 与 2 在 $\mathbb{F}_p^\times$ 中生成的子群有 $3\left\lfloor \frac{\mathscr{O}(p)}{3} \right\rfloor$ 个陪集 $A_1, B_1, C_1, \ldots, A_{\left\lfloor \frac{\mathscr{O}(p)}{3} \right\rfloor}, B_{\left\lfloor \frac{\mathscr{O}(p)}{3} \right\rfloor}, C_{\left\lfloor \frac{\mathscr{O}(p)}{3} \right\rfloor}$，使得对每个 $i = 1, \ldots, \left\lfloor \frac{\mathscr{O}(p)}{3} \right\rfloor$，都存在一个三元组 $(a_i, b_i, c_i) \in A_i \times B_i \times C_i$ 满足

$$a_i + b_i + c_i = 0 \quad \text{in } \mathbb{F}_p.$$

在本文中，我们用 $H = \langle -1, 2 \rangle$ 表示由 -1 与 2 在 $\mathbb{F}_p^\times$ 中生成的子群，并令

$$\ell_0 = [\mathbb{F}_p^\times : H]$$

H 在 $\mathbb{F}_p^\times$. 中的指标。注意，若 $4 \nmid o_p(2)$，则根据定义可得 $\mathscr{O}(p) = \ell_0$。此外，猜想 A 是一个非空命题，当且仅当 $\mathscr{O}(p) = \ell_0 \geq 3$。

猜想 A 背后的思路如下。假设猜想 A 成立，那么猜想中的每个三元组 (a_i, b_i, c_i) 都对应一个非等差码字 $x_i = \{0, a_i, -c_i\}$，其差集为 $\Delta(x_i) = \{\pm a_i, \pm b_i, \pm c_i\}$。因此，我们有 $\left\lfloor \frac{\mathscr{O}(p)}{3} \right\rfloor$ 个非等差码字，其差集两两不相交。根据 $\mathbb{F}_p^\times$ 中 $\cup_{i=1} \Delta(x_i)$ 的补集，他们的算法随后会生成 $p-1-2\mathscr{O}(p)$ 4 个等差码字，从而得到一个大小与 (1) 中给出的上界相符的冲突避免码。

作为示例，我们简要讨论 [FLS14, Example 3] 中处理的情形，其中长度 $p = 31$。注意，$o_{31}(2) = 5$，因此 $\mathscr{O}(31) = 3.$。于是，猜想 A 预测存在 $3\left\lfloor \frac{\mathscr{O}(31)}{3} \right\rfloor = 3$ 个陪集，并且每个陪集中各有一个元素，使得它们的和为零。可以发现，三元组 $(2, 3, -5)$ 给出了一个解，对应的码字为 $\{0, 2, 5\}$，其差集恰为 $\{\pm 2, \pm 3, \pm 5\}$；而 2、3 和 -5 恰好分别属于 $\mathbb{F}_p^\times$ 中 H 的三个不同陪集。此外，他们的算法还生成了六个等差码字：$\{0, 4, 8\}$、$\{0, 6, 12\}$、$\{0, 7, 14\}$、$\{0, 9, 18\}$、$\{0, 10, 20\}$ 和 $\{0, 15, 30\}$。总之，可以得出，长度为 31 的最优冲突避免码的大小为 $M(31) = 7.$

与此同时，在 [MZS14] 中，作者提出了一个猜想，该猜想根据 $\mathbb{F}_p^\times / H$ 的群结构，为猜想 A 中三元组 (A_i, B_i, C_i) 的存在性提供了解。

猜想 B（[MZS14，猜想]）。设 p 为奇素数。若 $\ell_0 \geq 3$，则存在 $b \in gH$ 和 $c \in g^2 H$，使得

$$1 + b + c = 0 \quad \text{in } \mathbb{F}_p$$

对于 $\mathbb{F}_p^\times$. 的某个生成元 g

注1.1。我们看到，通过令 $A_1 = H$、$B_1 = gH$、$C_1 = g^2H$、$A_2 = g^3H$、$B_2 = g^4H$、$C_2 = g^5H$ .....、$A_e = g^{3e-3}H$、$B_e = g^{3e-2}H$ 以及 $C_e = g^{3e-1}H$（其中 $e = \left\lfloor \frac{\ell_0}{3} \right\rfloor$），猜想 B 蕴含猜想 A。此外，猜想 B 并不假设 $4 \nmid o_p(2)$。

注意，子群 $H = \langle -1, 2 \rangle$ 由 ℓ_0 次幂的所有元素组成，这些元素属于 $\mathbb{F}_p^\times$.。由此可知，猜想 B 中的元素 b 和 c 分别具有 gy^{ℓ_0} 和 $g^2x^{\ell_0}$ 的形式，其中 x、$y \in \mathbb{F}_p^\times$。注意，若 $\ell_0 \geq 3$，则对角方程 $g^2X^{\ell_0} + gY^{\ell_0} + 1 = 0$ 的任意 $\mathbb{F}_p$-有理解 (x, y) 都必须满足 $xy \neq 0$，因为 $-1 \in H$，且 g 是 $\mathbb{F}_p^\times$. 的生成元。因此，任意 $\mathbb{F}_p$-有理解都会给出猜想 B 中一对元素 b 和 c。故猜想 B 等价于以下命题。

猜想 C. 设 p 为奇素数。若 $\ell_0 \geq 3$，则存在 $\mathbb{F}_p^\times$ 的一个生成元 g，使得对角方程

$$g^2X^{\ell_0} + gY^{\ell_0} + 1 = 0 \tag{2}$$

在 $\mathbb{F}_p$ 上可解。

猜想 C 的表述有一个优点：方程 (2) 的 $\mathbb{F}_p$-有理解的数量可以通过某些特征和来计算，而这些特征和已在数论中得到充分研究。通过证明猜想 C 的若干情形成立，我们也得到了猜想 B 和猜想 A 成立的相应情形。因此，通过研究方程 (2) 在 $\mathbb{F}_p$ 上的可解性，我们能够为构造最优 CAC 提供新结果。

受猜想 C 启发，我们不再局限于在素域 $\mathbb{F}_p$ 上、针对特定指数 ℓ_0 研究形如 (2) 的对角方程，而是考虑更一般的情形：取 $\mathbb{F}_p$ 的有限扩张作为基域，并允许方程中的指数比 ℓ_0 更一般。设 q 为一个素数幂，且 ℓ 是 $q-1$ 的一个真因子。我们考虑以下对角方程的可解性

$$g^2X^{\ell} + gY^{\ell} + 1 = 0 \tag{3}$$

在含有 q 个元素的有限域 $\mathbb{F}_q$ 上，其中 g 是 $\mathbb{F}_q$. 的乘法群 $\mathbb{F}_q^\times$的生成元。鉴于猜想 C，我们关心是否存在一个生成元 g，使得方程（3）有一个 $\mathbb{F}_q$- 有理解。然而，对于 q 的某些除数 -1（而非 ℓ_0.），答案可能是否定的。例如，当 $(q, \ell) = (13,6),(23,11)$ 时，不存在任何 $\mathbb{F}_q^\times$ 的生成元使得 (3) 有一个 $\mathbb{F}_q$-有理解。另一方面，作为下文主要结果的推论，只要 $q \geq 19$（若 $\ell = 6$）且 $q \geq 322$（若$\ell = 11.$），则 $\mathbb{F}_q^\times$的某个生成元 g 会使方程（3）有一个 $\mathbb{F}_q$-有理解。我们的第一个主要结果是给出 q 的一个下界，使得对于 $\mathbb{F}_q^\times$的某个生成元 g，方程（3）有一个$\mathbb{F}_q$-有理解。

定理 A（= 定理 4.3）。设 q 为一个素数幂，且 ℓ 是 q 的真因子 -1。如果

$$q \geq (2^{\omega(\ell)}(\ell - 3 - \delta) + 2)^2 - 2$$

其中 ω（ℓ）表示 ℓ 的不同素因子的个数，并且

$$\delta = \begin{cases} 1 & \text{if } 4 \mid \ell, \\ 0 & \text{otherwise,} \end{cases}$$

那么存在 $\mathbb{F}_q^\times$的一个生成元 g，使方程（3）在 $\mathbb{F}_q$上有解。

注 1.2. 由哈斯-韦伊界（见定理 1）可知，方程（3）的$\mathbb{F}_q$-有理解数量的下界为 $q + 1 - 2g_\ell\sqrt{q}$，其中 $g_\ell = (\ell-1)(\ell-2)/2$ 是方程（3）在 $\mathbb{F}_q$. 上定义的曲线的亏格。因此，只要满足 $q > (\ell-1)^2(\ell-2)^2$.，对于任意 $g \in \mathbb{F}_q^\times$，方程（3）都有一个 $\mathbb{F}_q$-有理解。我们有理由期待，在猜想 C 给出的较弱条件下，这一下界还能进一步改进。

猜想 C。定理 A 中我们证明，改进后的下界的数量级为 O(ℓ^2)。

定理 A 给出了猜想 C（以及猜想 A 和 B）成立的一个充分条件，适用于 q = p 为素数且 $\ell = \ell_0$ 的情形。因此，在给定的充分条件下，长度为 p、满足 $4 \nmid \mathrm{o}_p(2)$ 且重量为 3 的最优冲突避免码具有所需的大小。

推论 B. 设 p 是一个满足 $4 \nmid \mathrm{o}_p(2)$ 的奇素数，令 $\ell_0 = [\mathbb{F}_p^\times : \mathrm{H}]$，并令 $\omega(\ell_0)$ δ 如定理 A 中相对于 ℓ_0 的定义。若 $\mathrm{p} \geq (2^{\omega(\ell_0)}(\ell_0 - 3 - \delta) + 2)^2 - 2$，则长度为 p、重量为 3 的最优冲突避免码的大小为

$$\frac{p - 1 - 2\ell_0}{4} + \left\lfloor \frac{\ell_0}{3} \right\rfloor.$$

应用推论 B，我们可以无条件地证明对于 ℓ_0 值较小的素数，猜想 C 成立。例如，若 $1 \leq \ell_0 \leq 6$，则猜想 C 成立（参见推论 2.3、4.4 和 4.5）。结合 [MZS14]，中计算所得的结果，定理 A 确认了猜想 C 在很大范围的 ℓ_0 上成立。例如，如果 ℓ_0 是满足 $\ell_0 < 16411$ 的素数幂，或者它有两个满足 $\ell_0 < 8197$ 的不同的素因子，那么对于满足上述性质且 ℓ_0 的素数 p，猜想 C 成立（更多情形参见定理 5.1 和定理 5.2）。

本文的结构安排如下。第 2 节中，我们先固定一些记号，并讨论与方程（3）相关的一些众所周知的事实。特别地，通过应用哈斯-韦伊界，我们证明了当 $1 \leq \ell \leq 4$ 时，方程（3）在 $\mathbb{F}_q$ 上可解这一事实（推论 2.3）。随后，我们整理并证明第 3 节证明主要结果所需的结论。关键要素之一是拉马努金和，我们将在引理 3.2 中回顾它。第 4 节专门用于证明定理 A。通过恰当地整理方程（3）的解的个数表达式中的特征和，我们得以获得定理 A 给出的解的个数的所需界。在最后一节中，我们将主要结果应用于最优冲突避免码大小的问题，并推导出 ℓ_0 的一个较大范围，使得猜想 C（以及猜想 B 和 A）成立。

2. 预备知识

本节中，我们固定一些记号，并介绍若干与方程（3）的可解性问题相关的事实。设 $\mathbb{F}_q$ 为含 q 个元素的有限域，其中 q 是素数 p 的幂。取 $\mathbb{F}_q^\times$ 的一个生成元 g，以及 $q - 1$ 的一个真因子 ℓ。令 L 为 $\mathbb{F}_q^\times$. 中所有 ℓ 次幂元素构成的子群。我们有 $\mathbb{F}_q^\times/\mathrm{L}$ 由陪集 gL 生成，而 $\mathbb{F}_q^\times/\mathrm{L}$ 是循环群 ℓ 的阶。

回顾一下，我们关注的是方程（3）的可解性

$$g^2 X^\ell + g Y^\ell + 1 = 0$$

在 $\mathbb{F}_q$. 上。令 $\mathscr{C}_g$ 为由该方程定义的仿射平面曲线。注意， $\mathscr{C}_g$ 在 $\overline{\mathbb{F}_q}$上是非奇异且不可约的，其中 $\overline{\mathbb{F}_q}$是 $\mathbb{F}_q$. 的代数闭包。记 $\mathscr{C}_g$ 的 $\mathbb{F}_q$-有理点集为

$$\mathscr{C}_g(\mathbb{F}_q) = \left\{(x,y) \in \mathbb{F}_q^2 \mid g^2x^\ell + gy^\ell + 1 = 0\right\}$$

并令 $N_g = |\mathscr{C}_g(\mathbb{F}_q)|$ 为其基数。此外，令 $\mathscr{C}_g$ 为由齐次方程定义的射影平面中 $\mathscr{C}_g$的（扎里斯基）闭包

$$g^2X^\ell + gY^\ell + Z^\ell = 0. \tag{4}$$

注意到 $\mathscr{C}_g$ 也是非奇异的。我们用 N_g 表示 $\mathscr{C}_g(\mathbb{F}_q)$的基数。鉴于猜想 B 和猜想 C，我们尤其关注是否存在一个点 $(x,y) \in \mathscr{C}_g(\mathbb{F}_q)$满足 $xy \neq 0$. 下面的引理表明，除极少数特殊情形外，这始终成立。

引理 2.1. 方程 (4) 存在满足 $xyz = 0$ 的非平凡解 (x,y,z)，当且仅当以下情形之一成立：

(i) $\ell = 1$ 或 2；
(ii) $\ell = 4$ 且 $-1 \notin L$。

此外，如果 $\ell > 2$，那么 $xz \neq 0$.

证明。假设 (x,y,z) 是满足 $xyz = 0$ 的方程 (4) 的一个非平凡解。那么 x、y、z 中恰有一个为零。注意，如果 $x = 0$ 或 $z = 0$，那么 $-g \in L$，且 gL 在 $\mathbb{F}_q^\times/L$ 中的阶为 1 或 2；如果 $y = 0$，那么 $-g^2 \in L$，且 gL 在 $\mathbb{F}_q^\times/L$ 中的阶为 4。特别地，只要 $\ell \neq 2$，我们就有 $xz \neq 0$。在 $\ell = 4$ 的情况下，我们看到 $-L = g^2L \neq L$。由此可得 $-1 \notin L$。

反过来，如果 $\ell = 1$，显然方程 (4) 有一个满足 $xyz = 0$. 的非平凡解 (x, y, z)。假设 $\ell = 2$，则 $\mathbb{F}_q^\times/L = \{L, gL\}$。如果 $-1 \notin L$，那么 $-L = gL$。在这种情况下，对于某个 $a \in \mathbb{F}_q^\times$，$g = -a^2 \in L$。显然，我们有解 (x, y, z) = (1, a, 0) 和 (0, 1, a)。假设 $-1 \in L$，那么对于某个 $b \in \mathbb{F}_q^\times$，$-g^2 = b^2 \in L$；在这种情况下，我们有解 (x, y, z) = (1, 0, b)。

最后，假设 $\ell = 4$ 和 $-1 \notin L$。那么 g^2L 和 $-L$ 在循环群 $\mathbb{F}_q^\times/L$ 中的阶均为 2。因此，$-L = g^2L$，由此得到一个解 (x,y,z) = (1,0,b)，其中$-g^2 = b^4 \in L$。□

根据 [Wei48], ，方程（3）的解的数量 N_g 可以表示为一个特征和，下面我们回顾这一表示。通常，我们所说的 $\mathbb{F}_q$ 的乘法特征，是指群 $\mathbb{F}_q^\times$的特征，也就是从 $\mathbb{F}_q^\times$到 $\mathbb{C}^\times$. 的群同态。由于我们只讨论 $\mathbb{F}_q$的乘法特征，因此简称为特征。平凡特征记作 ε，满足 $\varepsilon(a) = 1$，对所有 $a \in \mathbb{F}_q^\times$. 均成立。我们将特征 χ 的定义域扩展为：若 $\chi = \varepsilon$，则 $\chi(0) = 1$；否则 $\chi(0) = 0$。我们将 χ 的扩展称为扩展特征；若不会引起混淆，仍将其记作 χ

我们固定一个阶为 ℓ. 的特征 χ。于是有

$$N_g = q + \sum_{1\le j,k\le \ell-1} \chi^j(-g^{-2})\chi^k(-g^{-1})J(\chi^j,\chi^k) \tag{5}$$

其中

$$J(\chi^j,\chi^k) = \sum_{a\in\mathbb{F}_q} \chi^j(a)\chi^k(1-a)$$

是关于 χ^j 和 χ^k的雅可比和。以下雅可比和的性质很有用。

引理 2.2（[LN97，定理 5.19、5.21、5.22]）。设 λ、ψ 是 $\mathbb{F}_q$的两个扩展特征。

(i) $J(\lambda,\psi) = J(\psi,\lambda)$;
(ii) $J(\varepsilon,\varepsilon) = q$;
(iii) $J(\lambda,\varepsilon) = 0$ *if* $\lambda \neq \varepsilon$;
(iv) $J(\lambda,\lambda^{-1}) = -\lambda(-1)$ *if* $\lambda \neq \varepsilon$;
(v) $|J(\lambda,\psi)| = \sqrt{q}$ *if* λ,ψ *and* $\lambda\psi$ *are all nontrivial.*

注意，对所有 $a\in\mathbb{F}_q^\times$，$|\chi^i(a)| = 1$。由引理 2.2 的 (iv) 和 (v)，可得 N_g 由 (5) 给出的以下估计

$$|N_g - q| \le M_0 + M_1\sqrt{q}$$

其中，M_0（分别为 M_1）表示满足 $\chi^j\chi^k = \varepsilon$（分别为 $\chi^j\chi^k \neq \varepsilon$）的有序对 (j, k) 的数量。注意，$M_0 = \ell - 1$ 和 $M_1 = (\ell-1)(\ell-2)$。因此，若

$$q > (\ell-1) + (\ell-1)(\ell-2)\sqrt{q}, \tag{6}$$

于是 $N_g > 0$。因此，当 q 足够大时（例如 $q > (\ell-1)^4$），对于任意 $g\in\mathbb{F}_q^\times$，都有 $N_g > 0$。

关于有限域上方程的有理解数量，哈斯-韦伊界 [Wei48] 提供了比上述粗略估计更精确的信息。

定理 1（哈斯-韦伊界）。设 $\mathscr{C}$ 是定义在 $\mathbb{F}_q$ 上的非奇异、绝对不可约射影曲线，且 $N_{\mathscr{C}} = |\mathscr{C}(\mathbb{F}_q)|$ 表示 $\mathscr{C}$上的 $\mathbb{F}_q$-有理点的数量。那么，

$$|N_{\mathscr{C}} - (q+1)| \le 2\mathfrak{g}\sqrt{q}$$

其中 $\mathfrak{g}$ 是 $\mathscr{C}$.的亏格

$\widetilde{}$将哈斯-韦伊界应用于 $\mathscr{C}_g$，可得

$$|\widetilde{N_g} - (q+1)| \le (\ell-1)(\ell-2)\sqrt{q}$$

$\widetilde{}$根据次数–亏格公式，$\mathscr{C}_g$ 的亏格为 $\mathfrak{g}_\ell = (\ell-1)(\ell-2)/2$ [Har77]。$\widetilde{}$因此，对于 $\mathbb{F}_q^\times$ 的任意生成元 g，只要 $q+1 > (\ell-1)(\ell-2)\sqrt{q}$，就有 $N_g > 0$；于是，$\bar{}$当 $q \ge (\ell-1)^2(\ell-2)^2$.时，$\widetilde{\mathscr{C}_g}(\mathbb{F}_q)$非空。

利用这个下界，可以很容易地验证猜想 C（以及猜想 B）在 ℓ. 取较小值时成立。以下结果是定理 1 的直接推论。为方便读者，我们给出一个证明。

推论 2.3. 对于 $1 \le \ell \le 4$，每个 $\mathbb{F}_q^\times$ 的生成元 g 都有 $N_g > 0$。此外，存在一点 $(x,y) \in \mathscr{C}_g(\mathbb{F}_q)$，使得 $xy \neq 0$，因此当 $\ell_0 = [\mathbb{F}_p^\times : H] \le 4.$ 时，猜想 C 成立

证明. 若 $\ell = 1$，则很容易推出结论，因此此情形的验证留给读者。我们先考虑 $\ell = 2.$ 的情形。注意，在这种情况下 $p > 2$ 且$\sim\mathfrak{g}_\ell = 0.$。因此，根据定理 1，$N_g = q + 1$。不难验证

$$N_g = \begin{cases} \widetilde{N_g} & \text{if } q \equiv 1 \pmod 4 \\ \widetilde{N_g} - 2 & \text{if } q \equiv 3 \pmod 4 \end{cases}.$$

因此，当 $q \equiv 1 \pmod 4$ 时，$N_g = q + 1$；当 $q \equiv 3 \pmod 4$ 时，$N_g = q - 1$。无论哪种情况，我们显然都有 $N_g > 0.$。还需证明存在一点 $(x, y) \in \mathscr{C}_g(\mathbb{F}_q)$，使得 $xy \neq 0.$。注意，在 $\mathscr{C}_g(\mathbb{F}_q)$ 中，满足 $x = 0$ 或 $y = 0.$ 的点至多有四个。当 $q \equiv 1 \pmod 4$ 时，我们有 $N_g = q + 1 \ge 6.$。接下来只需考察 $q \equiv 3 \pmod 4$ 的情形。由于根据假设，$\ell = 2$ 是 $q - 1$ 的真因子，因此我们知道 $q \ge 7$，并且还有 $N_g = q - 1 \ge 6.$。现在显然存在一点 $(x, y) \in \mathscr{C}_g(\mathbb{F}_q)$，使得 $xy \neq 0$，因为这两种情况下都有 $N_g > 4$。

~接下来，我们考虑 $\ell = 3$ 和 4 的情形。由于 $\ell > 2$，根据引理 2.1，我们有 $N_g = N_g$~。设 $\ell = 3.$。在这种情况下，$\mathscr{C}_g$ 的亏格为一。因此，哈斯-韦伊界给出

$$N_g \ge (q+1) - 2\sqrt{q} = (\sqrt{q} - 1)^2 > 0.$$

因此，在这种情况下，对于 $\mathbb{F}_q^\times$ 的任意生成元 g，都有 $N_g > 0$。假设存在方程（3）的一个解 (x, y)，使得对于 $\ell = 3.$，要么 $x = 0$，要么 $y = 0$。那么我们得到，g 或 g^2 是 $\mathbb{F}_q^\times.$ 中的立方。这意味着 gL 在群 $\mathbb{F}_q^\times/L$ 中的阶整除 2，这显然不成立，因为 $|\mathbb{F}_q^\times/L| = 3.$。因此，任意满足 $(\mathbb{F}_q)$ 的 $(x,y) \in \mathscr{C}_g$ 都必须满足 $xy \neq 0$，这正是所需。

假设 $\ell = 4$。直接计算可得，对于 $q > 49$，我们有 $N_g > 8$.由于方程（3）至多有八个解满足 $x = 0$ 或 $y = 0$ 对于$\ell = 4$，因此可知，对于 $q > 49$，存在 $(x, y) \in \mathscr{C}_g(\mathbb{F}_q)$，使得 $xy \neq 0$，如前所述。接下来只需检查满足 $q \le 49$ 且 4 是 $q - 1.$ 真因子的素数幂 q。因此，我们只需验证八种情况，即 $q = 9$、13、17、25、29、37、41、49。注意，若 $(x, y) \in \mathscr{C}_g(\mathbb{F}_q)$ 且 $xy \neq 0$，则 $(x^{-1}, x^{-1}y) \in \mathscr{C}_{g^{-1}}(\mathbb{F}_q)$。由此可知，$\mathscr{C}_g(\mathbb{F}_q)$ 含有一个坐标均非零的点，当且仅当 $\mathscr{C}_{g^{-1}}(\mathbb{F}_q)$ 也具有此性质。此外，对于 $\mathbb{F}_q^\times$ 的任意生成元 g′，在 $|\mathbb{F}_q^\times/L| = 4.$ 的情况下，我们有 $g'L \in \{gL、g^{-1}L\}$。由此可知，$\mathscr{C}_g(\mathbb{F}_q)$ 含有一个坐标均非零的点，当且仅当 $\mathscr{C}_{g'}(\mathbb{F}_q)$ 也具有此性质。因此，只需证明，对于 $\mathbb{F}_q^\times.$ 的一个生成元 g，$\mathscr{C}_g(\mathbb{F}_q)$ 含有一个坐标非零的点。我们

给出各个情形对应的下表。

q	9	13	17	25	29	37	41	49
g	α	2	3	β	2	5	6	γ
x	α	4	6	1	4	2	3	2
y	α	1	2	β^2	4	2	3	$2\gamma^7$

其中 $\alpha = 1+\sqrt{-1}$ 属于 $\mathbb{F}_9 = \mathbb{F}_3(\sqrt{-1})$，$\beta = 1+2\sqrt{2}$ 属于 $\mathbb{F}_{25} = \mathbb{F}_5(\sqrt{2})$，且 $\gamma = 4+\sqrt{-1}$ 属于 $\mathbb{F}_{49} = \mathbb{F}_7(\sqrt{-1})$。

至此，我们完成了对所有 $N_g > 0$. 的情形的验证。此外，我们还列出了所有满足 $xy \neq 0$ 的解 (x, y)，从而完成证明。□

我们想指出，无需使用哈斯-韦伊界，只需利用界 (6) 就可以证明推论 2.3。

鉴于猜想 C，我们只需找到 $\mathbb{F}_q^\times$ 的一个生成元 g，使得 $\mathscr{C}_g(\mathbb{F}_q)$ 非空。我们的目标不是计算 N_g，而是证明下列和

$$N(q,\ell) = \sum_{\mathbb{F}_q^\times = \langle g' \rangle} N_{g'} = \sum_{\substack{1 \le t \le q-1, \\ \gcd(t,q-1)=1}} N_{g^t}$$

在适当条件下是一个正整数。

3. 关键要素

本节汇集证明定理 A 所需的工具和结果。为简化记号，我们记 $(a_1,a_2) = \gcd(a_1,a_2)$，即整数 a_1 和 a_2. 的最大公约数。下面的引理是代数中的一个基本事实，我们将反复用到。由于在任何代数教材中都很容易找到它的证明，这里略去证明。

引理 3.1. 设 $n \in \mathbb{N}$，且 d 是 n 的一个因子。那么由下式诱导的典范群同态

$$\pi : (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/d\mathbb{Z})^\times$$

由.....诱导

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/d\mathbb{Z} \\ k+n\mathbb{Z} & \mapsto & k+d\mathbb{Z} \end{array}$$

是满射。此外，这个同态可分裂。具体而言，存在 $(\mathbb{Z}/n\mathbb{Z})^\times$ 的一个子群 M，它在 π 下同构于 $(\mathbb{Z}/d\mathbb{Z})^\times$，且 $(\mathbb{Z}/n\mathbb{Z})^\times = M \cdot N$，其中 $N = \ker(\pi)$。

对于 $n \in \mathbb{N}$ 和 $m \in \mathbb{Z}$，拉马努金和 $c_n(m)$（[Ram18] 或 [HSW00，第 179–199] 页）定义为

$$c_n(m) = \sum_{\substack{1 \le t < n, \\ (t,n)=1}} \zeta_n^{mt}$$

其中，ζ_n 是 $\mathbb{C}$ 中的本原 n 次单位根。在研究分圆多项式时，O. H¨older [H¨ol36] 证明了，和 $c_n(m)$ 可以用欧拉函数和 M¨obius 函数表示为一个优美的闭式。记 φ 欧拉 φ 函数， μ 记 M ¨obius 函数。我们在下面的引理中给出该公式，其中右侧也称为冯·斯特内克函数 [Ste03]。为方便读者，下面给出证明。关于其他证明，可参见 [AA53], [Mol52] 和 [HW08，定理 272]。

引理 3.2. 设 $n \in \mathbb{N}$ and $m \in \mathbb{Z}$。则

$$c_n(m) = \mu\left(\frac{n}{(n,m)}\right)\frac{\varphi(n)}{\varphi\left(\frac{n}{(n,m)}\right)}.$$

证明。首先，假设 $m = 1$。回顾一个初等公式：

$$\sum_{k|r}\mu(k) = \begin{cases} 1 & \text{if } r = 1; \\ 0 & \text{if } r > 0, \end{cases}$$

对于 $r \in \mathbb{N}$ ([Bur11，定理 6.6])。则

$$c_n(1) = \sum_{t=1}^{n}\zeta_n^t \sum_{k|(t,n)}\mu(k) = \sum_{k|n}\mu(k)\sum_{\substack{1\le t\le n,\\ k|(t,n)}}\zeta_n^t = \sum_{k|n}\mu(k)\sum_{1\le t'\le \frac{n}{k}}(\zeta_n^k)^{t'}$$

其中 $t' = tk$。由于 ζ_n^k是 1 的一个本原 nk 次根，最后一个和在 $k = n$ 时等于 1，在 $k < n$ 时等于 0。因此，$c_n(1) = \mu(n)$。

对于一般的 $m \in \mathbb{Z}$，我们将 $c_n(m)$ 改写为

$$c_n(m) = \sum_{t\in(\mathbb{Z}/n\mathbb{Z})^\times} z^t$$

其中 $z = \zeta_n^m$。设 $d = \frac{n}{(n,m)}$。回忆一下，$(\mathbb{Z}/n\mathbb{Z})^\times = M \cdot N$，其中 M 和 N 由引理 3.1 给出。注意，$z = \zeta_n^m$是 1 的本原 d 次单位根，因为 $\left(d, \frac{m}{(n,m)}\right) = 1$。因此，

$$c_n(m) = \sum_{t_1\in M}\sum_{t_2\in N} z^{t_1t_2} = \sum_{t_1\in M}|N|z^{t_1} = |N|c_d(1).$$

现在，由第一段可知，结论由 $|N| = \frac{\varphi(n)}{\varphi(d)}$ 以及 $c_d(1) = \mu(d)$ 得出。 □

注意，$(n, m) = (n, (n, m))$。因此，我们立即得到以下推论 e.

推论 3.3。设 $n \in \mathbb{N}$ 且 $m \in \mathbb{Z}$。那么 $c_n(m) = c_n((n, m))$。

因此，我们注意到，如果 m' 是一个整数，且 $m' \equiv m$（模 n），那么根据推论 3.3 可得 $c_n(m') = c_n(m)$。

下面的笛卡尔积分解有助于对整数对进行计数。粗略地说，下方的乘积被 $\mathbb{Z}\times\mathbb{Z}$ 上的平行线划分。

引理 3.4. 设 $n \in \mathbb{N}$ 且 $I = \{1, 2, \ldots, n-1\}$。对于每个 $a, b \in \mathbb{Z}$，有

$$I \times I = \biguplus_{d|n}\ \biguplus_{\substack{1\le t\le \frac{n}{d},\\ (t,\frac{n}{d})=1}} \{(x, y) \in I \times I \mid ax + by \equiv td \pmod{n}\}.$$

证明. 设 a,b $\in \mathbb{Z}$ 为两个固定整数，并设

$$S(d,t) = \{(x,y) \in I \times I \mid ax + by \equiv td \pmod{n}\}.$$

那么，对于所有这样的 d 和 t，S(d, t) 的并集是 I $\times$ I 的子集。这个并集确实包含 I $\times$ I 的所有元素。为说明这一点，令 (x, y) $\in$ I $\times$ I，并令 d $=$ (ax $+$ by, n)。取 1 $\leq$ t $\leq$ $\frac{n}{d}$，使得 t $\equiv$ $\frac{ax+by}{d}$ (mod $\frac{n}{d}$)。那么 (t, $\frac{n}{d}$) $=$ 1，且 ax $+$ by $\equiv$ td (mod n)。因此，(x, y) $\in$ S(d, t)。最后，如果 S(d, t) $\cap$ S(d′, t′) $\neq \varnothing$，那么在这个交集中取一对 (x, y)。我们得到 d $=$ (ax $+$ by, n) $=$ d′。此外，td $\equiv$ t′d (mod n) 意味着 t $\equiv$ t′ (mod $\frac{n}{d}$)。由于 $1 \leq t, t' \leq \frac{n}{d}$，我们有 t $=$ t′。□

4. 主要结果的证明

回顾一下，我们旨在证明以下和式

$$N(q,\ell) = \sum_{\substack{1 \leq t \leq q-1, \\ (t,q-1)=1}} N_{g^t}$$

不等于零，其中 g 是 $\mathbb{F}_q^{\times}$. 的一个固定生成元。显然，如果 $g^t L = g^s L$，那么 $N_{g^t} = N_{g^s}$。对于 N(q ℓ)，我们有如下约化。

命题 4.1. 设 g 是 $\mathbb{F}_q^{\times}$and $\ell \mid q - 1$ 的生成元。则

$$N(q,\ell) = \frac{\varphi(q-1)}{\varphi(\ell)} \sum_{\substack{1 \leq t \leq \ell, \\ (t,\ell)=1}} N_{g^t}.$$

证明。根据 N(q ℓ) 的定义，它是一个以 $(\mathbb{Z}/(q-1)\mathbb{Z})^{\times}$ 的所有元素为指标的和。回顾一下，$(\mathbb{Z}/(q-1)\mathbb{Z})^{\times} = M \cdot N$，其中 M 和 N 在 n $=$ q $-$ 1and d $=$ ℓ 时由引理 3.1 给出。注意，如果 $t_1 \in N$，则 $t_1 \equiv 1$ (模 ℓ) 且 $g^{t_1} L = gL$。因此，对于任意整数 t_2，$N_{g^{t_1 t_2}} = N_{g^{t_2}}$。于是，

$$N(q,\ell) = \sum_{t \in (\mathbb{Z}/(q-1)\mathbb{Z})^{\times}} N_{g^t} = \sum_{t_1 \in N} \sum_{t_2 \in M} N_{g^{t_1 t_2}} = |N| \sum_{t_2 \in M} N_{g^{t_2}}.$$

结论由此得出，因为 $|N| = \frac{\varphi(q-1)}{\varphi(\ell)}$ 且 $M \simeq (\mathbb{Z}/\ell\mathbb{Z})^{\times}$。 □

回顾式 (5),

$$N_{g^t} = q + \sum_{1 \leq j,k \leq \ell-1} \chi^j(-g^{-2t}) \chi^k(-g^{-t}) J(\chi^j, \chi^k)$$

其中 χ是 $\mathbb{F}_q$ 的一个非平凡特征，其阶为 ℓ。我们可以将 N_{g^t} 改写如下。

引理 4.2. 对于 $1 \leq t \leq \ell$ 和 (t ℓ) $=$ 1,

$$N_{g^t} = q + 1 + \sum_{\substack{1 \leq j,k \leq \ell-1, \\ j+k \neq \ell}} \chi(-1)^{j+k} \chi(g^{-1})^{(2j+k)t} J(\chi^j, \chi^k).$$

证明. 若 j $+$k $=\ell$，则由引理 2.2 的 (iv) 可得 J(χ^j,χ^k) $=-\chi(-1)^j$。由此可得

$$\sum_{\substack{1\le j,k\le \ell-1,\\ j+k=\ell}} \chi(-1)^{j+k}\chi(g^{-1})^{(2j+k)t}J(\chi^j,\chi^k) = -\sum_{j=1}^{\ell-1}\chi(-g^{-t})^j.$$

注意，χ 的核是 L。如果 $-g^{-t}\in$ L，那么 g^{-t}L $=-$L。这给出 $\ell=|\mathbb{F}_q^\times/L|\le 2$，因为 g^{-t}L 也生成 $\mathbb{F}_q^\times/$L，且 $1\le$t $\le\ell$ 和 (t, ℓ) $=1$。这不是我们的情形，因此$\chi(-g^{-t})\neq 1$.因此，$\sum_{j=1}^{\ell-1}\chi(-g^{-t})^j=-1$，结论得证。□

现在，我们可以证明主要定理了。

定理 4.3. 设 q 是一个素数的幂，且 ℓ是 q -1的真因子。如果

$$q \ge (2^{\omega(\ell)}(\ell-3-\delta)+2)^2-2$$

其中 $\omega(\ell)$ 是 ℓ 的不同的素因子的个数，并且

$$\delta=\begin{cases} 1 & \text{if } 4\mid\ell,\\ 0 & \text{otherwise,}\end{cases}$$

那么存在 $\mathbb{F}_q^\times$的一个生成元 g，使得 $N_g>0$.

证明。根据命题 4.1，只需考虑这个子和

$$N=\sum_{\substack{1\le t\le\ell,\\ (t,\ell)=1}} N_{g^t}$$

其中，g 是 $\mathbb{F}_q^\times$. 的一个固定生成元。引理 4.2 给出

$$N=\varphi(\ell)(q+1)+\sum_{\substack{1\le j,k\le\ell-1,\\ j+k\neq\ell}}\chi(-1)^{j+k}J(\chi^j,\chi^k)z(j,k) \quad \text{where}$$

$$z(j,k)=\sum_{\substack{1\le t\le\ell,\\ (t,\ell)=1}}\chi(g^{-1})^{(2j+k)t}.$$

注意，$\chi(g^{-1})=\zeta_\ell$ 是一个本原的 ℓ 次单位根。因此，

$$z(j,k)=\sum_{\substack{1\le t\le\ell,\\ (t,\ell)=1}}\zeta_\ell^{(2j+k)t}=c_\ell(2j+k),$$

是一个拉马努金和，并且

$$N=\varphi(\ell)(q+1)+\sum_{\substack{1\le j,k\le\ell-1,\\ j+k\neq\ell}}\chi(-1)^{j+k}J(\chi^j,\chi^k)c_\ell(2j+k).$$

令 I $=\{1,2,\ldots,\ell-1\}$，对于正整数 d $\mid\ell$以及满足 $1\le$t $\le\ell/$d 且 (t,d/ℓ) $=1$的整数 t，我们定义

$$S'(d,t)=\{(j,k)\in I\times I \mid 2j+k\equiv td \pmod{\ell} \text{ and } j+k\neq\ell\}.$$

删去 I ×I 中满足 j +k =ℓ的数对 (j, k) 后，由引理 3.4 可得

$$N-\varphi(\ell)(q+1)=\sum_{d|\ell}\sum_{\substack{1\le t\le \frac{\ell}{d},\\ (t,\frac{\ell}{d})=1}}\sum_{(j,k)\in S'(d,t)}\chi(-1)^{j+k}J(\chi^j,\chi^k)c_\ell(2j+k).$$

对于 (j, k) ∈S′(d,t)，由推论 3.3 可知 (2 j +k ℓ) =d，进而 cℓ(2 j +k) =cℓ(d)。因此，

$$N-\varphi(\ell)(q+1)=\sum_{d|\ell}c_\ell(d)f(d)$$

其中

$$f(d)=\sum_{\substack{1\le t\le \frac{\ell}{d},\\ (t,\frac{\ell}{d})=1}}\sum_{(j,k)\in S'(d,t)}\chi(-1)^{j+k}J(\chi^j,\chi^k).$$

我们需要估计 | f (d)|。

根据定义，S′(d,t) 中的每一对 (j, k) 都满足 j +k ≠0(mod ℓ)，因此由引理 2.2 的 (v) 可得 |J(χ^j,χ^k)| =√q。由于 |χ(−1)| = 1，所以

$$|f(d)|\le\sum_{\substack{1\le t\le \frac{\ell}{d},\\ (t,\frac{\ell}{d})=1}}|S'(d,t)|\sqrt{q}.$$

现在，我们计算 |S′(d, t)|。注意，S′(d, t) 中的每一对 (j, k) 都由满足 j ∈I 的 j 确定，条件是 j +k ≠ℓ. 因此，对于满足同余式 2 j +k ≡td (mod ℓ) 的 (j, k) ∈I × I，我们必须排除 j ≡td (mod ℓ) 的情形。注意，td ≤ℓ而 j ≤ℓ−1 时，该同余式只有在 d ≨ℓ且 j =td 时才可能成立。此外，由于 k ≠0，我们还需要排除 2 j ≡td (mod ℓ) 的情形。这取决于 ℓ的奇偶性。为避免混淆，我们将在下一段中讨论。

设 ℓ为奇数。令 s ∈I 满足 2s ≡1 (mod ℓ)。于是，我们需要排除满足 j ≡ std (mod ℓ) 的 j ∈I。若 d =ℓ，则不存在这样的 j，因为 j ≠0 (mod ℓ)。当 d ≨ℓ, 时，恰有一个 j0 ∈I 满足 j0 ≡std (mod ℓ)。请记住，我们还必须排除 j =t d 的情形。因此，若 ℓ为奇数，则

$$|S'(d,t)|=\begin{cases}|I| & \text{if } d=\ell;\\ |I|-2 & \text{if } d\neq\ell.\end{cases}$$

现在假设 ℓ为偶数。需要考虑三种情况：(i) td 为奇数；(ii) td 为偶数且 d ≨ℓ；(iii) t =1，d =ℓ。对于情况 (i)，由于 td 为奇数，不存在满足 2 j ≡td (mod ℓ) 的 j。只需排除 j =td 的情况。对于 (ii) 和 (iii)，有 td 为偶数，因此存在某个 j1 ∈I，使得 2 j1 ≡td (mod ℓ)。事实上，我们有 j1 ≡td2 (mod ℓ/2)。如果 d ≨ℓ, ，那么 j1 = td2 或 j1 = td/2 + ℓ/2，特别地，在这种情况下 j1 ≠td。如果 d =ℓ，那么 t =1 且 j1 = ℓ/2。我们得出结论：

$$|S'(d,t)|=\begin{cases}|I|-1 & \text{if } d=\ell;\\ |I|-1 & \text{if } d\neq\ell \text{ and } td \text{ is odd};\\ |I|-3 & \text{otherwise.}\end{cases}$$

结合 ℓ 的这两种情况，可得 $|S'(d,t)|$ 的表达式如下。

$$|S'(d,t)| = |I| - 2 + 2\left\lfloor \frac{d}{\ell} \right\rfloor - (-1)^{td}\lambda = |I| - 2 + 2\left\lfloor \frac{d}{\ell} \right\rfloor - (-1)^{d}\lambda$$

其中 $\lambda = \frac{1}{2}(1+(-1)^{\ell})$，并注意到当 ℓ 为偶数时，$td \equiv d \pmod 2$，因为 $(t, \frac{\ell}{d}) = 1$。特别地，$|S'(d,t)|$ 与 t 无关。因此，

$$|f(d)| \le \varphi\left(\frac{\ell}{d}\right)\left(|I| - 2 + 2\left\lfloor \frac{d}{\ell} \right\rfloor - (-1)^{d}\lambda\right)\sqrt{q}$$

and

$$\begin{aligned} |N - \varphi(\ell)(q+1)| &\le \sum_{d|\ell} |c_\ell(d) f(d)| \\ &\le \sum_{d|\ell} |c_\ell(d)| \varphi\left(\frac{\ell}{d}\right)\left(|I| - 2 + 2\left\lfloor \frac{d}{\ell} \right\rfloor - (-1)^{d}\lambda\right)\sqrt{q}. \end{aligned}$$

由引理 3.2，得 $c_\ell(d)\varphi(\frac{\ell}{d}) = \mu(\frac{\ell}{d})\varphi(\ell)$。将 $\varphi(\ell)$ 相除，得到

$$\left|\frac{N}{\varphi(\ell)} - (q+1)\right| \le \sum_{d|\ell}\left|\mu\left(\frac{\ell}{d}\right)\right|\left(|I| - 2 + 2\left\lfloor \frac{d}{\ell} \right\rfloor - (-1)^{d}\lambda\right)\sqrt{q}.$$

注意，若 $\frac{\ell}{d}$ 无平方因子，则 $|\mu(\frac{\ell}{d})| = 1$；否则，$|\mu(\frac{\ell}{d})| = 0$。观察可知，使 $\frac{\ell}{d}$ 无平方因子的 d 的个数为 $2^{\omega(\ell)}$。此外，

$$\sum_{\substack{d|\ell, \\ \mu(\frac{\ell}{d})\neq 0}} (-1)^{d}\lambda = 2^{\omega(\ell)}\delta.$$

由此可得

$$\left|\frac{N}{\varphi(\ell)} - (q+1)\right| \le \left(2^{\omega(\ell)}(|I| - 2 - \delta) + 2\right)\sqrt{q}.$$

因此，若 $q + 1 > (2^{\omega(\ell)}(|I| - 2 - \delta) + 2)\sqrt{q}$，则可得 $N > 0$。将 $\sqrt{q}$ 相除并将两边平方，最后一个不等式等价于

$$q + 2 + \frac{1}{q} > (2^{\omega(\ell)}(|I| - 2 - \delta) + 2)^2 = (2^{\omega(\ell)}(\ell - 3 - \delta) + 2)^2.$$

两边除 $\frac{1}{q}$ 之外的所有项都是整数，且 $\frac{1}{q} < 1$。结论得证。 □

推论 4.4. 若 q 模 5 同余于 1，则对于某个 $\mathbb{F}_q$ 的原根 g，$g^2X^5 + gY^5 + 1 = 0$ 在 $\mathbb{F}_q$ 中有解。

证明. 根据定理 4.3，当 $q \ge 34$ 时结论成立。对于 $q < 34$ 和 $q \equiv 1$（模 5），有 $q = 11$、16、31。对于 $q = 11$，有 $g = 7$ 和 $7^2 \cdot (-1)^5 + 7 \cdot (-1)^5 + 1 = 0$。对于 $q = 16$，有 $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$，其中 $\alpha^4 = 1 + \alpha$ 和 $\mathbb{F}_{16}^{\times} = \langle\alpha\rangle$。此外，$\alpha^2 \cdot (\alpha^2)^5 + \alpha \cdot (\alpha^2)^5 + 1 = 0$。对于 $q = 31$，有 $g = 3$ 和 $3^2 \cdot (-3)^5 + 3 \cdot 3^5 + 1 = 0$。□

推论 4.5. 若 q 模 6 同余于 1，则对于某个 $\mathbb{F}_q$ 的原根 g，$g^2X^6 + gY^6 + 1 = 0$ 在 $\mathbb{F}_q$ 中有解，当且仅当 $q > 13$。

证明。根据定理 4.3，结论对 $q \geq 194$ 成立。对于 $q < 194$ 和 $q \equiv 1$（模 6），我们先考察 $q = 7$ 和 $q = 13$。当 $q = 7$ 时，对所有 $x \in \mathbb{F}_7^\times$，都有 $x^6 = 1$。但对于任意 $\mathbb{F}_7$ 的原根 g，$g^2 + g + 1 \neq 0$。因此，这种情况下无解。当 $q = 13$ 时，对所有 $x \in \mathbb{F}_{13}^\times$，都有 $x^6 = \pm 1$。容易验证，对于 $\mathbb{F}_{13}$ 的所有原根 $g = 2$、6、7、11，$g^2X^6 + gY^6 + 1 = 0$ 无解。对于其余满足 $13 < q < 194$ 的情况，下表给出了某个原根 g 的一个解：

q	19	25	31	37	43	49	61	67	73	79	97	103	
g	2	α	3	2	3	β	2	2	5	3	5	5	
X	1	α^3	19	2	1	β^3	24	4	1	6	5	5	
Y	2	α	27	1	28	β^3	4	43	59	6	29	32	

q	109	121	127	139	151	157	163	169	181	193
g	6	γ	3	2	6	5	2	κ	2	5
X	16	γ^7	84	2	1	22	8	1	86	1
Y	26	γ^4	3	103	132	82	1	κ^2	148	127

其中 $\alpha = 3 + \sqrt{2}$ 属于 $\mathbb{F}_{25} = \mathbb{F}_5(\sqrt{2})$，$\beta = 4 + \sqrt{-1}$ 属于 $\mathbb{F}_{49} = \mathbb{F}_7(\sqrt{-1})$，$\gamma = 2 + \sqrt{2}$ 属于 $\mathbb{F}_{121} = \mathbb{F}_{11}(\sqrt{2})$，且 $\kappa = 7 + 2\sqrt{2}$ 属于 $\mathbb{F}_{169} = \mathbb{F}_{13}(\sqrt{2})$。□

5. 应用：重量为 3 的冲突避免码

本节将主要结果应用于冲突避免码的构造。我们考虑特殊情形：$q = p$，且 $\ell = \ell_0$ 为 H 在 $\mathbb{F}_p^\times$. 中的指标。下面先证明推论 B。

证明。设 p 为一个素数，使得 2 的乘法阶 $o_p(2)$ 不是 4 的倍数。假设 p 满足条件

$$p \geq (2^{\omega(\ell_0)}(\ell_0 - 3 - \delta) + 2)^2 - 2$$

其中，当 $4 \mid \ell_0$ 时 $\delta = 1$，否则 $\delta = 0$。由定理 A 可知，存在 $\mathbb{F}_p^\times$ 的一个生成元 g，使得方程 (2) 在 $\mathbb{F}_p$. 上有解。根据 $1 \leq \ell_0 \leq 4$ 的推论 2.3 和 $\ell_0 \geq 5$ 的引理 2.1，可知存在方程 (2) 的一个解 $(x, y) \in \mathbb{F}_p^2$，满足 $xy \neq 0$.。因此，对于满足上述不等式的素数 p，猜想 C 及猜想 B 均成立。正如第 1 节所述，猜想 A 对这些素数也成立。结合 [FLS14], 中给出的算法，我们得出长度为 p、重量为 3 的最优冲突避免码的大小为

$$M(p, \ell_0) = \frac{p - 1 - 2\ell_0}{4} + \left\lfloor \frac{\ell_0}{3} \right\rfloor$$

如所期望的那样。□

我们研究素数长度最优冲突避免码的规模时，采用的策略是考察猜想 B（等价地，猜想 C）。在论文 [MZS14] 中，作者

宣布猜想 B 已被验证对素数 $p \le 2^{30}$成立。应用推论 B，我们能够扩展猜想 B 成立的素数 p 的范围。对于 $\ell \in \mathbb{N}$，令

$$b(\ell) = (2^{\omega(\ell)}(\ell - 3 - \delta) + 2)^2 - 2$$

为定理 A 中出现的下界。设 p 是一个素数，使得 H 在 $\mathbb{F}_p^\times$ 中的指标 ℓ_0 满足 b(ℓ_0) $\le 2^{30}$，则 $p \le 2^{30}$ 或 $p > 2^{30} \ge b(\ell_0)$。由此可知，猜想 C 对这个素数 p 成立。这引出了关于整数 ℓ 满足 $b(\ell) \le 2^{30}$. 的问题。答案取决于 ℓ. 的不同素因子个数。对于 $\omega(\ell) < 4$，可以验证，若满足以下条件之一，则 $b(\ell) \le 2^{30}$：

$$\begin{cases} \ell < 16411 \text{ with } \omega(\ell) = 1, \\ \ell < 8197 \text{ with } \omega(\ell) = 2, \\ \ell < 4100 \text{ with } \omega(\ell) = 3. \end{cases}$$

此外，只要 $\ell < 2070$，也有 $b(\ell) \le 2^{30}$。因此，我们得到以下结果。

定理 5.1. 对于满足以下任一条件的素数 p，猜想 C 成立： ℓ_0

$$\begin{cases} \ell_0 < 16411 \textit{ with } \omega(\ell_0) = 1, \\ \ell_0 < 8197 \textit{ with } \omega(\ell_0) = 2, \\ \ell_0 < 4100 \textit{ with } \omega(\ell_0) = 3, \\ \ell_0 < 2070. \end{cases}$$

对于满足 $b(\ell) > 2^{30}$ 的整数 ℓ，我们考察介于2^{30} 与 b(ℓ)之间的素数集合。令

$$P(\ell) = \left\{\text{primes } p > 2^{30} \mid [\mathbb{F}_p^\times : \langle -1, 2\rangle] = \ell \text{ and } p < b(\ell)\right\}.$$

对于 P(ℓ) 中的素数，我们借助计算机进行计算，以验证猜想 C。例如，我们得到 P(2070) $= \varnothing$，因此对于满足 $\ell_0 = 2070.$ 的素数 p，猜想 C 成立。通过计算机搜索，对于 $2070 \le \ell \le 3000$，P(ℓ) 的并集中共有 423 个素数。该并集中的最大素数是 7324065841，且$\ell = 2730.$。我们已验证猜想 C 对这些素数成立。

定理 5.2. 对于满足 $[\mathbb{F}_p^\times : \langle -1、2\rangle] \le 3000$ 的素数 p，猜想 C 成立。

关于方程（3）的可解性，我们有如下简单观察。

命题 5.3. 设 ℓ 是 $q - 1$ 的真因子，且 $\ell' \mid \ell.$。假设方程（3）在 $\mathbb{F}_q$ 上对于指数 ℓ 可解，那么对于指数 ℓ' 也可解。

命题 5.3 对 q = p（一个素数）以及方程（3）中的p_2^{-1} 给出了如下考量。在这种~~情~~况下，L $= \{\pm 1\}$，因此只需考虑四种可能性 $\pm g^2 \pm g + 1 = 0$，其中 g $\in \mathbb{N}$ 是模 p 的原根（即 g 是 $\mathbb{F}_p^\times$的生成元）。显然，$g^2 \pm g + 1 = 0$ 当且仅当 $g^3 = \pm 1$，此时 $p - 1 = 3, 6$。

这对 $p = 7$ 和 $g = 3$成立。其余两种情况 $-g^2 \pm g + 1 = 0$ 等价，因为 $-g^2 + g + 1 = 0$ 当且仅当 $-g^{-2} - g^{-1} + 1 = 0$。换句话说，我们只需考虑在 $\mathbb{F}_p$上等式 $g^2 = g + 1$。这样的原根 g 称为模 p 的斐波那契本原根，因为黄金比例 φ_{gr} 满足 $\varphi_{gr}^2 = \varphi_{gr} + 1$。使得 $\mathbb{F}_p$ 具有斐波那契本原根的素数 p 构成数列 A003147：5, 11, 19, 31, 41, 59, 61, 71, 79, 109, . . .，见在线整数数列百科全书 [Slo]。因此，$N(p, (p-1)/2) > 0$ 当且仅当 $\mathbb{F}_p$ 具有斐波那契本原根。另一方面，子群 $H = \langle -1, 2 \rangle$ 的阶 $|H|$ 是偶整数。因此，$\ell_0 = p^{-1} \bmod |H|$必须整除 p_2^{-1}。由命题 5.3 可知，若 $\mathbb{F}_p$ 具有斐波那契本原根，则方程 (2) 在 $\mathbb{F}_p$ 上有解。在这种情况下，存在一个解 $(x, y) \in \mathbb{F}_p^2$，使得 $xy \neq 0$，因此猜想 C 成立。

Pro位置 5.4. 如果 $\mathbb{F}_p$ 有斐波那契本原根，则猜想 C 对此 p 成立 .

关于一个相关问题，对于上文证明的猜想 C 中成立的情形，我们想知道有多少个素数 p，使得由-1 和 2 生成的子群 H 在 $\mathbb{F}_p^\times$中的指标为 ℓ_0。这个问题可以视为阿廷本原根猜想的推广。根据广义黎曼猜想（GRH），[Mur91，定理 1] 证明了存在无穷多个素数 p，使得指标 $[\mathbb{F}_p^\times : H] = \ell_0$。假设 GRH 成立，由推论 B 可得，存在无穷多个素数 p，使得 ℓ_0 满足定理 5.2 中的条件，因此，对于无穷多个素数 p，素数长度的最优冲突避免码的大小等于 $M(p, \ell_0)$。

致谢

我们感谢 Yuan-Hsun Lo 教授让我们注意到 [FLS14]。第一作者部分由 MOST 资助项目 110-2115-M-003-007-MY2 提供支持。第二作者部分由 MOST 资助项目 111-2115-M-003-005 提供支持。第三作者由 MOST 资助项目 110-2811-M-003-530 提供支持。

参考文献

[AA53] D.R. Anderson 和 T.M. Apostol. 拉马努金和及其推广的求值。《杜克数学杂志》，20(2):211–216，1953。doi:10.1215/S0012-7094-53-02021-3.[Bur11] D.M. Burton.《初等数论》。麦格劳-希尔，纽约，2011。[FLM10] H.-L. Fu、Y.-H. Lin 和 M. Mishima. 偶数长度、重量 3 的最优冲突避免码。《IEEE信息论汇刊》，56(11):5747–5756，2010。doi:10.1109/TIT.2010.2069270.[FLS14] H.-L. Fu、Y.-H. Lo 和 S.W. Shum. 奇数长度、重量三的最优冲突避免码。《设计、码与密码学》，72(2):289–309，2014。doi:10.1007/s10623-012-9764-5.[GV93] L. Gy¨orfi 和 I. Vajda. 无反馈多址碰撞信道协议序列的构造。《IEEE信息论汇刊》，39(5):1762–1765，1993。doi:10.1109/18.259673.[Har77] R. Hartshore.《代数几何》，《数学研究生教材》第 52 卷。Springer，纽约，1977。doi:10.1007/978-1-4757-3849-0。

[HLS] L.-C. Hsia、H.-C. Li 和 W.-L. Sun. 素数长度的冲突避免码与分圆数。预印本。[H¨ol36] O. H¨older. 关于圆分方程 $K_m(x) = 0$的理论。（德语）Prace Matematyczno-Fizyczne, 43(1):13–23，1936。网址：http://eudml.org/doc/215570.[HSW00] G.H. Hardy、P.V. Seshu Aiyar 和 B.M. Wilson，编。《斯里尼瓦瑟·拉马努金论文集》。AMS Chelsea Publishing，普罗维登斯，RI，2000。1927 年原版的第三次印刷。附有 B.C. Berndt 撰写的新序言和评注。[HW08] G.H. Hardy 和 E.M. Wright.《数论导论》。牛津大学出版社，牛津，第六版，2008。由 D.R. Heath-Brown 和 J. Silverman 修订。附有 A. Wiles 撰写的序言。[JMJ+07] M. Jimbo、M. Mishima、S. Janiszewski、A.Y. Teymorian 和 V.D. Tonchev. 关于长度为 $n = 4m$、供三名活跃用户使用的冲突避免码。《IEEE信息论汇刊》，53(8):2732–2742，2007。doi:10.1109/TIT.2007.901233.[Lev07] V.I. Levenshtein. 冲突避免码与循环三元系。《问题信息传输》，43(3):199–212，2007。doi:10.1134/S0032946007030039.[LMSJ14]Y. Lin、M. Mishima、J. Satoh 和 M. Jimbo. 奇数长度、重量三的最优等差冲突避免码。《Finite Fields Appl.》，26:49–68，2014。doi:10.1016/j.ffa.2013.11.001.[LN97] R. Lidl 和 H. Niederreiter.《有限域》，《数学及其应用百科全书》第 20 卷。剑桥大学出版社，剑桥，第二版，1997。doi:10.1017/CBO9780511525926.[LT05] V.I. Levenshtein 和 V.D. Tonchev. 供三名活跃用户使用的最优冲突避免码。IEEE 国际信息论研讨会论文集，第 535–537 页，2005。doi:10.1109/ISIT.2005.1523392.[Mat90] P. Mathys. 一类供 t 名活跃用户（共 n 名用户）使用的多址通信系统编码。《IEEE信息论汇刊》，36(6):1206–1219，1990。doi:10.1109/18.59923.[MFU09]M. Mishima、H.-L. Fu 和 S. Uruno. 长度为 $n \equiv 0$ （模 16）、重量 3 的最优冲突避免码。《设计、码与密码学》，52(3):275–291，2009。doi:10.1007/s10623-009-9282-2.[MM17] M. Mishima 和 K. Momihara. 一系列新的重量 3 最优紧冲突避免码。《离散数学》，340(4):617–629，2017。doi:10.1016/j.disc.2016.12.003.[Mol52] R. Moller. 模素数、具有给定指数的数的幂和。《美国数学月刊》，59(4):226–230，1952。另附 H.S. Zuckerman 的补充评注。doi:10.1080/00029890.1952.11988111.[Mom07]K. Momihara. 重量三的紧等差冲突避免码的充要条件。《设计、码与密码学》，45(3):379–390，2007。doi:10.1007/s10623-007-9139-5.[Mur91] L. Murata. 一个与原根的阿廷猜想类似的问题及其应用。《数学文献》，57(6):555–565，1991。doi:10.1007/BF01199060.[MZS14]W. Ma、C. Zhao 和 D. Shen. 奇数长度、重量 3 的新型最优冲突避免码构造。《设计、码与密码学》，73(3):791–804，2014。doi:10.1007/s10623-013-9827-2.[NGM92] Q.A. Nguyen、L. Gy¨orfi 和 J.L. Massey. 二元定重循环码与循环可置换码的构造。《 IEEE 信息论汇刊》，38(3):940–949，1992。doi:10.1109/18.135636.[Ram18] S. Ramanujan. 关于某些三角和及其在数论中的应用。《剑桥哲学学会汇刊》，22(13):259–276，1918。

[Slo] N.J.A. Sloane。OEIS基金会（2023），在线整数数列百科全书，电子版发布于 http://oeis.org。.[Ste03] R.v. Sterneck。关于加法数论的一个类似物。（德语）《德国数学家协会年报》，12:110–113，1903。网址：http://eudml.org/doc/144877。[TR02] B.S. Tsybakov 和 A.R. Rubinov。冲突避免码的一些构造。《问题信息传输》，38(4):268–279，2002。doi:10.1023/A:1022045812079。[Wei48] A. Weil。《关于代数曲线及由其导出的簇》。Hermann，1948。[WF13] S.-L. Wu 和 H.-L. Fu。长度为 n $=2^k\pm1$、重量为 3 的最优紧等差冲突避免码。《组合设计杂志》，21(6):223–231，2013。doi:10.1002/jcd.21332。国立台湾师范大学数学系，台北 11677，台湾，中华民国。电子邮箱：hsia@math.ntnu.edu.tw 国立台湾师范大学数学系，台北 11677，台湾，中华民国。电子邮箱：li@math.ntnu.edu.tw 国立台湾师范大学数学系，台北 11677，台湾，中华民国。电子邮箱：wlsun@ntnu.edu.tw