

参赛学生姓名：曾德烨

中学：福建省南平第一中学

省份：福建省

国家/地区：南部赛区

指导老师姓名：包文涛

指导老师单位：福建省南平第一中学

论文题目：一类增广梅森数的若干初步结论
和猜想

一类增广梅森数的若干初步结论和猜想

福建省南平第一中学 曾德烨

摘要

本文令 $F(a, p) = \frac{a^p - 1}{a - 1}$ 作为梅森数的一类增广，得到以下有关互素性、代数

恒等式、因子形式等初步结论：

$F(a, m)$ 与 $a - 1$ 互素，当且仅当 $\forall p \mid m, a \bmod p \neq 1$ ；

当 p 为奇素数且 $a \bmod p \neq 1$ ，那么 $F(a, p) = \frac{a^p - 1}{a - 1}$ 的全体因子均具有 $2np + 1$

的形式，其中 $n \in \mathbb{N}$ ；

若 $F(a, p) = b^k$ ，则 $k \neq p - 1$ 。

并提出以下猜想：

对任意非幂整数 a ，存在无穷多个素数 p ，使 $F(a, p)$ 取得素数；

固定奇素数 p ，设 $\pi_p(z) = \#\{z \leq a \leq z^2 - 1 : F(a, p) \in P\}$ ，则

$$\pi_p(z) \sim \frac{z^2}{2(p-1)\ln z}, z \rightarrow \infty;$$

若 $p \in P$ 且 $p \neq 2$ ，当且仅当 $a = 3, p = 5$ 或 $a = 18, p = 3$ ， $F(a, p)$ 为完全幂方数。
以及指明其在密码学上的应用。

本成果入选 2026 年国际基础科学大会高中生学术海报展（全球仅 56 项）。

关键词：梅森数，增广梅森数，广义梅森数，完全幂方，费马小定理，艾森斯坦判据，Zsigmondy 定理，素数定理，Nagel-Ljunggren 猜想，Bunyakovsky 猜想

目 录

1 前言	3
2 引理	3
3 简单结论	4
3.1 关于 $F(a, p)$	4
3.2 关于 $F(a, m)$	8
3.3 关于 $F(a^{p^n}, q)$	9
4 关于 $F(a, p)$ 的猜想和讨论	11
4.1 关于素性检验	11
4.2 关于猜想二	13
4.3 关于完全幂方问题	12
5 致谢	14

1 前言

梅森素数的研究已经相当成熟且精深。不过，在形式上的另辟蹊径似乎恰好值得钻研。从梅森数的定义出发，我思考的开始是：

令 $a, p \in \mathbb{N}^*, a \neq 2, a^p - 1 = q$ 在何种情况下取得素数？

由于 $a^p - 1 = (a - 1) \cdot \sum_{i=0}^{p-1} a^i$ ，它在 $a > 2$ 时总不是素数。那么将此式除去 $a - 1$ ，

能否取得素数？定义 $F(a, p) = \frac{a^p - 1}{a - 1}$ ，并提出以下问题：

$\forall p \in P, p \neq 2, \forall a \bmod p \neq 1, F(a, p)$ 中素数的存在性：

$p \in P, a \bmod p \neq 1, F(a, p)$ 因子的特征和分布的情况。

2 引理和符号说明

引理 1 费马小定理： $p \in P, \forall a \in \mathbb{N}, a^p \equiv a \pmod{p}$ 。

引理 2 艾森斯坦判据： $F(x) := \{a_0 + a_1x + \dots + a_nx^n \mid n \in \mathbb{N}^*, \forall a_i \in \mathbb{Z}\}, f(x) \in F(x)$,

若 $\exists p \in P, \begin{cases} a_n \bmod p \neq 0 \\ a_i \bmod p = 0, i \neq n \\ a_0 \bmod p^2 \neq 0 \end{cases}$ ，则 $f(x)$ 在 $F(x)$ 上不可约。

引理 3 Zsigmondy 定理： 任意 $n \geq 2, a^n - b^n$ ，若存在 $a^n - b^n$ 的素因子 p ，使得 p 不整除任何 $a^k - b^k (1 \leq k < n)$ ，则称 p 为 $a^n - b^n$ 的本原素因子。对互素整数 $a, b (a > b)$ ，除特定反例外。对任意 $n \geq 2, a^n - b^n$ 至少有一个本原素因子。

仅有的特定反例：

1. $n = 2$ ，且 $a + b$ 是 2 的幂；

2. $n = 6$ ，且 $a = 2, b = 1$ 。

引理 4 Ljunggren 定理: 方程 $\frac{x^n-1}{x-1} = y^q$ 在 q 为偶数, 即函数 $\frac{x^n-1}{x-1}$ 为偶次幂数, 唯有两解 $x=3, n=5$ 和 $x=7, n=4$

引理 5 素数定理: 令 $\pi(x)$ 表示不超过 x 的素数个数, 则当 $x \rightarrow \infty$ 时, $\pi(x) \sim \frac{x}{\ln x}$, 等价地, $\pi(x) \sim Li(x) = \int_2^x \frac{dt}{\ln t}$, 后者近似精度更高.

引理 6 LET 引理: 若 p 是奇素数, $p|(a-b)$, 且 $p \nmid ab$, 则对任意正整数 n :

$$v_p(a^n - b^n) = v_p(a-b) + v_p(n), \quad v_p(x) \text{ 表示 } x \text{ 中质因数 } p \text{ 的个数.}$$

符号说明 1: 记素数集为 P

符号说明 2: 记广义梅森数 $\frac{a^p-1}{a-1}$ 为 $F(a, p) = \sum_{i=0}^{p-1} a^i = \Phi_p(a)$

本文还需要借助以下猜想:

Nagell-Ljunggren 猜想: Nagell-Ljunggren 方程 $\frac{x^n-1}{x-1} = y^q$ (其中 $x > 1, y > 1, n > 2, q \geq 2$ 均为整数), 截至目前, 该方程在 $n \geq 2$ 时, 已知只有 3 个解,

$$\begin{cases} x=3, n=5, y=11, q=2 \\ x=7, n=4, y=20, q=2 \\ x=18, n=3, y=7, q=3 \end{cases}, \text{ 但有限性仍是开放问题}$$

Bunyakovsky 猜想: 若整系数多项式满足首项为正, 不可约且无固定素因子, 则其代入整数时能产生无穷多个素数. 然而, 该猜想至今未被证明.

3 简单结论

首先, $F(a, p) = \frac{a^p-1}{a-1} = \Phi_p(a) = \sum_{i=0}^{p-1} a^i$, 对于 a, p 都为单调递增数列, 证明如下:

对于 a , 有 $F(a+1, p) - F(a, p) = \sum_{i=0}^{p-1} (a+1)^i - \sum_{j=0}^{p-1} a^j = \sum_{i=0}^{p-1} (a+1)^i - a^i > 0$, 得 $F(a, p)$ 对于 a 都为单调递增数列

对于 p , 有 $F(a, p+1) - F(a, p) = \frac{a^{p+1}-1}{a-1} - \frac{a^p-1}{a-1} = \frac{a^{p+1}-a^p}{a-1} = a^p > 0$, 得 $F(a, p)$ 对于

p 都为单调递增数列

3.1 关于 $F(a, p)$

结论 3.1.1 $F(a, m)$ 与 $a-1$ 互素, 当且仅当 $\forall p|m, a \bmod p \neq 1$.

证明: 若要证明结论 3.1.1, 还需借助引理 1

引理 1: 对于任意整数 $n \geq 1$, 有 $(\frac{a^n - 1}{a - 1}, a - 1) = (n, a - 1)$

引理 1 证明:

因为 $a \equiv 1 \pmod{a-1}$, 则 $a^{n-1} \equiv 1^{n-1} \equiv 1 \pmod{a-1}$, 所以

$$\frac{a^n - 1}{a - 1} = \sum_{i=0}^{n-1} a^i \equiv \sum_{i=0}^{n-1} 1 \equiv n \pmod{a-1}, \text{ 即 } \frac{a^n - 1}{a - 1} = n + k(a - 1). \text{ 于是:}$$

$$(\frac{a^n - 1}{a - 1}, a - 1) = (n + k(a - 1), a - 1) = (n, a - 1), \text{ 引理 1 得证.}$$

由引理 1, 原式变为: $(\frac{a^m - 1}{a - 1}, a - 1) = (m, a - 1)$

则问题等价于:

$(m, a - 1) = 1$, 当且仅当 $\forall p|m, a \bmod p \neq 1$.

充分性: 当 $\forall p|m, a \bmod p \neq 1$, 如果 $(m, a - 1) > 1$, 则存在素数 p , 使得 $p|m, p|a - 1$, 即 $p|m, a \equiv 1 \pmod{p}$, 矛盾. 所以 $(m, a - 1) = 1$.

必要性: 当 $(m, a - 1) = 1$, 假设存在素数 $p|m$, 使得 $a \equiv 1 \pmod{p}$, 则 $p|a - 1$, 所以 $p|(m, a - 1)$, 与 $(m, a - 1) = 1$ 矛盾.

由上, 命题得证.

结论 3.1.2 $F(a, p), F(a, q)$ 互素, 当且仅当 p, q 互质.

证明: 必要性: 由于

$$F(a, p) = F(a, (p, q)) \cdot F\left(a^{(p, q)}, \frac{p}{(p, q)}\right) \text{ 与}$$

$$F(a, q) = F(a, (p, q)) \cdot F\left(a^{(p, q)}, \frac{q}{(p, q)}\right),$$

又因为 $F(a, p)$ 关于 a, p 单调递增, 所以若 $F(a, p) F(a, q)$ 与互素, 则

$$F(a, (p, q)) = 1, \text{ 即 } (p, q) = 1$$

充分性:

令 $(p, q) = 1$, 则 $\exists s, t \in N^*$, 使得 $ps - qt = 1$. 有

$$((a-1) \cdot F(a, p), (a-1) \cdot F(a, q)) = (a-1, (a-1) \cdot M(a, q)) = a-1,$$

即 $(F(a, p), F(a, q)) = 1$. 命题得证

结论 3.1.3 $(F(a, p), F(a, q)) = F(a, (p, q))$.

证明: 由于

$$F(a, p) = F(a, (p, q)) \cdot F\left(a^{(p, q)}, \frac{p}{(p, q)}\right) \text{ 与}$$

$$F(a, q) = F(a, (p, q)) \cdot F\left(a^{(p, q)}, \frac{q}{(p, q)}\right),$$

又因为 $F(a, p)$ 关于 a, p 单调递增, 所以 $(F(a, p), F(a, q)) = F(a, (p, q))$.

命题得证.

结论 3.1.4 $F(a, p) | F(a^q, p)$, 其中 $q \in N^*$.

证明:

令

$$Y = F(a, p) = \frac{a^p - 1}{a - 1} = \sum_{i=0}^{p-1} a^i,$$

$$X = F(a^q, p) = \frac{a^{pq} - 1}{a^q - 1} = \sum_{i=0}^{p-1} a^{iq}.$$

由 Y 的定义, 得

$$a^p - 1 = (a - 1) \cdot Y$$

所以

$$a^p \equiv 1 \pmod{Y}$$

于是对任意非负整数 k , 将指数模 p 约化:

$$a^k = a^{p[k/p] + (k \bmod p)} = (a^p)^{[k/p]} \cdot a^{k \bmod p} \equiv a^{k \bmod p} \pmod{Y}$$

因此

$$X = \sum_{i=0}^{p-1} a^{iq} \equiv \sum_{i=0}^{p-1} a^{iq \bmod p} \pmod{Y}$$

因为 $(p, q) = 1$, 当 i 遍历 $0, 1, 2, \dots, p-1$ 时, $iq \bmod p$ 也恰好遍历 $0, 1, 2, \dots, p-1$ 每个值, 所以

$$\sum_{i=0}^{p-1} a^{iq \bmod p} = \sum_{j=0}^{p-1} a^j = Y \equiv 0 \pmod{Y}$$

因此 $X \equiv 0 \pmod{Y}$

$$\text{即 } \frac{a^p - 1}{a - 1} \mid \frac{a^{pq} - 1}{a^q - 1}$$

命题得证。

结论 3.1.5 设 $p \in \{x \in \mathbb{P} \mid x \neq 2\}, n \in \mathbb{N}^*$, 若 $a \bmod p \neq 1$, 则 $F(a, p)$ 的 q 任意素因子 q 均满足 $q \equiv 1 \pmod{2p}$, 即 q 具有 $2np + 1$ 的形式. 进而, $F(a, p)$ 的全体正因子均具有 $2np + 1$ 的形式.

证明:

设 q 为 $F(a, p)$ 的任一素因子.

设 q 为素数且 $q \nmid a$. 称最小的正整数 t 使得 $a^t \equiv 1 \pmod{q}$ 为 a 模 q 的阶, 记作 $\text{ord}_q(a)$.

因为 $a \bmod p \neq 1$, 由结论 3.1.1, $(a-1, F(a, p)) = 1$, 故 $q \nmid a-1$. $a \equiv 1 \pmod{q}$, 所以 a 模的阶 $\text{ord}_q(a)$ 由定义且 $\text{ord}_q(a) > 1$. 由 $q \mid F(a, p)$ 得 $q \mid \frac{a^p - 1}{a - 1}$, 又因为 $q \nmid a-1$, 故 $q \mid a^p - 1$, 即 $a^p \equiv 1 \pmod{q}$. 因此 $\text{ord}_q(a) \mid p$. 由于 p 是素数, 所以 $\text{ord}_q(a) = 1$ 或 p . 又因为 $\text{ord}_q(a) > 1$, 故 $\text{ord}_q(a) = p$.

由费马小定理, $\text{ord}_q(a) \mid q-1$, 因此 $p \mid q-1$ (1). 因为 $F(a, p) = 1 + a + \dots + a^{p-1}$, 则:

若 a 为偶数, 则 $F(a, p)$ 为偶数个数偶数之和再加 1, 结果为奇数;

若 a 为奇数, 则 $F(a, p)$ 为偶数个数奇数之和再加 1, 结果也为奇数.

故 $F(a, p)$ 恒为奇数, 因此其任意素因子 $q \neq 2$, 即 $F(a, p)$ 的任意素因子 q 定为奇素数, 所以 $2|q-1$ (2).

由 (1) (2) 及 $(2, p)=1$, 得 $2p|q-1$, 即 $q=2np+1$

而任意两个形如 $2n_1p+1, 2n_2p+1$ 因子相乘:

$(2n_1p+1) \cdot (2n_2p+1) = 2(2n_1n_2p+n_1+n_2)p+1$ 仍具有 $2np+1$ 的形式. 由素数基本定理, $F(a, p)$ 的全部因子均由这些素因子组合相乘而得, 故全体因子均具有 $2np+1$ 的形式. 命题得证.

3.2 关于 $M(a, m)$

显然地, 有 $p, q \in \{x \in N^* | x \neq 1\}$

1. 令 $m = p \cdot q$, 其中, 则有

$$F(a, m) = \frac{a^m - 1}{a - 1} = \frac{a^p - 1}{a - 1} \cdot \frac{a^{p \cdot q} - 1}{a^p - 1} = \frac{a^q - 1}{a - 1} \cdot \frac{a^{q \cdot p} - 1}{a^q - 1}.$$

此时 $F(a, m)$ 具有至少两个真因子.

2. 令 $p | m, a \equiv 1 \pmod{p}$, 则有

$$F(a, m) = \sum_{n=0}^{m-1} a^n \equiv \sum_{n=0}^{m-1} 1 \equiv 0 \pmod{p}.$$

此时 $M(a, m)$ 具有真因子 p .

设 q 为素数且 $q \nmid a$. 称最小的正整数 t 使得 $a^t \equiv 1 \pmod{q}$ 为 a 模 q 的阶, 记作 $\text{ord}_q(a)$.

由引理 3 Zsigmondy 定理: 任意 $n \geq 2, a^n - b^n$, 若存在 $a^n - b^n$ 的素因子 q , 使得 q 不整除任何 $a^k - b^k (1 \leq k < n)$, 则称 q 为 $a^n - b^n$ 的本原素因子. 对互素整数 $a, b (a > b)$, 除

特定反例外, 对任意 $n \geq 2, a^n - b^n$ 至少有一个本原素因子.

仅有的特定反例:

1. $n = 2$, 且 $a + b$ 是 2 的幂;

2. $n = 6$, 且 $a = 2, b = 1$.

又由定义, 当 $b = 1$ 时, 除特例外本原素因子 q 整除 $a^n - 1 = (a - 1) \cdot \sum_{i=0}^{n-1} a^i$, 本原素因子

q 不整除 $a^d - 1 = (a - 1) \cdot \sum_{i=0}^{d-1} a^i$ ($1 \leq d < n$), 所以本原素因子 q 必然不整除 $a - 1$. 该定理是本节所有讨论的基石.

结论 3.2.1: 设 $a \geq 2, m \geq 2$, 则 $F(a, m)$ 除两个例外情形外, 至少存在一个本原素因子:

例外情形:

(1) $m = 2$, 且 $a + 1$ 是 2 的幂

(2) $a = 2, m = 6$

证明:

直接对 $a^m - 1$ 应用 Zsigmondy 定理. 定理保证除上述两个例外外, 存在素因子 q , 使

得 $q \mid a^m - 1$, 又因为 q 不整除 $a - 1$, 所以 $q \mid \frac{a^m - 1}{a - 1} = F(a, m)$. 命题得证.

结论 3.2.2: 设 p 为奇素数, 若 $(a - 1, F(a, p)) = 1$, 则 $F(a, p)$ 的全体因子均具有 $2np + 1$ ($n \in N^*$) 的形式.

证明: 因为, $(a - 1, F(a, p)) = 1 \Leftrightarrow a \bmod p \neq 1$, 所以该命题等价于结论 3.1.5, 故命题得证. 而当 p 为合数时, 无法满足 $a \bmod p \neq 1$, 故无法推广到合数.

3.3 关于 $F(a^{p^n}, q)$

若 $(p, q) = 1$, 存在 $1 < m < M(a^{p^n}, q)$, 且 $m \mid F(a^{p^n}, q)$. 于是仅当 $q = p$, $F(a^{p^n}, q)$ 可能取得素数.

对 $F(a^{p^n}, q)$ 进行讨论, 得到:

结论 3.3.1 设 p 为奇素数, $m > n \geq 0$, 则 $(F(a^{p^m}, p), F(a^{p^n}, p)) = \begin{cases} 1, & a - 1 \neq np, n \in N \\ p, & a \equiv 1 \pmod{p} \end{cases}$

证明:

设 q 为 $F(a^{p^m}, p)$ 与 $F(a^{p^n}, p)$ 的任一公共素因子

当 $q \neq p$ 时, 若 $a^{p^n} \equiv 1 \pmod{q}$, 则

$$F(a^{p^n}, p) = \sum_{i=0}^{p-1} (a^{p^n})^i \equiv \sum_{i=0}^{p-1} 1 \equiv p \not\equiv 0 \pmod{q}, \text{ 与 } q \mid F(a^{p^n}, p) \text{ 矛盾。因此 } a^{p^n} \equiv 1 \pmod{q}。$$

由 $q \mid F(a^{p^n}, p)$ 且 $a^{p^n} \equiv 1 \pmod{q}$, 可得

$$(a^{p^n})^p \equiv 1 \pmod{q}$$

故 $\text{ord}_q(a^{p^n}) = p$ 。

又因为 $m > n$, 有 $a^{p^m} = (a^{p^n})^{p^{m-n}}$ 。根据乘法阶的性质:

$$\text{ord}_q(a^{p^m}) = \frac{\text{ord}_q(a^{p^n})}{\left(\text{ord}_q(a^{p^n}), p^{m-n}\right)} = \frac{p}{(p, p^{m-n})} = 1$$

于是 $a^{p^m} \equiv 1 \pmod{q}$, 从而

$$F(a^{p^m}, p) \equiv \sum_{i=0}^{p-1} i = p \not\equiv 0 \pmod{q}, \text{ 与 } q \mid F(a^{p^m}, p) \text{ 矛盾。}$$

故不存在 $q \neq p$ 的公共素因子。

当 $q = p$ 时,

$$\text{由费马小定理, } a^{p^n} \equiv a \pmod{p}, \text{ 于是 } F(a^{p^n}, p) \equiv \sum_{i=0}^{p-1} a^i \pmod{p}$$

若 $a \equiv 1 \pmod{p}$, 则 $F(a^{p^n}, p) \equiv p \equiv 0 \pmod{p}$, 即 p 为公共因子;

若 $a \not\equiv 1 \pmod{p}$, 则 $\sum_{i=0}^{p-1} a^i \equiv \frac{a^p - 1}{a - 1} \equiv 0 \pmod{p}$ 当且仅当 $a \equiv 1 \pmod{p}$, 故 p 不整除。

进一步, 当 $a \equiv 1 \pmod{p}$ 时, 由 LTE 定理:

$$v_p(F(a^{p^n}, p)) = v_p(a^{p^{n+1}} - 1) - v_p(a^{p^n} - 1) = 1,$$

故公共因子中 p 的指数恰好为 1。

综上,

$$(F(a^{p^m}, p), F(a^{p^n}, p)) = \begin{cases} 1, & a - 1 \neq np, n \in \mathbb{N} \\ p, & a \equiv 1 \pmod{p} \end{cases}$$

命题得证。

4 关于 $F(a, p)$ 的猜想和讨论

当 p 取得素数, 不难发现 $F(x, p) = \Phi_p(x)$. 由于此类数事实上为分圆多项式在整数上的取值, 亦与梅森数 F_p 在形式上相近. 不妨称之为增广梅森数. 以下给出若干猜测:

1. 对任意非幂整数 a , 存在无穷多个素数 p , 使 $F(a, p)$ 取得素数;
2. 给定 $p \in P$, 对充分大的 z , 均存在一个 $z \leq a \leq z^2$, 使 $F(a, p)$ 取得素数;
3. 若 $p \in P$ 且 $p \neq 2$, 仅当 $a=3, p=5$, $F(a, p)$ 为完全幂方数.

第一个猜测是自然给出的; 第三个是由 $F(3, 5) = 11^2$ 而启发提出的. 特别地, 第二个猜测与启发式推导有关.

4.1 关于素性检验

对梅森素数的检验, 我们可以使用高效且优美的卢卡斯-莱默检验法. 由于 $F(a, p)$ 与其在形式上的相似, 我们自然地希望同步推广这种检验法. 然而, 在换底增广后重新建立类似检验会相当困难.

不妨采用最基础的试除法去检验一个数的素性, 即回归素数定义, 将 1 到这个数本身对这个数做带余除法, 若只有 1 和这个数本身能整除这个数, 则这个数为素数; 反之, 则为合数. 然而, 将 1 一直整除至这个数本身, 运算量大, 当碰到比较大的数时, 计算机的反应速度会大大降低甚至出现卡顿. 改进试除法, 便可以提高计算的效率.

由基础知识, 可得**结论 4.1**:

对于任意一个正整数 a , 它的因子在实数轴上被平分在 $\sqrt{a}$ 两侧, 且两侧乘积为 a 的因子是一一对应的.

由**结论 3.1.1**, $F(a, p)$ 与 $a-1$ 互素, 当且仅当 $\forall q|p, a \bmod q \neq 1$.

因为 $p \in P$, 所以仅有 $1|p$ 和 $p|p$, 则此时 $F(a, p)$ 与 $a-1$ 互素的充要条件变为 $a \bmod p \neq 1$, 则同理 $F(a, p)$ 为素数的必要条件为 $a \bmod p \neq 1$.

由**结论 3.1.5**, 如果 $a \bmod p \neq 1$, 则 $F(a, p)$ 所有因子均具有 $2np+1 (n \in N)$ 的形式.

综上, 我们只需先检测 $a \bmod p$ 是否等于 1, 再确立从 $n=1$ 开始直到 $2np+1$

(小于 $\sqrt{F(a,p)}$) 是否能整除 $F(a,p)$ 即可。

照此思路,运用 Python 进行编程,便可做一个检验广义梅森数 $F(a,p)$ 的素性的交互式页面,如下图所示

```

1 def prime(f,a,p): 1个用法
2     import math
3     limit=int(math.isqrt(f))
4     test_number=0
5     if a%p!=1:
6         n=(f-1)//2//p
7         for i in range(1,n):
8             factor=2*p*i+1
9             if factor>limit:
10                break
11            if f%factor==0:
12                test_number+=1
13                break
14        if test_number==0:
15            return True
16        else:
17            return False
18    else:
19        return False
20
21 a=int(input("a="))
22 p=int(input("p="))
23 F=(a**p-1)//(a-1)
24 if prime(F,a,p):
25     print("prime")
26 else:
27     print("not prime")

```

由 Bunyakovsky 猜想:若整系数多项式满足首项为正,不可约且无固定素因子,则其代入整数时能产生无穷多个素数.发现,猜想 1:对任意非幂整数 a ,存在无穷多个素数 p ,使 $F(a,p)$ 取得素数是 Bunyakovsky 猜想的特例.然而,该猜想至今未被证明.所以猜想 1 仍为开放性问题.

4.2 关于猜想 2

猜想 2 给定 $p \in P$,对充分大的 z ,均存在一个 $z \leq a \leq z^2 - 1$,使 $F(a,p)$ 取得素数.

猜想二本质上是 Bunyakovsky 猜想在分圆多项式上的特例.Bunyakovsky 猜想自 1857 年提出至今未解决,因此本节不试图证明,而是提供启发式证据和数据支持.

固定素数 p ,考虑区间 $[z, z^2]$ 内的整数 a ,定义 $\pi_p(z) = \#\{z \leq a \leq z^2 - 1 : F(a,p) \in P\}$

由素数定理,一个大小约为 N 的整数为素数的概率约为 $\frac{1}{\ln N}$.当 a 在区间 $[z, z^2]$ 内

变化时, $F(a,p) = 1 + a + \dots + a^{p-1}$ 的数量级约为 a^{p-1} ,故其对数约为 $(p-1)\ln a$.因此,

在概率模型下, $F(a,p)$ 为素数的概率约为 $\frac{1}{\ln F(a,p)} \approx \frac{1}{(p-1)\ln a}$.

于是区间内期望的素数个数约为 $E(z, p) = \sum_{a=z}^{z^2-1} \frac{1}{(p-1)\ln a} \approx \frac{1}{p-1} \int_z^{z^2} \frac{dt}{\ln t}$.

利用积分渐近当 $x \rightarrow \infty$, $\int_2^x \frac{dt}{\ln t} \sim \frac{x}{\ln x}$, 可得, 当 $z \rightarrow \infty$

$$E(z, p) \sim \frac{1}{p-1} \cdot \frac{z^2}{\ln(z^2)} = \frac{z^2}{2(p-1)\ln z}.$$

为检验猜想的合理性, 我们对若干小素数 p 即增长区间以猜想一的素性检验为基础进行初步数值搜索。受计算资源所限, 我们取 $p = 3, 5, 7$, z 分别取 10, 20, 30, 统计各区间实际观测到的素数个数 N , 与启发式期望 $E(z, p)$ (取整) 对比。发现, 所有的测试区间内, 实测素数个数均明显高于启发式期望值。

于是, 计算超额比率 $R = \frac{N-E}{\sqrt{E}}$ (取两位有效数字), 得到如下数据:

p	z	区间 $[z, z^2]$	观测值 N	启发式期望 E	超额比率 R
3	10	[10,99]	26	12	4.52
3	20	[20,399]	81	38	6.98
3	30	[30,899]	160	75	9.81
5	10	[10,99]	24	6	7.35
5	20	[20,399]	68	19	11.24
5	30	[30,899]	121	38	13.46
7	10	[10,99]	20	4	8.00
7	20	[20,399]	56	13	11.93
7	30	[30,899]	104	25	15.80

这表明, 事实上, 原始期望严重低估了 $F(a, p)$ 的素数概率, 忽略了结论 3.1.5 中所揭示的固有算数结构。由结论 3.1.5: 若 $a \bmod p \neq 1$, $F(a, p)$ 的任意素因子 q 均具有 $2np+1$ 的形式, 表明 $F(a, p)$ 天然避开了所有小于 $2p$ 的素因子, 导致 $F(a, p)$ 为素数概率增大。

综上, 提出猜想二的加强形式:

猜想二: 固定奇素数 p , 设 $\pi_p(z) = \#\{z \leq a \leq z^2-1: F(a, p) \in P\}$, 则

$$\pi_p(z) \sim \frac{z^2}{2(p-1)\ln z}, z \rightarrow \infty. \text{ 特别地, } \pi_p(z) \geq 1 \text{ 对一切充分大的 } z \text{ 成立。但, 猜}$$

想二仍未开放性问題。

4.3 关于完全幂方问题

考虑 $F(3,5)=11^2$ ，作出猜想：

猜想 3 若 $p \in P$ 且 $p \neq 2$ ，仅当 $a=3, p=5$ ， $F(a, p)$ 为完全幂方数.

运用 Python 编程进行一定范围的搜寻,发现当 $a \in [2, 19]$, $p=3, 5$ 时, 只有 $F(3, 5)$, $F(18, 3)$ 为完全幂方数, 其中 $F(3, 5)$ 是完全平方数, $F(18, 3)$ 是完全立方数. 发现原猜想 3 存在错误.

```
import math
for p in range(3, 6):
    q=0
    for j in range(2, p):
        if p%j==0:
            q+=1
            break
    if q==0:
        for i in range(2, 6):
            for a in range(2, 20):
                F=int((a**p-1)/(a-1))
                t=round(math.pow(F, (1/i)))
                j=math.pow(t, i)
                if j==F:
                    print(F, a, p, i)
```

由 Ljunggren 定理方程 $\frac{x^n-1}{x-1} = y^q$ 在 q 为偶数, 即函数 $\frac{x^n-1}{x-1}$ 为偶次幂数, 唯有两解 $x=3, n=5$ 和 $x=7, n=4$, 得若将猜想 3 改为若 $p \in P$ 且 $p \neq 2$ ，仅当 $a=3, p=5$ ， $F(a, p)$ 为偶次幂方数, 则猜想 3 成立.

又由 Nagell-Ljunggren 猜想得, 若 $p \in P$ 且 $p \neq 2$ ， $F(3, 5)$ ， $F(18, 3)$ 为完全幂方数. 发现猜想 3 实际上为 Nagell-Ljunggren 方程在素数域上的解, 也就是说猜想 3 为 Nagell-Ljunggren 猜想的特例, 于是得出修正后的猜想 3:

若 $p \in P$ 且 $p \neq 2$ ，当且仅当 $a=3, p=5$ 或 $a=18, p=3$ ， $F(a, p)$ 为完全幂方数.

然而, Nagell-Ljunggren 猜想截至目前还未得证, 故猜想 3 仍未开放性问题的

又发现: $F(a, 3) = a^2 + a + 1$

$$\therefore a^2 < F(a, 3) = a^2 + a + 1 < (a+1)^2$$

$\therefore$ 两个相邻的完全平方数之间不会有另一个不同于二者完全平方数, 由此 $F(a, 3)$

不可能为完全平方数, 即若 $F(a, 3)$ 为完全幂方数则次幂不可能为 2 次幂

$$\therefore F(a, p) = \sum_{i=1}^{p-1} a^i > a^{p-1} \text{ 恒成立, 又由二项式定理, 得}$$

$(a+1)^{p-1} = \sum_{k=0}^{p-1} C_{p-1}^{k-(p-1)} a^k$, 又 $\because$ 令 $j = k - (p-1)$, $\therefore C_{p-1}^{k-(p-1)} = C_{p-1}^j \geq 1$, 当且仅当 $j = 0$

或 $j = p-1$ 即 $k = 0$ 或 $k = p-1$, 等号成立, $\therefore a^{p-1} < F(a, p) = \sum_{i=1}^{p-1} a^i < (a+1)^{p-1}$ 恒成立,

又 $\because$ 两个相邻的 $p-1$ 次方幂数之间不可能有另一个不同于二者 $p-1$ 次方幂数, 由

此 $F(a, p)$ 不可能为 $p-1$ 次方幂数, 即若 $F(a, p) = b^k$, 则 $k \neq p-1$

于是, 得出结论 4.3:

若 $F(a, p) = b^k$, 则 $k \neq p-1$

5 总结和实际应用

总结:

本文提出的结论大致可以分为以下几类:

互素性:

结论 3.3.1: $F(a, m)$ 与 $a-1$ 互素, 当且仅当 $\forall p \mid m, a \bmod p \neq 1$.

结论 3.1.2: $F(a, p), F(a, q)$ 互素, 当且仅当 p, q 互质.

结论 3.3.1: 设 p 为奇素数, $m > n \geq 0$, 则

$$\left(F(a^{p^m}, p), F(a^{p^n}, p) \right) = \begin{cases} 1, & a-1 \neq np, n \in N \\ p, & a \equiv 1 \pmod{p} \end{cases}$$

代数恒等式:

结论 3.1.3: $(F(a, p), F(a, q)) = F(a, (p, q))$

结论 3.1.4: $F(a, p) \mid F(a^q, p)$, 其中 $q \in N^*$.

结论 4.3: 若 $F(a, p) = b^k$, 则 $k \neq p-1$.

本原素因子:

结论 3.2.1: 设 $a \geq 2, m \geq 2$, 则 $F(a, m)$ 除两个例外情形外, 至少存在一个本原素

因子: 例外情形: (1) $m = 2$, 且 $a+1$ 是 2 的幂; (2) $a = 2, m = 6$.

因子形式:

结论 3.1.5: 设 $p \in \{x \in P \mid x \neq 2\}, n \in N^*$, 若 $a \bmod p \neq 1$, 则 $F(a, p)$ 的 q 任意素因子

q 均满足 $q \equiv 1 \pmod{2p}$, 即 q 具有 $2np+1$ 的形式. 进而, $F(a, p)$ 的全体正因子均具有 $2np+1$ 的形式.

结论 3.2.2: 设 p 为奇素数, 若 $(a-1, F(a, p))=1$, 则 $F(a, p)$ 的全体因子均具有 $2np+1$ ($n \in \mathbb{N}^*$) 的形式.

经典结论:

结论 4.1: 对于任意一个正整数 a , 它的因子在实数轴上被平分在 $\sqrt{a}$ 两侧, 且两侧乘积为 a 的因子是一一对应的.
以及以下开放性猜想:

猜想一: 对任意非幂整数 a , 存在无穷多个素数 p , 使 $F(a, p)$ 取得素数;

猜想二: 固定奇素数 p , 设 $\pi_p(z) = \#\{z \leq a \leq z^2 - 1 : F(a, p) \in P\}$, 则

$$\pi_p(z) \sim \frac{z^2}{2(p-1)\ln z}, z \rightarrow \infty.$$

猜想三: 若 $p \in P$ 且 $p \neq 2$, 当且仅当 $a=3, p=5$ 或 $a=18, p=3$, $F(a, p)$ 为完全幂方数.

实际应用:

在密码系统生成安全大素数时, 通常需要先筛选候选数再进行 Miller-Rabin 测试。

对于形如 $F(a, p) = \frac{a^p - 1}{a - 1}$ 的候选数, 传统试除需遍历所有整数至 $\sqrt{N}$ 。利用本文

结论 3.1.5, 试除空间可由 $O(\sqrt{N})$ 压缩至 $O\left(\frac{\sqrt{N}-1}{2p}\right)$, 极大的减少了运算时间。

6 致谢

在我所处的山区城市中，我对数学的热情从未被扼杀，即便学校的数学竞赛指导相对稀缺。自学成为了我在这个领域内拓展的唯一方式，我沉浸在各种数学竞赛题目中，逐渐对数论产生了浓厚兴趣。在这个广阔的研究领域内，梅森素数引发了我对数的思考，它既是一种挑战也是一种动力，激励我在此基础上展开自己的探索。

我深知，学术研究的道路上，遇见一位好的指导老师是何等的重要。我的指导老师不仅是我学术道路上的引路人，更是我高中生涯中的良师益友。他严谨的学风、对学生无微不至的关怀以及对教育事业的献身精神，都深深地影响了我。

在这次关于数论及梅森素数的研究过程中，老师的每一次指点与建议都如同一盏明灯，照亮我前行的道路。从选题、文献回顾、理论学习到实证研究、论文撰写等每一个环节，都离不开老师的悉心指导。尤其是在证明方面的学习，需要扎实的数论基础。而老师总是能在我困惑之时无偿地给予方向性的建议，使我能够不断进步、深入学习。

感谢我的导师为我所做的一切。他为我提供的不仅仅是学术上的指导，更多的是对年轻学子的培养和对教育事业的执着。他时常鼓励我独立思考、大胆尝试，使我能够勇敢地面对学术挑战。他在时间上的支持以及对我研究工作的关心，让我深深感受到了作为教师的责任与使命。

此外，我也要感谢我的家人和朋友们。他们一直是我坚强的后盾，给予我无尽的支持与鼓励。在面对困难和挫折时，他们总是会给予我最大的帮助和鼓励，让我能够更加坚定地面对挑战并取得成功。他们的爱与支持是我前进的动力源泉。

在本次研究中，我独立完成了一项具有实际意义的学术研究工作。从选题到相关知识的学习、从猜想的提出到证明都凝结了我的心血和努力。我深知每一次的成功都离不开自身的努力和坚持。同时，我也要感谢我的导师和同学们在我研究过程中给予的帮助和支持，没有他们的陪伴与支持我的研究工作难以顺利完成。

在此过程中我也意识到了自学的重要性以及如何将所学知识应用到实际的研究中。特别是在数论相关基础的学习中，我遇到了很多困难和挑战，但通过不断地学习和实践，我逐渐掌握了新的知识并成功将其应用到实际的研究中。这使我更加坚定了对数学研究的信心和决心。

在今年（2026年）8月，我参加了 ICBS 高中生海报展，国内外的教授科学家和清华大学求真书院的大学生给了我的研究提出了许多的建议，我自此基础上做出了完善和修改，在此表以感谢。

我也要特别感谢所有参与阅读和评审的评委专家、老师们。您辛苦了，感谢您的阅读，谢谢您，谢谢！

