2023 年数学新星研修论坛的几道数论题目

赖力

(北京大学, 100871)

在 2023 年 8 月 3–10 日于上海举办的数学新星研修论坛中, 我与同学们交流讨论了九道数论问题. 这些题目来自于美国数学月刊 (AMM) 以及不同年代的几篇数学论文.

陈澍同学给出了第 4 题 (Morley 同余式) 的一个简洁证明; 周嘉豪同学简化了第 6 题的证明; 翁斌同学加强了第 7 题的结论. 另外还有多位同学对一些题目给出了不同的解答, 在此我一并感谢. 前面提到的几位同学的证明均比题目来源处的原始证明更加简洁, 这印证了“数学新星”的寓意. 我也受到鼓舞, 于是将这几道题目的解答进行了整理, 期待它们能够给更多的同学带来启发.

毫无疑问, 这些题目会有不同的、更简便的解答方式. 限于时间与水平, 我在此文中没有追求一题多解或者最简解答. 作为我个人对题目难度的一个大致判断: 题目 1、2、5 的难度大约在高中数学联赛的水平, 其余题目的难度则超过了联赛.

1 题目

1. 我们用 $\{x\}$ 表示实数 x 的小数部分. 设 p,q 是两个互素的正整数, 其中 $p>q>1$. 求证: 存在无穷多个正整数 n 使得

$$\left\{\frac{p^n}{q^n}\right\}>\frac{1}{p}.$$

2. 对任何正整数 k, 我们记 p_k 为第 k 个素数, 记 $a_k=p_kp_{k+1}$. (例如 $a_1=2\cdot3$, $a_2=3\cdot5$, $a_3=5\cdot7$, $a_4=7\cdot11$, ...) 一个正整数 m 被称作 “好数”, 如果 m 可以表示成 $m=\prod_{k=1}^{\infty}a_k^{s_k}$ 的形式, 其中 $\{s_k\}_{k\geqslant1}$ 是非负整数数列, 且仅有有限个 k 使得 $s_k\neq0$. (例如, 1, $a_2a_3^3a_9^2$, $a_5^2a_8^7$, a_4 均是好数.) 我们将前 n 个正整数 $1,2,\dots,n$ 中好数的个数记作 $f(n)$. 求证: 对任何正整数 n, 我们有

$$\frac{1}{2}\lfloor\sqrt{n}\rfloor\leqslant f(n)\leqslant\lfloor\sqrt{n}\rfloor.$$

3. 求证: 不定方程 $y^2=3^a+2^b+1$ 的全部正整数解为 $(y,a,b)=(6,1,5),(6,3,3)$.

4. 求证 Morley 同余式: 对于任何素数 $p\geqslant5$, 我们有

$$(-1)^{\frac{p-1}{2}}\binom{p-1}{\frac{p-1}{2}}\equiv4^{p-1}\pmod{p^3}.$$

5. 设 $P(X)=\sum_{i=0}^{n}a_iX^i$ 是一个 n 次多项式, 且它的所有系数 $a_0,a_1,\dots,a_n$ 均属于集合 $\{-1,1\}$. 求证:

$$\operatorname{ord}_{X=1}P(X)<2^{v_2(n+1)}.$$

其中 $\mathrm{ord}_{X=1} P(X) = \max\{k \in \mathbb{N} \cup \{0\} \mid (X-1)^k \text{ 整除 } P(X)\}$ 为 $P(X)$ 在 $X=1$ 处的根的重数, 而 $v_2(n+1) = \max\{k \in \mathbb{N} \cup \{0\} \mid 2^k \text{ 整除 } n+1\}$ 为 $n+1$ 含 2 的幂次.

6. 已知正整数 n 满足

$$v_2(\sigma(n)) > \log_2 n,$$

求证: n 一定是若干个互不相同的 Mersenne 素数的乘积.
(注: $\sigma(n) = \sum_{d|n} d$ 表示 n 的正约数之和. $v_2(m)$ 表示正整数 m 含 2 的幂次, 即满足 $2^k \mid m$ 的最大的非负整数 k. 我们称满足 $p+1$ 是 2 的方幂的素数 p 为 Mersenne 素数.)

7. 我们记 $S_2(n)$ 为 n 在二进制表示下的数字和.

(1) 求证: 对任何实数 $\alpha \in [0, +\infty)$, 以及对于 $\alpha = +\infty$, 均存在一列正整数 $\{n_k\}_{k \geqslant 1}$ 使得

$$\lim_{k \to \infty} \frac{S_2(n_k^2)}{S_2(n_k)} = \alpha.$$

(2) 求证: 存在无穷多个正整数 n 使得

$$\frac{S_2(n^2)}{S_2(n)} \leqslant \frac{4(\log_2 \log_2 n)^2}{\log_2 n}.$$

8. 设 p 是一个奇素数. 我们定义 Fekete 多项式

$$f_p(z) = \sum_{a=0}^{p-1} \left(\frac{a}{p}\right) z^a.$$

这里 $\left(\frac{a}{p}\right)$ 是 Legendre 符号. 求证: $f_p(z)$ 至少有 $\frac{p-1}{2}$ 个根在单位圆周上.

9. 求证: 对任何正整数 m, n, 区间 $[m, m+10n^{\frac{3}{2}}]$ 中存在 n 个两两不同的正整数 $a_1, a_2, \ldots, a_n$ 使得 $k \mid a_k$, $(k = 1, 2, \ldots, n)$.

2 解答与评注

题 1 我们用 $\{x\}$ 表示实数 x 的小数部分. 设 p, q 是两个互素的正整数, 其中 $p > q > 1$. 求证: 存在无穷多个正整数 n 使得

$$\left\{\frac{p^n}{q^n}\right\} > \frac{1}{p}.$$

证明 对任何正整数 n, 我们记 $x_n = \lfloor \frac{p^n}{q^n} \rfloor$, $y_n = \{\frac{p^n}{q^n}\}$. 则我们有 $x_{n+1} + y_{n+1} = \frac{p^{n+1}}{q^{n+1}} = \frac{p}{q}(x_n + y_n)$, 于是

$$qx_{n+1} - px_n = py_n - qy_{n+1}, \quad \forall\, n \in \mathbb{N}. \tag{1}$$

我们用反证法. 假设本题结论不成立, 则存在 n_0 使得对任何正整数 $n \geqslant n_0$ 有 $0 \leqslant y_n \leqslant \frac{1}{p}$. 由于 $\gcd(p, q) = 1$ 且 $q > 1$, 故 $y_n \neq 0$, 所以

$$0 < y_n \leqslant \frac{1}{p}, \quad \forall\, n \geqslant n_0. \tag{2}$$

式 (2) 推出

$$-1 < p \cdot 0 - q \cdot \frac{1}{p} < py_n - qy_{n+1} < p \cdot \frac{1}{p} - q \cdot 0 = 1, \quad \forall\, n \geqslant n_0.$$

注意到 (1) 式左端是整数, 由于区间 $(-1, 1)$ 中的整数仅有 0, 故

$$py_n - qy_{n+1} = 0, \quad \forall\, n \geqslant n_0.$$

这表明 $\{y_n\}_{n \geqslant n_0}$ 是一个公比为 $\frac{p}{q}$ 的等比数列, 于是

$$y_n = \left(\frac{p}{q}\right)^{n-n_0} y_{n_0}, \quad \forall\, n \geqslant n_0.$$

但是 $\frac{p}{q} > 1$, $y_{n_0} > 0$, 当 $n \to +\infty$ 上式推出 $y_n \to +\infty$, 与 (2) 矛盾. □

评注 一个未被解决的研究性问题是: 数列 $\{\left(\frac{3}{2}\right)^n\}$, $n = 1, 2, 3, \ldots$ 是否在区间 $[0, 1]$ 中稠密?

题 2 (1950, Erdös) 对任何正整数 k, 我们记 p_k 为第 k 个素数, 记 $a_k = p_k p_{k+1}$. (例如 $a_1 = 2 \cdot 3$, $a_2 = 3 \cdot 5$, $a_3 = 5 \cdot 7$, $a_4 = 7 \cdot 11$, ...) 一个正整数 m 被称作 "好数", 如果 m 可以表示成 $m = \prod_{k=1}^{\infty} a_k^{s_k}$ 的形式, 其中 $\{s_k\}_{k \geqslant 1}$ 是非负整数数列, 且仅有有限个 k 使得 $s_k \neq 0$. (例如, 1, $a_2 a_3^3 a_9^2$, $a_5^2 a_8^7$, a_4 均是好数.) 我们将前 n 个正整数 $1, 2, \ldots, n$ 中好数的个数记作 $f(n)$. 求证: 对任何正整数 n, 我们有

$$\frac{1}{2}\lfloor \sqrt{n} \rfloor \leqslant f(n) \leqslant \lfloor \sqrt{n} \rfloor.$$

问题来源 Paul Erdös, *Number of integers of special form.* The American Mathematical Monthly 1950, Problem 635.

证明 首先我们证明好数的表示方式是唯一的. 假设

$$m = \prod_{k=1}^{\infty} a_k^{s_k} = \prod_{k=1}^{\infty} a_k^{s'_k},$$

其中 s_k, s'_k $(k \in \mathbb{N})$ 是非负整数, 且只有有限项非零. 利用 $a_k = p_k p_{k+1}$ 将 m 写为标准的素因子分解, 我们有

$$m = p_1^{s_1} \prod_{k=2}^{\infty} p_k^{s_k + s_{k-1}} = p_1^{s'_1} \prod_{k=2}^{\infty} p_k^{s'_k + s'_{k-1}},$$

于是由算术基本定理的唯一性部分, 我们有 $s_1 = s'_1$, $s_k + s_{k-1} = s'_k + s'_{k-1}$, $\forall\, k = 2, 3, \ldots$. 由此易得 $s_k = s'_k$, $\forall\, k \in \mathbb{N}$. 即好数的表示方式是唯一的.

现在定义映射 $g : \{\text{全体好数}\} \longrightarrow \{\text{正的完全平方数}\}$ 如下: 设好数 m 的唯一表示为 $m = \prod_{k=1}^{\infty} a_k^{s_k}$, 其中 s_k $(k \in \mathbb{N})$ 是非负整数, 且只有有限项非零, 则我们定义 $g(m) = \prod_{k=1}^{\infty} p_k^{2s_k}$. (显然 $g(m)$ 是正的完全平方数.)

我们断言 g 是单射. 事实上, 若两个好数 $m = \prod_{k=1}^{\infty} a_k^{s_k}$ 与 $m' = \prod_{k=1}^{\infty} a_k^{s'_k}$ 使得 $g(m) = g(m')$, 则由 g 的定义, 有 $\prod_{k=1}^{\infty} p_k^{2s_k} = \prod_{k=1}^{\infty} p_k^{2s'_k}$. 从而由算术基本定理的唯一性部分, 我们得到 $s_k = s'_k$, $\forall\, k \in \mathbb{N}$. 于是 $m = m'$.

注意到 $a_k > p_k^2$, $\forall\, k \in \mathbb{N}$. 故对于任何好数 m, 我们有 $g(m) \leqslant m$. 于是当 m 是好数且 $m \leqslant n$ 时, 有 $g(m)$ 是正的完全平方数且 $g(m) \leqslant n$. 这表明 g 的限制给出了以下的单射:

$$\big\{\text{不超过 } n \text{ 的好数}\big\} \longrightarrow \big\{\text{不超过 } n \text{ 的正的完全平方数}\big\}.$$

比较两个集合的元素个数, 我们便得到 $f(n) \leqslant \lfloor \sqrt{n} \rfloor$.

另一方面, 我们定义映射 $h : \{\text{全体奇完全数}\} \longrightarrow \{\text{好数}\}$ 如下: 由算术基本定理, 任何奇完全数 m 可以唯一的写成 $m = \prod_{k=1}^{\infty} p_{k+1}^{2s_k}$ 的形式, 其中 s_k $(k \in \mathbb{N})$ 是非负整数, 且只有有限项非零, 则我们定义 $h(m) = \prod_{k=1}^{\infty} a_k^{s_k}$. 由于好数的表示方式唯一, 故 h 是单射. 注意到 $a_k < p_{k+1}^2$, $\forall\, k \in \mathbb{N}$, 故对任何奇完全平方数 m, 我们有 $h(m) \leqslant m$. 于是 h 的限制给出以下的单射:

$$\big\{\text{不超过 } n \text{ 的奇完全平方数}\big\} \longrightarrow \big\{\text{不超过 } n \text{ 的好数}\big\}.$$

比较集合的元素个数, 我们便得到 $\frac{1}{2}\lfloor \sqrt{n} \rfloor \leqslant f(n)$. □

评注 构造单射、满射是常用的估计集合元素个数的方法.

题 3 (2011, Leitner) 求证: 不定方程 $y^2 = 3^a + 2^b + 1$ 的全部正整数解为 $(y, a, b) = (6, 1, 5), (6, 3, 3)$.

问题来源 [5, Theorem 3.1].

证明 设正整数 y, a, b 满足 $y^2 = 3^a + 2^b + 1$.

当 $a = 1$ 时, 有 $(y+2)(y-2) = 2^b$. 故 $y+2, y-2$ 均是 2 的方幂. 设 $y+2 = 2^{b_1}$, $y-2 = 2^{b_2}$, 其中 b_1, b_2 为非负整数, $b_1 > b_2$. 则 $4 = (y+2) - (y-2) = 2^{b_1} - 2^{b_2}$. 比较前式左右两端含 2 的幂次得到 $b_2 = v_2(4) = 2$, 故 $y = 6$. 解得 $(y, a, b) = (6, 1, 5)$. 易验证此解的确满足原不定方程.

当 $b=3$ 时, 有 $(y+3)(y-3)=3^a$. 故 $y+3, y-3$ 均是 3 的方幂. 设 $y+3=3^{a_1}$, $y-3=3^{a_2}$, 其中 a_1, a_2 为非负整数, $a_1>a_2$. 则 $6=(y+3)-(y-3)=3^{a_1}-3^{a_2}$, 比较前式左右两端含 3 的幂次得到 $a_2=v_3(6)=1$, 故 $y=6$. 解得 $(y,a,b)=(6,3,3)$. 易验证此解的确满足原不定方程.

以下设 $a\neq 1$ 且 $b\neq 3$. 我们将证明此时无解.

因 $a\neq 1$, 故 $a\geqslant 2$, 我们有 $3^a\equiv 0 \pmod 9$. 代入原不定方程, 得

$$y^2\equiv 2^b+1 \pmod 9.$$

注意 y^2 模 9 的余数只可能为 $0,1,4,7$. 而 $2^6\equiv 1 \pmod 9$,

$$2^b+1\equiv\begin{cases}2 \pmod 9, & \text{当 } b\equiv 0 \pmod 6,\\ 3 \pmod 9, & \text{当 } b\equiv 1 \pmod 6,\\ 5 \pmod 9, & \text{当 } b\equiv 2 \pmod 6,\\ 0 \pmod 9, & \text{当 } b\equiv 3 \pmod 6,\\ 8 \pmod 9, & \text{当 } b\equiv 4 \pmod 6,\\ 6 \pmod 9, & \text{当 } b\equiv 5 \pmod 6.\end{cases}$$

于是必有 $y^2\equiv 2^b+1\equiv 0 \pmod 9$, 且

$$b\equiv 3 \pmod 6. \tag{3}$$

由 (3) 以及 $b\neq 3$, 我们有 $b\geqslant 9$. 从而 $2^b\equiv 0 \pmod{16}$. 代入原不定方程, 得到

$$y^2\equiv 3^a+1 \pmod{16}.$$

注意 y^2 模 16 的余数只可能为 $0,1,4,9$. 而 $3^4\equiv 1 \pmod{16}$,

$$3^a+1\equiv\begin{cases}2 \pmod{16}, & \text{当 } a\equiv 0 \pmod 4,\\ 4 \pmod{16}, & \text{当 } a\equiv 1 \pmod 4,\\ 10 \pmod{16}, & \text{当 } a\equiv 2 \pmod 4,\\ 12 \pmod{16}, & \text{当 } a\equiv 3 \pmod 4.\end{cases}$$

故必有 $y^2\equiv 3^a+1\equiv 4 \pmod{16}$, 且

$$a\equiv 1 \pmod 4. \tag{4}$$

由 (4) 以及 $3^4\equiv 1 \pmod 5$, 我们有 $3^a\equiv 3 \pmod 5$. 代入原不定方程, 得到

$$y^2\equiv 2^b+4 \pmod 5.$$

注意 y^2 模 5 的余数只可能为 $0,1,4$. 由 (3) 知 b 为奇数, 故 b 模 4 余 $1,3$, 而

$$2^b+4\equiv\begin{cases}1 \pmod 5, & \text{当 } b\equiv 1 \pmod 4,\\ 2 \pmod 5, & \text{当 } b\equiv 3 \pmod 4.\end{cases}$$

故必有 $y^2\equiv 2^b+4\equiv 1 \pmod 5$, 且 $b\equiv 1 \pmod 4$. 结合 (3), 我们得到

$$b\equiv 9 \pmod{12}. \tag{5}$$

由 Fermat 小定理知 $2^{12}\equiv 1 \pmod{13}$, 于是 (5) 推出 $2^b\equiv 2^9\equiv 5 \pmod{13}$. 代入原不定方程, 得到

$$y^2\equiv 3^a+6 \pmod{13}.$$

注意 y^2 模 13 的余数只可能为 $0,1,3,4,9,10,12$. 而 $3^3\equiv 1 \pmod{13}$,

$$3^a+6\equiv\begin{cases}7 \pmod{13}, & \text{当 } a\equiv 0 \pmod 3,\\ 9 \pmod{13}, & \text{当 } a\equiv 1 \pmod 3,\\ 2 \pmod{13}, & \text{当 } a\equiv 2 \pmod 3.\end{cases}$$

故必有 $y^2\equiv 3^a+6\equiv 9 \pmod{13}$, 且 $a\equiv 1 \pmod 3$. 结合 (4), 我们得到

$$a\equiv 1 \pmod{12}. \tag{6}$$

最后考虑模 7. 由于 $3^6\equiv 1 \pmod 7$, 由 (6) 我们得到 $3^a\equiv 3 \pmod 7$. 由 (3) 我们有 $3\mid b$, 而 $2^3\equiv 1 \pmod 7$, 故 $2^b\equiv 1 \pmod 7$. 代入原不定方程, 我们得到

$$y^2\equiv 3+1+1\equiv 5 \pmod 7,$$

这不可能! (因为 y^2 模 7 的余数只可能为 $0,1,2,4$.) 所以当 $a\neq 1$ 且 $b\neq 3$ 时原不定方程无解.

综上, 原不定方程的所有正整数解为 $(y,a,b)=(6,1,5),(6,3,3)$. □

评注 解不定方程的常用方法有: 1. 同余、2. 因式分解、3. 比较素数幂次. 本解答中前两种方法均发挥了作用. 对于指数型的不定方程, 在初等的范围里考虑同余是最常用的办法.

题 4 (1895, Morley) 求证: 对于任何素数 $p\geqslant 5$, 我们有

$$(-1)^{\frac{p-1}{2}}\binom{p-1}{\frac{p-1}{2}}\equiv 4^{p-1} \pmod{p^3}.$$

问题来源 [6].

证明 (陈澍) 对于任何 $a,b\in\{0,1\}$, 我们记

$$S_a=\sum_{\substack{0<i<p\\ i\equiv a\pmod 2}}\frac{1}{i},\qquad S_{a,b}=\sum_{\substack{0<i<j<p\\ i\equiv a\pmod 2,\ j\equiv b\pmod 2}}\frac{1}{ij}.$$

引理 1 设 p 是奇素数. 则我们有

$$2^{p-1}\equiv 1+pS_1+p^2S_{1,1}\pmod{p^3},\tag{7}$$

$$(-1)^{\frac{p-1}{2}}\binom{p-1}{\frac{p-1}{2}}\equiv 2^{p-1}\left(1-pS_0+p^2S_{0,0}\right)\pmod{p^3}.\tag{8}$$

引理 1 的证明 我们有

$$\begin{aligned}2^{p-1}&=\frac{(2p-2)!!}{(p-1)!}=\frac{\prod_{i\equiv 1\pmod 2}^{0<i<p}(p+i)}{(p-2)!!}=\frac{\prod_{i\equiv 1\pmod 2}^{0<i<p}(p+i)}{\prod_{i\equiv 1\pmod 2}^{0<i<p}i}\\&=\prod_{\substack{0<i<p\\ i\equiv 1\pmod 2}}\left(1+\frac{p}{i}\right)\\&\equiv 1+pS_1+p^2S_{1,1}\pmod{p^3},\end{aligned}$$

故 (7) 得证. 而

$$\begin{aligned}(-1)^{\frac{p-1}{2}}\binom{p-1}{\frac{p-1}{2}}&=(-1)^{\frac{p-1}{2}}\frac{(p-1)!}{\left(\frac{p-1}{2}\right)!^2}=(-1)^{\frac{p-1}{2}}2^{p-1}\frac{(p-1)!}{(p-1)!!^2}\\&=(-1)^{\frac{p-1}{2}}2^{p-1}\frac{(p-2)!!}{(p-1)!!}=(-1)^{\frac{p-1}{2}}2^{p-1}\frac{\prod_{i\equiv 0\pmod 2}^{0<i<p}(p-i)}{\prod_{i\equiv 0\pmod 2}^{0<i<p}i}\\&=2^{p-1}\prod_{\substack{0<i<p\\ i\equiv 0\pmod 2}}\left(1-\frac{p}{i}\right)\\&\equiv 2^{p-1}\left(1-pS_0+p^2S_{0,0}\right)\pmod{p^3},\end{aligned}$$

故 (8) 得证. 引理 1 证毕.

引理 2 设素数 $p\geqslant 5$. 则我们有

$$S_1\equiv -S_0\pmod{p^2},\tag{9}$$

$$S_{1,1}\equiv S_{0,0}\pmod p.\tag{10}$$

引理 2 的证明 由 Wolstenholme 定理 (仅这里用到了 $p\geqslant 5$), 我们有 $S_0+S_1=\sum_{i=1}^{p-1}\frac{1}{i}\equiv 0\pmod{p^2}$, 故 (9) 得证. 而 (10) 是因为

$$\begin{aligned}S_{1,1}&=\sum_{\substack{0<i<j<p\\ i\equiv j\equiv 1\pmod 2}}\frac{1}{ij}=\sum_{\substack{0<k<l<p\\ k\equiv l\equiv 0\pmod 2}}\frac{1}{(p-l)(p-k)}\\&\equiv\sum_{\substack{0<k<l<p\\ k\equiv l\equiv 0\pmod 2}}\frac{1}{kl}\equiv S_{0,0}\pmod p.\end{aligned}$$

引理 2 证毕.

回到原题, 对任何素数 $p \geqslant 5$, 我们有

$$\begin{aligned}(-1)^{\frac{p-1}{2}}\binom{p-1}{\frac{p-1}{2}} &\equiv 2^{p-1}\left(1-pS_0+p^2S_{0,0}\right) \pmod{p^3} \quad (\text{式 (8)})\\ &\equiv 2^{p-1}\left(1+pS_1+p^2S_{1,1}\right) \pmod{p^3} \quad (\text{引理 2})\\ &\equiv 2^{p-1}\cdot 2^{p-1} \pmod{p^3} \quad (\text{式 (7)})\\ &\equiv 4^{p-1} \pmod{p^3}.\end{aligned}$$

证毕. □

题 5 设 $P(X)=\sum_{i=0}^{n}a_iX^i$ 是一个 n 次多项式, 且它的所有系数 $a_0,a_1,\ldots,a_n$ 均属于集合 $\{-1,1\}$. 求证:

$$\operatorname{ord}_{X=1}P(X)<2^{v_2(n+1)}.$$

其中 $\operatorname{ord}_{X=1}P(X)=\max\{k\in\mathbb{N}\cup\{0\}\mid (X-1)^k \text{ 整除 } P(X)\}$ 为 $P(X)$ 在 $X=1$ 处的根的重数, 而 $v_2(n+1)=\max\{k\in\mathbb{N}\cup\{0\}\mid 2^k \text{ 整除 } n+1\}$ 为 $n+1$ 含 2 的幂次.

问题来源: Tamás Erdélyi, *Zeros of polynomials with unit coefficients.* The American Mathematical Monthly 2009, Problem 11437.

证明 (Richard Stong) 记 $r=v_2(n+1)$, 设 $n+1=2^rs$, 其中 s 是奇数. 我们用反证法, 假设 $X=1$ 是多项式 $P(X)$ 的至少 2^r 重根, 则 $X=1$ 是 $P(X)$ 的 2^r-1 阶导数 $P^{(2^r-1)}(X)$ 的根. 于是有

$$0=\frac{1}{(2^r-1)!}P^{(2^r-1)}(1)=\sum_{i=2^r-1}^{n}a_i\binom{i}{2^r-1}.$$

由于 $a_i=\pm1\equiv 1 \pmod 2$, 我们得到

$$0=\sum_{i=2^r-1}^{n}a_i\binom{i}{2^r-1}\equiv\sum_{i=2^r-1}^{n}\binom{i}{2^r-1} \pmod 2. \tag{11}$$

利用裂项 $\binom{i}{2^r-1}=\binom{i+1}{2^r}-\binom{i}{2^r}$, 我们有

$$\sum_{i=2^r-1}^{n}\binom{i}{2^r-1}=\binom{n+1}{2^r}=\binom{2^rs}{2^r}. \tag{12}$$

由 (11), (12) 我们得到 $\binom{2^rs}{2^r}$ 是偶数. 但根据 Lucas 定理, $\binom{2^rs}{2^r}$ 是奇数, 矛盾. 于是 $P(X)$ 在 $X=1$ 处根的重数严格小于 2^r, 证毕. □

评注 John E. Littlewood 问: 对于一个次数为 n, 系数为 ±1 的多项式 $P(X)$, 它在 $X=1$ 处的根的重数的最大可能值是多少? (以下我们把系数是 ±1 的多项式称作 Littlewood 多项式.)

例子: 当 $n+1=2^m$ 为 2 的方幂时, 多项式 $P(X)=\prod_{k=0}^{m-1}(X^{2^k}-1)$ 是一个 n 次的 Littlewood 多项式, 并且 $\operatorname{ord}_{X=1}P(X)=m=\log_2(n+1)$.

1997 年, Boyd [2] 证明了: 对任何 $\varepsilon>0$, 存在 $n_0(\varepsilon)$, 使得对任何次数为 $n\geqslant n_0(\varepsilon)$ 的 Littlewood 多项式我们有

$$\operatorname{ord}_{X=1}P(X)\leqslant(1+\varepsilon)\frac{\ln^2 n}{\ln\ln n}.$$

题 6 (2021, Amdeberhan, Moll, Sharma, and Villamizar) 已知正整数 n 满足

$$v_2(\sigma(n))>\log_2 n,$$

求证: n 一定是若干个互不相同的 Mersenne 素数的乘积.
(注: $\sigma(n)=\sum_{d|n}d$ 表示 n 的正约数之和. $v_2(m)$ 表示正整数 m 含 2 的幂次, 即满足 $2^k\mid m$ 的最大的非负整数 k. 我们称满足 $p+1$ 是 2 的方幂的素数 p 为 Mersenne 素数.)

问题来源 [1, Theorem 1.3]

证明 我们先证明两个引理.

引理 1 设素数 p 不是 Mersenne 素数, α 是任何正整数; 或者 p 是 Mersenne 素数, 但正整数 $\alpha\geqslant 2$. 则我们有

$$v_2(\sigma(p^\alpha))\leqslant\log_2(p^\alpha)-1.$$

引理 1 的证明 若 $p=2$ 或者 α 是偶数, 则 $\sigma(p^\alpha)=1+p+p^2+\cdots+p^\alpha$ 是奇数. 此时 $v_2(\sigma(p^\alpha))=0$, 而 $\log_2(p^\alpha)\geqslant\log_2(2)=1$, 故结论成立. 以下设 p 是奇素数且 α 为奇数.

注意

$$\sigma(p^\alpha)=\frac{p^{\alpha+1}-1}{p-1}=(p+1)\cdot\frac{p^{2\cdot\frac{\alpha+1}{2}}-1}{p^2-1}.$$

由于 $4\mid p^2-1$, 由升幂引理, 我们有 $v_2(p^{2\cdot\frac{\alpha+1}{2}}-1)=v_2(p^2-1)+v_2\left(\frac{\alpha+1}{2}\right)$. 于是欲证的不等式等价于

$$\begin{aligned}&\log_2(p^\alpha)\geqslant v_2(\sigma(p^\alpha))+1\\ \Leftrightarrow\ &\log_2(p^\alpha)\geqslant v_2(p+1)+v_2(\alpha+1)\\ \Leftrightarrow\ &p^\alpha\geqslant 2^{v_2(p+1)}\cdot 2^{v_2(\alpha+1)}.\end{aligned}$$

如果 $\alpha\geqslant 3$, 则

$$\begin{aligned}p^\alpha&\geqslant p\cdot 3^{\alpha-1}=p\cdot(1+2)^{\alpha-1}\\ &\geqslant p\cdot(1+(\alpha-1)\cdot 2+2^{\alpha-1})\\ &>p\cdot(2\alpha+2)>(p+1)(\alpha+1)\\ &\geqslant 2^{v_2(p+1)}\cdot 2^{v_2(\alpha+1)},\end{aligned}$$

结论成立. 剩下的情况是 $\alpha = 1$, $p > 2$ 且 p 不是 Mersenne 素数. 此时 $p+1$ 不是 2 的方幂, 故 $2^{v_2(p+1)} \leqslant \frac{p+1}{3}$. 于是

$$p^\alpha = p > \frac{p+1}{3} \cdot 2 \geqslant 2^{v_2(p+1)} \cdot 2^{v_2(\alpha+1)},$$

结论成立. 引理 1 证毕.

引理 2 设 $q_1, q_2, \ldots, q_s$ 是若干个不同的 Mersenne 素数 ($s \geqslant 0$). 则

$$v_2(\sigma(q_1 q_2 \cdots q_s)) < \log_2(q_1 q_2 \cdots q_s) + 1.$$

引理 2 的证明 (周嘉豪) 我们有 $\sigma(q_1 q_2 \cdots q_s) = (1+q_1)(1+q_2)\cdots(1+q_s)$. 由于 $1+q_i$ 均是 2 的方幂, 故 $v_2(\sigma(q_1 q_2 \cdots q_s)) = \log_2((1+q_1)(1+q_2)\cdots(1+q_s))$. 欲证的不等式等价于 $(1+q_1)(1+q_2)\cdots(1+q_s) < 2q_1 q_2 \cdots q_s$, 等价于

$$\prod_{i=1}^{s} \left(1 - \frac{1}{1+q_i}\right) > \frac{1}{2}.$$

根据 Bernoulli 不等式, 我们有

$$\prod_{i=1}^{s} \left(1 - \frac{1}{1+q_i}\right) \geqslant 1 - \sum_{i=1}^{s} \frac{1}{1+q_i},$$

于是只用证明 $\sum_{i=1}^{s} \frac{1}{1+q_i} < \frac{1}{2}$. 由于 $1+q_i$, $(i = 1, 2, \ldots, s)$ 是两两不同的 2 的方幂, 且至少是 4, 故

$$\sum_{i=1}^{s} \frac{1}{1+q_i} < \sum_{k=2}^{\infty} \frac{1}{2^k} = \frac{1}{2}.$$

引理 2 证毕.

回到原题, 根据算术基本定理, 任何一个正整数 n 可以表示成以下的形式:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t} q_1 q_2 \cdots q_s,$$

其中 t, s 是非负整数 (可以为零); $p_1, p_2, \ldots, p_t, q_1, q_2, \ldots, q_s$ 是 $t+s$ 个两两不同的素数; $\alpha_1, \alpha_2 \ldots, \alpha_t$ 是正整数; $q_1, q_2, \ldots, q_s$ 是两两不同的 Mersenne 素数; 而对于每个 $i \in \{1, 2, \ldots, t\}$, 要么 p_i 不是 Mersenne 素数, 要么 p_i 是 Mersenne 素数但 $\alpha_i \geqslant 2$.

根据引理 1, 我们有

$$v_2(\sigma(p_i^{\alpha_i})) \leqslant \log_2(p_i^{\alpha_i}) - 1, \quad i = 1, 2, \ldots, t.$$

根据引理 2, 我们有

$$v_2(\sigma(q_1 q_2 \cdots q_s)) < \log_2(q_1 q_2 \cdots q_s) + 1.$$

将上面所有式子相加并利用 $\sigma(\cdot)$ 是积性函数, 我们得到

$$v_2(\sigma(n)) < \log_2(n) - t + 1.$$

如果 $v_2(\sigma(n)) > \log_2(n)$, 则上式推出 $t < 1$, 只能 $t = 0$, 于是 n 形如

$$n = q_1 q_2 \cdots q_s.$$

所以 n 是若干个两两不同的 Mersenne 素数的乘积 (显然 $n \neq 1$, 故 $s \geqslant 1$). 证毕. □

题 7 我们记 $S_2(n)$ 为 n 在二进制表示下的数字和.

(1) (1992, IMO 预选题) 求证: 对任何实数 $\alpha \in [0, +\infty)$, 以及对于 $\alpha = +\infty$, 均存在一列正整数 $\{n_k\}_{k\geqslant 1}$ 使得

$$\lim_{k\to\infty} \frac{S_2(n_k^2)}{S_2(n_k)} = \alpha.$$

(2) (1978, Stolarsky) 求证: 存在无穷多个正整数 n 使得

$$\frac{S_2(n^2)}{S_2(n)} \leqslant \frac{4(\log_2 \log_2 n)^2}{\log_2 n}.$$

问题来源 [8].

证明 (1) 我们先证明一个引理.

引理 记 $m_k = 2^{2^k-1} - \sum_{j=1}^{k} 2^{2^k-2^j}$, $k \in \mathbb{N}$. 则我们有

$$S_2(m_k) = 2^k - k, \quad S_2(m_k^2) = 1 + \frac{k(k-1)}{2}.$$

引理的证明 对任何整数 $A > a_1 > a_2 > \cdots > a_k \geqslant 0$, 我们有

$$\begin{aligned} 2^A - 2^{a_1} - 2^{a_2} - \cdots - 2^{a_k} &= (2^A - 2^{a_1+1}) + (2^{a_1} - 2^{a_2+1}) + \cdots + (2^{a_{k-2}} - 2^{a_{k-1}+1}) + (2^{a_{k-1}} - 2^{a_k}) \\ &= (\overline{\underbrace{11\cdots1}_{A-a_1-1\text{ 个 }1}\ 0\ \underbrace{11\cdots1}_{a_1-a_2-1\text{ 个 }1}\ 0\cdots\ \underbrace{11\cdots1}_{a_{k-2}-a_{k-1}-1\text{ 个 }1}\ 0\ \underbrace{11\cdots1}_{a_{k-1}-a_k\text{ 个 }1}\ \underbrace{00\cdots0}_{a_k\text{ 个 }0}})_2, \end{aligned}$$

故 $S_2(2^A - 2^{a_1} - 2^{a_2} - \cdots - 2^{a_k}) = (A - a_1 - 1) + (a_1 - a_2 - 1) + \cdots + (a_{k-2} - a_{k-1} - 1) + (a_{k-1} - a_k) = A - a_k - k + 1$. 特别地, 取 $A = 2^k - 1$, $a_j = 2^k - 2^j$, $(j = 1, 2, \ldots, k)$, 我们得到

$$S_2(m_k) = 2^k - k.$$

又, 我们计算 m_k^2 如下:

$$\begin{aligned} m_k^2 &= 2^{2^{k+1}-2} - \sum_{j=1}^{k} 2^{2^{k+1}-2^j} + \left(\sum_{j=1}^{k} 2^{2^k-2^j}\right)^2 \\ &= 2^{2^{k+1}-2} - \sum_{j=1}^{k} 2^{2^{k+1}-2^j} + \sum_{j=1}^{k} 2^{2^{k+1}-2^{j+1}} + \sum_{(i,j):\ 1\leqslant i<j\leqslant k} 2^{2^{k+1}-2^i-2^j+1} \\ &= 2^0 + \sum_{(i,j):\ 1\leqslant i<j\leqslant k} 2^{2^{k+1}-2^i-2^j+1}. \end{aligned}$$

注意 $\{0\} \cup \{2^{k+1} - 2^i - 2^j + 1\}_{1\leqslant i<j\leqslant k}$ 中的数两两不同, 故

$$S_2(m_k^2) = 1 + \frac{k(k-1)}{2}.$$

引理证毕.

回到原题, 我们分以下几步.

第一步: 先考虑 $\alpha \in [0, 1)$ 的情况. 此时记 $\theta = \frac{1+\alpha}{1-\alpha}$, 则 $\theta \geqslant 1$ 并且 $\frac{\theta-1}{\theta+1} = \alpha$. 我们取

$$n_k = 2^{t_k} m_k - 1, \quad \text{其中 } t_k = \lfloor \theta 2^k \rfloor.$$

注意 m_k 是奇数. 如果记 m_k 的二进制表示为 $m_k = (\overline{d_v d_{v-1} \cdots d_1 d_0})_2$, 则个位数 $d_0 = 1$. 我们有

$$n_k = 2^{t_k} m_k - 1 = (\overline{d_v d_{v-1} \cdots d_1 0 \underbrace{11\cdots1}_{t_k \text{ 个 } 1}})_2,$$

所以

$$S_2(n_k) = S_2(m_k) - 1 + t_k = \lfloor \theta 2^k \rfloor + 2^k - k - 1.$$

而 $n_k^2 = 2^{2t_k} m_k^2 - 2^{t_k+1} m_k + 1 = 2^{t_k+1}(2^{t_k-1} m_k^2 - m_k) + 1$. 记 m_k^2 与 m_k 的二进制表示分别为 $m_k^2 = (\overline{c_u c_{u-1} \cdots c_1 c_0})_2$, $m_k = (\overline{d_v d_{v-1} \cdots d_1 d_0})_2$. 则由 m_k 是奇数知 $c_0 = d_0 = 1$. 记 $d'_j = 1 - d_j$, $j = 0, 1, \ldots, v$. 注意 $m_k < 2^{2^k-1}$, 而 $t_k \geqslant 2^k$, 故 $2^{t_k-1} > m_k$. 所以 $v < t_k - 1$, 故 n_k^2 的二进制表示为

$$n_k^2 = (\overline{c_u c_{u-1} \cdots c_1 0 \underbrace{11\cdots1}_{t_k-v-2 \text{ 个 } 1} d'_v d'_{v-1} \cdots d'_1 1 \underbrace{00\cdots0}_{t_k \text{ 个 } 0} 1})_2,$$

我们有

$$\begin{aligned} S_2(n_k^2) &= (S_2(m_k^2) - 1) + (t_k - S_2(m_k)) + 1 \\ &= S_2(m_k^2) - S_2(m_k) + t_k \\ &= \lfloor \theta 2^k \rfloor - 2^k + \frac{k(k+1)}{2} + 1. \end{aligned}$$

于是

$$\lim_{k\to\infty}\frac{S_2(n_k^2)}{S_2(n_k)}=\lim_{k\to\infty}\frac{\lfloor\theta 2^k\rfloor-2^k+\frac{k(k+1)}{2}+1}{\lfloor\theta 2^k\rfloor+2^k-k-1}=\frac{\theta-1}{\theta+1}=\alpha.$$

第二步: 我们来证明如果存在一列正整数 $\{n_k\}_{k\geqslant 1}$ 使得 $\lim_{k\to\infty}\frac{S_2(n_k^2)}{S_2(n_k)}=\alpha$ 并且 $\lim_{k\to\infty}S_2(n_k)=+\infty$, 则存在另一列正整数 $\{N_k\}_{k\geqslant 1}$ 使得 $\lim_{k\to\infty}\frac{S_2(N_k^2)}{S_2(N_k)}=\alpha+1$ 并且 $\lim_{k\to\infty}S_2(N_k)=+\infty$.

事实上, 取

$$N_k=2^{T_k}n_k+1,\quad \text{其中 } T_k=n_k+1.$$

则显然 $S_2(N_k)=S_2(n_k)+1$. (于是从 $\lim_{k\to\infty}S_2(n_k)=+\infty$ 推出 $\lim_{k\to\infty}S_2(N_k)=+\infty$.) 而 $N_k^2=2^{T_k+1}(2^{T_k-1}n_k^2+n_k)+1$. 由于 $2^{T_k-1}>n_k$, 故

$$S_2(N_k^2)=S_2(n_k^2)+S_2(n_k)+1.$$

所以

$$\frac{S_2(N_k^2)}{S_2(N_k)}=\frac{S_2(n_k^2)+S_2(n_k)+1}{S_2(n_k)+1}=\frac{\frac{S_2(n_k^2)}{S_2(n_k)}+1+\frac{1}{S_2(n_k)}}{1+\frac{1}{S_2(n_k)}},$$

利用 $\lim_{k\to\infty}\frac{S_2(n_k^2)}{S_2(n_k)}=\alpha$ 以及 $\lim_{k\to\infty}S_2(n_k)=+\infty$, 我们便推出

$$\lim_{k\to\infty}\frac{S_2(N_k^2)}{S_2(N_k)}=\frac{\alpha+1+0}{1+0}=\alpha+1.$$

由前两步的结论, 我们固定 α 的小数部分, 对 α 的整数部分进行归纳, 便可证明对任何 $\alpha\in[0,+\infty)$, 存在一列正整数 $\{n_k\}_{k\geqslant 1}$ 使得 $\lim_{k\to\infty}\frac{S_2(n_k^2)}{S_2(n_k)}=\alpha$ 并且 $\lim_{k\to\infty}S_2(n_k)=+\infty$.

最后, 对于 $\alpha=+\infty$, 我们取 $n_k=\sum_{j=1}^{k}2^{2^j}$. 则 $n_k^2=\sum_{j=1}^{k}2^{2^{j+1}}+\sum_{(i,j):\ 1\leqslant i<j\leqslant k}2^{2^i+2^j+1}$. 于是 $S_2(n_k)=k$, $S_2(n_k^2)=\frac{k(k+1)}{2}$, 所以 $\lim_{k\to\infty}\frac{S_2(n_k^2)}{S_2(n_k)}=+\infty$. 至此 (1) 小问全部得证.

(2) **(翁斌)** 我们证明以下更强的结论:

(i) 对任何正整数 n, 我们有 $\frac{S_2(n^2)}{S_2(n)}\geqslant\frac{1}{\log_2(n+1)}$;

(ii) 存在常数 $C>0$, 使得存在无穷多个正整数 n, 满足 $\frac{S_2(n^2)}{S_2(n)}\leqslant\frac{C}{\log_2 n}$.

事实上, 由于 n 的二进制表示中有 $S_2(n)$ 个数字是 1, 故 $n\geqslant 2^0+2^1+\cdots+2^{S_2(n)-1}=2^{S_2(n)}-1$, 即 $S_2(n)\leqslant\log_2(n+1)$. 又 $S_2(n^2)\geqslant 1$, 故 $\frac{S_2(n^2)}{S_2(n)}\geqslant\frac{1}{\log_2(n+1)}$. (i) 得证.

对于 (ii), 我们考虑以下多项式

$$f(x)=2x^4+2x^3-x^2+2x+2,$$

直接计算得

$$f(x)^2=4x^8+8x^7+4x^5+17x^4+4x^3+8x+4.$$

这里的关键性质是 $f(x)^2$ 的系数均是非负整数. 取 $n = f(2^k)$, 其中正整数 k 充分大, 则我们有

$$\begin{aligned} S_2(n) &= k + 4, \\ S_2(n^2) &= 8, \\ \log_2(n) &< 4k + 2. \end{aligned}$$

于是我们有

$$\frac{S_2(n^2)}{S_2(n)} = \frac{8}{k+4} < \frac{32}{\log_2(n)}.$$

形如 $n = f(2^k)$, k 充分大的正整数 n 显然有无穷多个, 故 (ii) 得证. 至此 (2) 小问得证.

(用 (2) 小问中的构造, 我们也可以简化 (1) 小问的证明.) □

评注 2015 年, Saunders [7] 证明了对任何正有理数 α, 存在正整数 n 使得 $\frac{S_2(n^2)}{S_2(n)} = \alpha$.

题 8 设 p 是一个奇素数. 我们定义 Fekete 多项式

$$f_p(z) = \sum_{a=0}^{p-1} \left(\frac{a}{p}\right) z^a.$$

这里 $\left(\frac{a}{p}\right)$ 是 Legendre 符号. 求证: $f_p(z)$ 至少有 $\frac{p-1}{2}$ 个根在单位圆周上.

问题来源 [3].

证明 首先我们注意到, 对任何 $k \in \{1, 2, \ldots, p-1\}$, 我们有

$$f_p(e^{2\pi ik/p}) = \sum_{a=0}^{p-1} \left(\frac{a}{p}\right) e^{2\pi ika/p}.$$

当 a 跑遍模 p 的一个完全剩余系时, ka 也跑遍模 p 的一个完全剩余系. 作换元 $b = ka$, 则我们得到

$$\begin{aligned} f_p(e^{2\pi ik/p}) &= \left(\frac{k}{p}\right) \sum_{a=0}^{p-1} \left(\frac{ak}{p}\right) e^{2\pi ika/p} \\ &= \left(\frac{k}{p}\right) \sum_{b=0}^{p-1} \left(\frac{b}{p}\right) e^{2\pi ib/p} \\ &= \left(\frac{k}{p}\right) f_p(e^{2\pi i/p}), \end{aligned}$$

即

$$f_p(e^{2\pi ik/p}) = \left(\frac{k}{p}\right) f_p(e^{2\pi i/p}), \quad k = 1, 2, \ldots, p-1. \tag{13}$$

对任何实数 θ, 我们定义

$$g(\theta)=e^{-p\pi i\theta}f_p(e^{2\pi i\theta}).$$

利用首尾配对, 我们计算得

$$\begin{aligned}g(\theta)&=\sum_{a=1}^{\frac{p-1}{2}}\left(\left(\frac{a}{p}\right)e^{2\pi i(a-p/2)\theta}+\left(\frac{-a}{p}\right)e^{2\pi i(p/2-a)\theta}\right)\\&=\begin{cases}2\sum_{a=1}^{\frac{p-1}{2}}\left(\frac{a}{p}\right)\cos\left((2a-p)\pi\theta\right), & \text{当素数 } p\equiv 1 \pmod 4,\\ 2i\sum_{a=1}^{\frac{p-1}{2}}\left(\frac{a}{p}\right)\sin\left((2a-p)\pi\theta\right), & \text{当素数 } p\equiv 3 \pmod 4.\end{cases}\end{aligned}$$

定义

$$\widetilde{g}(\theta)=\begin{cases}g(\theta), & \text{当素数 } p\equiv 1 \pmod 4,\\ ig(\theta), & \text{当素数 } p\equiv 3 \pmod 4,\end{cases}$$

则 $\widetilde{g}(\theta)$ 是实数. 于是函数 $\widetilde{g}:\mathbb{R}\to\mathbb{R}$ 是一个实值连续函数.

由 (13) 我们有 $g\left(\frac{k}{p}\right)=(-1)^{k-1}\left(\frac{k}{p}\right)g\left(\frac{1}{p}\right)$, $k=1,2,\ldots,p-1$. 于是当 $k\in\{1,2,\ldots,k-2\}$ 且 $\left(\frac{k}{p}\right)=\left(\frac{k+1}{p}\right)$ 时我们有

$$\widetilde{g}\left(\frac{k+1}{p}\right)=-\widetilde{g}\left(\frac{k}{p}\right),$$

由实值连续函数的介值定理, 此时 $\widetilde{g}$ 在区间 $\left[\frac{k}{p},\frac{k+1}{p}\right)$ 上有一个零点. 故此时 f_p 在单位圆周上从 $e^{2\pi ik/p}$ (含) 到 $e^{2\pi i(k+1)/p}$ (不含) 的劣弧上有一个根. 又注意到 $z=1$ 是 $f_p(z)$ 的一个根, 于是 $f_p(z)$ 在单位圆周上的根的个数 (不计重数)

$$\begin{aligned}&\geqslant 1+\#\left\{k\in\{1,2,\ldots,p-2\}\mid\left(\frac{k}{p}\right)=\left(\frac{k+1}{p}\right)\right\}\\&=1+\sum_{k=1}^{p-2}\frac{\left(\frac{k}{p}\right)\left(\frac{k+1}{p}\right)+1}{2}\\&=\frac{p}{2}+\frac{1}{2}\sum_{k=1}^{p-2}\left(\frac{k}{p}\right)\left(\frac{k+1}{p}\right)\\&=\frac{p}{2}+\frac{1}{2}\sum_{k=1}^{p-2}\left(\frac{k^{-1}}{p}\right)\left(\frac{k+1}{p}\right)\\&=\frac{p}{2}+\frac{1}{2}\sum_{k=1}^{p-2}\left(\frac{1+k^{-1}}{p}\right).\end{aligned}\tag{14}$$

注意到当 k 跑遍模 p 的一个既约剩余系时, 数论逆 $k^{-1}\pmod p$ 也跑遍模 p 的一个既约剩余系. 而当 $k\equiv -1\pmod p$ 时 $k^{-1}\equiv -1\pmod p$. 所以当 k 跑遍 $1,2,\ldots,p-2$ 时, $k^{-1}\pmod p$ 也跑

遍 $1, 2, \ldots, p-2 \pmod p$. 于是

$$\sum_{k=1}^{p-2}\left(\frac{1+k^{-1}}{p}\right)=\sum_{a=2}^{p-1}\left(\frac{a}{p}\right)=-1.$$

代入 (14), 我们便证明了 $f_p(z)$ 在单位圆周上至少有 $\frac{p-1}{2}$ 个不同的根. □

评注 2000 年, Conrey, Granville, Poonen, and Soundararajan [3] 证明了 $\lim_{p\to\infty}\frac{N(p)}{p}=c_0$ 存在, 这里 $N(p)$ 是 $f_p(z)$ 在单位圆周上的根的个数 (计重数), 并且 $0.500668 < c_0 < 0.500813$.

题 9 (Erdös and Pomerance) 求证: 对任何正整数 m, n, 区间 $[m, m+10n^{\frac{3}{2}}]$ 中存在 n 个两两不同的正整数 $a_1, a_2, \ldots, a_n$ 使得 $k \mid a_k$, $(k = 1, 2, \ldots, n)$.

问题来源 [4, Theorem 4].

证明 我们将使用 Hall 定理: 设 $G = (V_1, V_2)$ 是一个二部图. 则存在 V_1 到 V_2 的完全匹配当且仅当对于 V_1 的任何一个子集 S, 有 $|N(S)| \geqslant |S|$, 其中 $N(S)$ 是 S 的邻域. 一个推论是: 如果存在常数 C 使得 $d(v_1) \geqslant C \geqslant d(v_2)$ 对任何 $v_1 \in V_1$ 与任何 $v_2 \in V_2$ 成立, 则存在 V_1 到 V_2 的完全匹配.

我们将证明以下的命题: 对任何正整数 m, n, 区间 $(m, m+4n\lfloor\sqrt{n}\rfloor+n]$ 中存在 n 个两两不同的正整数 $a_1, a_2, \ldots, a_n$ 使得 $k \mid a_k$, $(k = 1, 2, \ldots, n)$.

把区间 $(m, m+4n\lfloor\sqrt{n}\rfloor]$ 划分成 $4\lfloor\sqrt{n}\rfloor$ 个长度为 n 的小区间: $(m+(s-1)n, m+sn]$, $s = 1, 2, \ldots, 4\lfloor\sqrt{n}\rfloor$. 对任何整数 j, 我们用 $\langle j\rangle$ 表示 j 所在的小区间. 根据抽屉原理, 对任何 $k \in \{1, 2, \ldots, n\}$, 每个小区间中均存在 k 的倍数.

考虑二部图 $G_0 = (I_0, J_0)$, 其中 $I_0 = \{1, 2, \ldots, n\}$, $J_0 = (m, m+4n\lfloor\sqrt{n}\rfloor] \cap \mathbb{Z}$. 对于 $i \in I_0$, $j \in J_0$, 顶点 i 与 j 相连当且仅当 $i \mid j$. 则 I_0 中每个顶点的度数均 $\geqslant 4\lfloor\sqrt{n}\rfloor$.

如果 J_0 中每个顶点的度数均 $\leqslant \lfloor\sqrt{n}\rfloor$, 则由 Hall 定理, 二部图 G_0 中存在 I_0 到 J_0 的完全匹配, 命题得证. 剩下的情况是: 存在 $j_1 \in J_0$ 使得度数 $d_{G_0}(j_1) > \sqrt{n}$. 则存在 I_0 的子集 K_1, 满足 $|K_1| > \sqrt{n}$, 并且对任何 $k \in K_1$ 有 $k \mid j_1$. 此时我们取 $a_k = j_1 + k$, $(k \in K_1)$, 则有 $k \mid a_k$, $a_k \in \langle j_1\rangle \cup \langle j_1+n\rangle$, 并且 a_k $(k \in K_1)$ 两两不同.

记 $I_1 = I_0 \setminus K_1$, 记 $J_1 = J_0 \setminus (\langle j_1-n\rangle \cup \langle j_1\rangle \cup \langle j_1+n\rangle)$. 考虑二部图 $G_1 = (I_1, J_1)$. 则 I_1 中每个顶点的度数 (在二部图 G_1 中的度数) 均 $\geqslant 4\lfloor\sqrt{n}\rfloor - 3 \geqslant \lfloor\sqrt{n}\rfloor$.

如果 J_1 中每个顶点的度数均 $\leqslant \lfloor\sqrt{n}\rfloor$, 则由 Hall 定理, 二部图 G_1 中存在 I_1 到 J_1 的完全匹配, 命题得证. 剩下的情况是: 存在 $j_2 \in J_1$ 使得度数 $d_{G_1}(j_2) > \sqrt{n}$. 则存在 I_1 的子集 K_2, 满足 $|K_2| > \sqrt{n}$, 并且对任何 $k \in K_2$ 有 $k \mid j_2$. 此时我们取 $a_k = j_2 + k$, $(k \in K_2)$, 则有 $k \mid a_k$, $a_k \in \langle j_2\rangle \cup \langle j_2+n\rangle$, 并且 a_k $(k \in K_1 \cup K_2)$ 两两不同.

注意 $n=|I_0|\geqslant|K_1\cup K_2|>2\sqrt{n}$, 故 $\sqrt{n}>2$. 记 $I_2=I_1\setminus K_2$, 记 $J_2=J_1\setminus(\langle j_2-n\rangle\cup\langle j_2\rangle\cup\langle j_2+n\rangle)$. 我们再考虑二部图 $G_2=(I_2,J_2)$. 则 I_2 中每个顶点的度数 (在二部图 G_2 中的度数) 均 $\geqslant 4\lfloor\sqrt{n}\rfloor-6\geqslant\lfloor\sqrt{n}\rfloor$.

如果 J_2 中每个顶点的度数均 $\leqslant\lfloor\sqrt{n}\rfloor$, 则由 Hall 定理, 二部图 G_2 中存在 I_2 到 J_2 的完全匹配, 命题得证. 剩下的情况是: 存在 $j_3\in J_2$ 使得度数 $d_{G_2}(j_3)>\sqrt{n}$. 则存在 I_2 的子集 K_3, 满足 $|K_3|>\sqrt{n}$, 并且对任何 $k\in K_3$ 有 $k\mid j_3$. 此时我们取 $a_k=j_3+k$, $(k\in K_3)$, 则有 $k\mid a_k$, $a_k\in\langle j_3\rangle\cup\langle j_3+n\rangle$, 并且 a_k $(k\in K_1\cup K_2\cup K_3)$ 两两不同.

一般地, 设 t 是一个正整数. 假设上述方式进行 t 步之后仍未证明命题, 则我们逐步得到了 $j_1,j_2,\ldots,j_t$, $K_1,K_2,\ldots,K_t$, a_k $(k\in K_1\cup K_2\cup\cdots\cup K_t)$. 它们满足: $K_1,K_2,\ldots,K_t$ 是 I_0 的两两不交的子集, $|K_s|>\sqrt{n}$, $(s=1,2,\ldots,t)$, $k\mid a_k$, $a_k\in\langle j_1\rangle\cup\langle j_1+n\rangle\cup\cdots\cup\langle j_t\rangle\cup\langle j_t+n\rangle$, $(k\in K_1\cup\cdots\cup K_t)$. 则 $n=|I_0|\geqslant|K_1\cup\cdots\cup K_t|>t\sqrt{n}$, 故 $t\leqslant\lfloor\sqrt{n}\rfloor$. 记 $I_t=I_0\setminus(K_1\cup K_2\cdots\cup K_t)$, 记 $J_t=J_0\setminus(\langle j_1-n\rangle\cup\langle j_1\rangle\cup\langle j_1+n\rangle\cup\cdots\cup\langle j_t-n\rangle\cup\langle j_t\rangle\cup\langle j_t+n\rangle)$. 考虑二部图 $G_t=(I_t,J_t)$, 则 I_t 中每个顶点在二部图 G_t 中的度数均 $\geqslant 4\lfloor\sqrt{n}\rfloor-3t\geqslant\lfloor\sqrt{n}\rfloor$. 如果 J_t 中每个顶点的度数 $\leqslant\lfloor\sqrt{n}\rfloor$, 则由 Hall 定理, 二部图 G_t 中存在 I_t 到 J_t 的完全匹配, 命题成立. 剩下的情况: 存在 $j_{t+1}\in J_t$ 使得度数 $d_{G_t}(j_{t+1})>\sqrt{n}$. 则存在 I_t 的子集 K_{t+1}, 满足 $|K_{t+1}|>\sqrt{n}$, 并且对任何 $k\in K_{t+1}$ 有 $k\mid j_{t+1}$. 此时我们取 $a_k=j_{t+1}+k$, $(k\in K_{t+1})$, 则 $k\mid a_k$, $a_k\in\langle j_{t+1}\rangle\cup\langle j_{t+1}+n\rangle$.

上述过程有限步必终止 (因为 $t\leqslant\lfloor\sqrt{n}\rfloor$), 而终止的方式只能是在某步时二部图 $G_t=(I_t,J_t)$ 存在 I_t 到 J_t 的完全匹配, 按此匹配定义 a_k $(k\in I_t)$, 结合之前定义好的 a_k $(k\in K_1\cup K_2\cup\cdots\cup K_t)$, 便证明了命题. □

参考文献

[1] Tewodros Amdeberhan, Victor H. Moll, Vaishavi Sharma, and Diego Villamizar, *Arithmetic properties of the sum of divisors*. J. Number Theory 223 (2021), 325–349.

[2] David W. Boyd, *On a problem of Byrnes concerning polynomials with restricted coefficients*. Math. Comp. 66 (1997), 1697–1703.

[3] John B. Conrey, Andrew J. Granville, Bjorn Poonen, and Kannan Soundararajan, *Zeros of Fekete polynomials*. Ann. Inst. Fourier (Grenoble) 50 (2000), no.3, 865–889.

[4] Paul Erdös and Carl Pomerance, *Matching the natural numbers up to n with distinct multiples in another interval*. Nederl. Akad. Wetensch. Proc. Ser. A 83 (1980), 147–161.

[5] Dominik J. Leitner, *Two exponential diophantine equations*. Journal de Théorie des Nombres de Bordeaux 23 (2011), 479–487.

[6] Frank Morley, *Note on the congruence* $2^{4n} \equiv (-1)^n \frac{(2n)!}{(n!)^2}$, *where* $2n+1$ *is a prime*. Ann. of Math. 9 (1894/95), no. 1–6, 168–170.

[7] John C. Saunders, *Sums of digits in q-ary expansions*. Int. J. Number Theory 11 (2015), no. 2, 593–611.

[8] Kenneth B. Stolarsky, *The binary digits of a power*. Proc. Amer. Math. Soc. 71 (1978), no. 1, 1–5.