第七十三届
William Lowell Putnam 数学竞赛

Leonard F. Klosinski　Gerald L. Alexanderson
Mark Krusemeyer

2012 年 12 月 1 日举行了第 73 届 William Lowell Putnam 数学竞赛. 竞赛由 William Lowell Putnam 奖励基金会资助. 该基金会是由 Putnam 夫人为纪念其丈夫而出资设立的. 每年一次的竞赛由美国数学协会 (the Mathematical Association of America) 主办. 按照竞赛规则, 结果如下.

一等奖 25,000 美元奖给哈佛 (Harvard) 大学数学系, 3 名队员每人获 1,000 美元奖金. 二等奖 20,000 美元奖给麻省理工学院 (MIT) 数学系, 3 名队员每人获 800 美元奖金. 三等奖 15,000 美元奖给洛杉矶加州大学 (UCLA) 数学系, 3 名队员每人获 600 美元奖金. 四等奖 10,000 美元奖给石溪 (Stony Brook) 大学 [1] 数学系, 3 名队员每人获 400 美元奖金. 五等奖 5,000 美元奖给卡内基梅隆 (Carnegie-Mellon) 大学数学系, 3 名队员每人获 200 美元奖金.

(按校名的英文序) 杨百翰 (Brigham Young) 大学, 西北 (Northwestern) 大学, 普林斯顿 (Princeton) 大学, 不列颠哥伦比亚 (British Columbia) 大学, 耶鲁 (Yale) 大学的代表队获荣誉提名奖.

个人成绩前 5 名 (其中麻省理工学院 3 名, 哈佛大学 2 名) 每人获 2,500 美元奖金, 并成为 Putnam 会员 (Putnam Fellow). 个人成绩第 6—16 名每人获 1,000 美元奖金. 个人成绩第 17—25 名每人获 250 美元奖金. 第 26 名 (含) 之后的 59 位个人获荣誉提名奖. 并表扬了其他的 17 名个人. (即得分在前 101 位的个人选手获得了奖金或表扬 —— 译注.)

来自加拿大和美国的 578 个学院和大学的 4277 名学生参加了这次竞赛. 有 402 个院校组队参赛. 命题委员会由德克萨斯基督教 (Texas Christian) 大学的 George T. Gilbert (主席), 布林莫尔 (Bryn Mawr) 学院的 Djordje Milićević 和位于 Ann Arbor 的密歇根 (Michigan) 大学的 Hugh Montgomery 组成. 他们出了题, 而且提供了众多解答中最优秀的解答. 与本文不同的解答已在《数学杂志 (Mathematics Magazine)》, 86:1 (2013), p.74—80 中刊出, 并已载于网上 http://dx.doi.org/10.4169/math.mag.86.1.074. [2]

译自: The Amer. Math. Monthly, Vol.120 (2013), No.8, p.679–687, The Seventy-Third William Lowell Putnam Mathematical Competition, Leonard F. Klosinski, Gerald L. Alexanderson, and Mark Krusemeyer.

1) 又称为 State University of New York at Stony Brook, 石溪纽约州立大学.—— 译注

2) 本文自开始至正文 "问题" 之前为译者根据原文编译.—— 译注

问　题

问题 A1　令 $d_1, d_2, \ldots, d_{12}$ 是开区间 $(1, 12)$ 中的实数. 证明, 存在不同的指标 i, j, k, 使得 d_i, d_j, d_k 是一个锐角三角形的边长.

问题 A2　令 $*$ 是一个集合 S 上的一个可交换和结合的二元运算. 假设对于 S 中的每个 x 和 y, 存在 $z \in S$, 使得 $x * z = y$. (这个 z 可以依赖于 x 和 y.) 证明, 若 $a, b, c \in S$, 并且 $a * c = b * c$, 则 $a = b$.

问题 A3　令 $f: [-1, 1] \to \mathbb{R}$ 是一个连续函数, 使得

(i) $f(x) = \dfrac{2 - x^2}{2} f\left(\dfrac{x^2}{2 - x^2}\right)$ 对每个 $x \in [-1, 1]$,

(ii) $f(0) = 1$, 并且

(iii) $\lim\limits_{x \to 1^-} \dfrac{f(x)}{\sqrt{1 - x}}$ 存在并且有限.

证明, f 是唯一的, 并把 $f(x)$ 表成闭形式.

问题 A4　令 $q > 0$ 和 r 是整数, 并令 A 和 B 是实直线上的两个区间. 令 T 是所有 $b + mq$ 的集合, 其中 b 和 m 是整数, 并且 $b \in B$, 并令 S 是所有 $a \in A$ 使得 $ra \in T$ 的集合. 证明, 如果 A 和 B 的长度的乘积小于 q, 则 S 是 A 与某个算术级数的交.

问题 A5　令 $\mathbb{F}_p$ 表示模素数 p 的整数域, 并令 n 是一个正整数. 令 v 是 $\mathbb{F}_p^n$ 中的一个固定的向量, 令 M 是其元在 $\mathbb{F}_p$ 中的 $n \times n$ 矩阵, 并用 $G(x) = v + Mx$ 定义 $G: \mathbb{F}_p^n \to \mathbb{F}_p^n$. 令 $G^{(k)}$ 表示 G 与其本身的 k 重复合, 即, $G^{(1)}(x) = G(x)$, 并且 $G^{(k+1)}(x) = G(G^{(k)}(x))$. 确定所有的数对 p, n, 对于这些数对, 存在 v 和 M, 使得 p^n 个向量 $G^{(k)}(0)$ $(k = 1, 2, \ldots, p^n)$ 各不相同.

问题 A6　令 $f(x, y)$ 是 $\mathbb{R}^2$ 上的一个实值连续函数. 假设, 对于面积为 1 的每个矩形区域 R, $f(x, y)$ 在 R 上的二重积分都等于 0. $f(x, y)$ 必定恒等于 0 吗?

问题 B1　令 S 是从 $[0, \infty)$ 到 $[0, \infty)$ 的一个函数类, 它满足

(i) 函数 $f_1(x) = e^x - 1$ 和 $f_2(x) = \ln(x + 1)$ 在 S 中;

(ii) 若 $f(x)$ 和 $g(x)$ 在 S 中, 则函数 $f(x) + g(x)$ 和 $f(g(x))$ 在 S 中;

(iii) 若 $f(x)$ 和 $g(x)$ 在 S 中, 且对所有 $x \geq 0$ 有 $f(x) \geq g(x)$, 则函数 $f(x) - g(x)$ 在 S 中.

证明, 如果 $f(x)$ 和 $g(x)$ 在 S 中, 那么函数 $f(x)g(x)$ 也在 S 中.

问题 B2　令 P 是一个给定的 (非退化) 多面体. 证明, 存在一个具有下述性质的常数 $c(P) > 0$: 如果 n 个球的体积和等于 V, 并且此 n 个球包含 P 的整个表面, 那么 $n > c(P)/V^2$.

问题 B3　$2n$ 个队的一次循环锦标赛历时 $2n - 1$ 天, 具体如下. 每一天, 每个队与另一队进行一次比赛, 在这 n 次比赛中的每一次中都有一队获胜, 一队败北. 在赛事的进程中, 每个队恰与其余每个队比赛一次. 是否必定能够在每天选取一个获胜队, 而使任何被选取的队不多于一次被选?

问题 B4 假设 $a_0 = 1$, 并且对于 $n = 0, 1, 2, \ldots$ 有 $a_{n+1} = a_n + e^{-a_n}$. 当 $n \to \infty$ 时, $a_n - \log n$ 是否有一个有限的极限? (这里 $\log n = \log_e n = \ln n$.)

问题 B5 证明, 对于任意两个有界函数 $g_1, g_2 : \mathbb{R} \to [1, \infty)$, 存在函数 $h_1, h_2 : \mathbb{R} \to \mathbb{R}$, 使得对每个 $x \in \mathbb{R}$, 有

$$\sup_{s \in \mathbb{R}} \big(g_1(s)^x g_2(s)\big) = \max_{t \in \mathbb{R}} \big(x h_1(t) + h_2(t)\big).$$

问题 B6 令 p 是一个奇素数, 使得 $p \equiv 2 \pmod 3$. 用 $\pi(x) \equiv x^3 \pmod p$ 定义模 p 剩余类的一个置换 π. 证明, π 是一个偶置换, 当且仅当 $p \equiv 3 \pmod 4$.

解　答

在下面每个题号后面 12 个数组成的数组 $(n_{10}, n_9, n_8, \ldots, n_0, n_{-1})$ 中, n_j $(10 \geq j \geq 0)$ 是得分前 189 名参赛者中该题得 j 分的学生人数, 而 n_{-1} 是其中未交该题解答的人数.

A1 (142, 28, 14, 0, 0, 0, 0, 0, 2, 0, 1, 2)

解答 以非减次序排列诸 d_i. 我们证明, 对于某个 i, 有 $d_{i+2}^2 < d_{i+1}^2 + d_i^2$. 如果 $d_3^2 \geq d_2^2 + d_1^2$, 则 $d_3^2 \geq 2d_1^2$. 如果此外还有 $d_4^2 \geq d_3^2 + d_2^2$, 则 $d_4^2 \geq 3d_1^2 = F_4 d_1^2$, 其中 F_i 表示第 i 个 Fibonacci (斐波那契) 数. 由归纳法, 或者我们成功了, 或者 $d_{12}^2 \geq F_{12} d_1^2$.[1] 但是 $F_{12} = 144$, $d_{12} < 12$, 并且 $d_1 > 1$, 因而我们必定对某个 i 有 $d_{i+2}^2 < d_{i+1}^2 + d_i^2$.

A2 (151, 21, 8, 0, 0, 0, 0, 0, 0, 0, 7, 2)

解答 假设 $a * c = b * c$, 并令 $e_a, d \in S$ 满足 $a * e_a = a$ 和 $c * d = e_a$. 则

$$a = a * e_a = a * (c * d) = (a * c) * d = (b * c) * d = b * (c * d) = b * e_a.$$

把 a, b 交换后重复这些步骤, 即有: 存在 $e_b \in S$, 使得 $a * e_b = b * e_b = b$. 因而

$$\begin{aligned} a &= b * e_a \\ &= (a * e_b) * e_a \\ &= a * (e_b * e_a) \\ &= a * (e_a * e_b) \\ &= (a * e_a) * e_b \\ &= a * e_b = b. \end{aligned}$$

A3 (49, 31, 13, 0, 0, 0, 0, 0, 16, 11, 25, 44)

解答 $f(x) = \sqrt{1 - x^2}$.

证明 注意, f 是偶函数, 因而只需在 $(0, 1]$ 上讨论即可. 我们用一系列代换来简化

1) 这里原文为 $d_i^2 \geq F_i d_1^2$, 疑为 $d_{12}^2 \geq F_{12} d_i^2$ 之误. 原文所说的 "成功了", 即指 "对于某个 i, 有 $d_{i+2}^2 < d_{i+1}^2 + d_i^2$".—— 译注

原来的泛函方程. 首先，我们在区间 $[1,\infty)$ 中令 $g(x)=xf(1/x)$. 则

$$g(2x^2-1)=(2x^2-1)f(1/(2x^2-1))=2x^2\frac{2-1/x^2}{2}f\left(\frac{1/x^2}{2-1/x^2}\right)$$
$$=2x^2f(1/x)=2xg(x).$$

现在，对于 $y\geq 0$ 令 $u(y)=g(\cosh y)$. 则 $u(2y)=2\cosh yu(y)$. 最后，对于 $y>0$, 令 $w(y)=u(y)/\sinh y$, 即得 $w(2y)=w(y)$. 因为极限

$$\lim_{y\to 0^+}w(y)=\lim_{y\to 0^+}\frac{f(\operatorname{sech}y)}{\tanh y}=\lim_{x\to 1^-}\frac{f(x)}{\sqrt{1-x^2}}=\frac{1}{\sqrt{2}}\lim_{x\to 1^-}\frac{f(x)}{\sqrt{1-x}}$$

存在，我们即推得 $w(y)$ 是常数，因而对于某个常数 c 有 $f(x)=c\sqrt{1-x^2}$. 从 $f(0)=1$, 我们得到 $f(x)=\sqrt{1-x^2}$.

A4 (5, 0, 0, 0, 0, 0, 0, 0, 0, 2, 97, 85)

解答 假设 A 与 B 长度之积小于 q. 令

$$M=\begin{bmatrix}1 & 0\\ r & q\end{bmatrix},$$

并令 $\Lambda=M\mathbb{Z}^2$, 它是 $\mathbb{Z}^2$ 中的一个格. 考虑 Λ 位于矩形 $A\times B$ 中的元素；我们首先证明，这些格点必定共线. 如果这些格点中有 3 个点不在一条直线上，则以这 3 个点为顶点的三角形的面积至少为 $(1/2)\det(M)=q/2$. 然而，在矩形中的一个三角形的面积至多为此矩形面积的一半，而所论矩形的面积小于 q, 这是一个矛盾. 令 L 表示这些格点所在的那条直线. 在 L 上的格点形成一个算术级数. 此外，矩形 $A\times B$ 是凸的，因而 L 与此矩形之交是一条线段. 集合 S 即为这条线段上的格点的 x 坐标，因而它们形成一段算术级数.

A5 (8, 0, 1, 0, 0, 0, 0, 0, 3, 2, 60, 115)

解答 对于 $n=1$ 和所有的 p, 以及对于 $n=2$, $p=2$, 这样的 v 和 M 存在.

对于 $n=1$, 令 $v=[1]$ 和 $M=[1]$. 对于 $p=n=2$, 令

$$v=\begin{bmatrix}1\\ 0\end{bmatrix},\quad M=\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}.$$

反之，假设 v 和 M 存在. 首先我们观察到，为了得到不同的值，出现 0 的最早的可能是 $G^{(p^n)}(0)$. 这样，

$$v+Mv+M^2v+\cdots+M^{p^n-1}v=0.$$

用 M 相乘，比较两个表达式，得到 $M^{p^n}v=v$. 不过，对所有的 k, 有

$$M^{p^n}(v+Mv+M^2v+\cdots+M^kv)=v+Mv+M^2v+\cdots+M^kv.$$

这样，M^{p^n} 是单位矩阵. 由此即得，M 的极小多项式整除 $x^{p^n}-1=(x-1)^{p^n}$. 由 Cayley-Hamilton (凯莱 – 哈密顿) 定理， M 的极小多项式整除其特征多项式；特别，极小多项式至多为 n 次的，因而 $(M-I)^n=0$.

如果 $n=1$ 和 $p=n=2$ 都不成立，则 $p^{n-1}-1\geq n$, 因而 $(M-I)^{p^{n-1}-1}=0$. 然而，

$$(x-1)^{p^{n-1}-1}=\frac{(x-1)^{p^{n-1}}}{x-1}=\frac{x^{p^{n-1}}-1}{x-1}=1+x+\cdots+x^{p^{n-1}-1}.$$

然而 $G^{(p^{n-1})}(0)=0$, 这是一个矛盾.

A6 (3, 3, 0, 0, 0, 0, 0, 0, 0, 0, 52, 131)

解答 考虑积分

$$F(x,y)=\int_0^x\int_0^y f(u,v)dvdu=\int_0^y\int_0^x f(u,v)dudv.$$

条件给出：对每个 $a>0$, 有 $F(a,1/a)=0$. 关于 a 求导，我们得到

$$0=\frac{\partial F}{\partial x}-\frac{1}{a^2}\frac{\partial F}{\partial y}=\frac{1}{a}\left(a\int_0^{1/a}f(a,v)dv-\frac{1}{a}\int_0^a f(u,1/a)du\right).$$

换言之 (如果需要，我们可以转换和旋转全部设置), 如果我们有两条相互垂直的线段 PA 和 PB, 使得 $|PA|\cdot|PB|=1$, 那么 f 在 PA 和 PB 上的平均值是相等的. 特别，如果 A' 是一个点，使得点 P 是线段 AA' 的中点，那么 f 在 PA 和 PA' 上的平均值是相等的. 通过归纳法论证，如果 $A_1,A_2,\ldots,A_n$ 是沿着一条直线上的等距点，那么 f 在诸线段 A_iA_{i+1} 上的平均值是相等的. 现在假设 f 不恒等于零. 显然 f 不能是常数；取两个点 A 和 B, 满足 $f(A)\neq f(B)$, 并把线段 AB 分成足够多的等长度小区间，以致 f 在包含 A 和 B 的两个小区间上的平均值不相等. 这就产生了一个矛盾.

B1 (174, 9, 0, 0, 0, 0, 0, 0, 3, 2, 0, 1)

解答 由规则 (ii), 有 $f_2(f(x))=\ln(f(x)+1)\in S$ 及 $\ln(g(x)+1)\in S$, 因而

$$\ln(f(x)+1)+\ln(g(x)+1)=\ln(f(x)g(x)+f(x)+g(x)+1)\in S.$$

取 f_1 与上述右端函数的复合，我们得到

$$f(x)g(x)+f(x)+g(x)\in S.$$

因为 $f(x)+g(x)\in S$ 以及对所有 $x\in[0,\infty)$ 有 $f(x)g(x)+f(x)+g(x)\geq f(x)+g(x)$, 即得 $f(x)g(x)\in S$.

B2 (84, 14, 12, 0, 0, 0, 0, 0, 20, 17, 20, 22)

解答 只需对用 "P 的一个特别的面" 来代替 "P 的整个表面" 解相同的问题即可. 令 F 是这样一个面，并令 $\{B_1,\ldots,B_n\}$ 是半径分别为 $r_1,\ldots,r_n$ 的 n 个球的集合，使得 $V=\frac{4}{3}\pi\sum_{j=1}^n r_j^3$, 并且 $F\subseteq\cup_{j=1}^n B_j$. 用 $A(X)$ 表示二维图形 X 的面积，并用 A 表示 F 的面积. 由

$$A(F\cap B_j)\leq\pi r_j^2$$

即得

$$A\leq\sum_{j=1}^n A(F\cap B_j)\leq\pi\sum_{j=1}^n r_j^2=(9\pi/16)^{1/3}\sum_{j=1}^n V_j^{2/3}.$$

此时，由函数 $x^{2/3}$ 的凹性 (或 Jensen (延森) 不等式), 我们推得

$$A\leq(9\pi/16)^{1/3}n\left(\frac{1}{n}\sum_{j=1}^n V_j\right)^{2/3}=(9\pi/16)^{1/3}n^{1/3}V^{2/3},$$

因而 $n\geq\dfrac{16A^3}{9\pi}\dfrac{1}{V^2}$, 以致对满足 $0<c<16A^3/9\pi$ 的任何 $c=c(P)$ 得到结论.

B3 (44, 2, 3, 0, 0, 0, 0, 0, 4, 27, 48, 61)

解答 如果 W_k 是第 k 轮比赛中 n 个胜者的集合，我们需要证明族 $(W_k)_{k=1}^{2n-1}$ 有一组不同的代表.[1] 由 Hall (霍尔) 定理，需证者成立，当且仅当这些集合中任意 s 个的并集至少有 s 个元素. 现假设，这些集合中有 s 个集合，它们的并集 (s 轮比赛的胜者) 至多有 $s-1$ 个元素 (队). 这意味着其余 $2n-s+1$ 个队在我们的 s 轮比赛中全输了，因而他们中任意两个队在这 s 轮比赛中都未相遇. 对于这些 $2n-s+1$ 个队中的参赛队，至少还需 $2n-s$ 轮比赛才能与其他队都比赛到，但是这会使我们的比赛至少进行 $2n$ 轮；多出 1 轮了！

B4 (25, 3, 0, 0, 0, 0, 0, 0, 3, 1, 95, 62)

解答 是的；事实上，所论极限是 0. 令 $w_n = e^{a_n}$. 则 $\log w_{n+1}/w_n = 1/w_n$. 数列 a_n 严格增地趋向于无穷 (如果它有一个有限的极限 L, 我们就会有 $L = L + e^{-L}$), 因而数列 w_n 也是递增地趋向于无穷. 因而 $\log w_{n+1}/w_n$ 趋向于 0, 所以 w_{n+1}/w_n 趋向于 1. 因为当 $\delta \to 0$ 时 $\log(1+\delta) = \delta + O(\delta^2)$, 由此即得

$$\frac{1}{w_n} = \log\left(1 + \frac{w_{n+1}-w_n}{w_n}\right) = \frac{w_{n+1}-w_n}{w_n} + O\left(\frac{(w_{n+1}-w_n)^2}{w_n^2}\right).$$

因而

$$w_{n+1} - w_n = 1 + O\left(\frac{(w_{n+1}-w_n)^2}{w_n}\right).$$

因为对于大的 n, 右端第 1 项大于右端第 2 项, 由此即得对于大的 n 有 $w_{n+1} - w_n \asymp 1$. (一般而言，记号 $f \asymp g$ 意味着 f 和 g 是正的，并且存在正常数 C_1, C_2, 使得 $C_1 \le f/g \le C_2$.) 求和即得，对于大的 n 有 $w_n \asymp n$. 因而，上面列出的关系式给出

$$w_{n+1} - w_n = 1 + O(1/n).$$

对此求和，我们发现 $w_n = n + O(\log n)$. 因而

$$a_n - \log n = \log \frac{w_n}{n} = \log\big(1 + O((\log n)/n)\big) = O((\log n)/n).$$

B5 (2, 0, 1, 0, 0, 0, 0, 0, 0, 1, 18, 167)

解答 注意，每个形如

$$f(x) = \sup_{t\in\mathbb{R}}(xh_1(t) + h_2(t)) \tag{1}$$

的函数 $f\colon \mathbb{R} \to \mathbb{R}$ 是凸的，其中 $h_1, h_2\colon \mathbb{R} \to \mathbb{R}$ 是两个任意的函数，只要对于每个 $x \in \mathbb{R}$, (1) 右端的上确界存在. 事实上，对于每个 $x, y \in \mathbb{R}$ 和每个 $\lambda \in (0,1)$, 有

$$\begin{aligned}
&\lambda f(x) + (1-\lambda) f(y)\\
&= \sup_{t\in\mathbb{R}}(\lambda x h_1(t) + \lambda h_2(t)) + \sup_{t\in\mathbb{R}}\big((1-\lambda) y h_1(t) + (1-\lambda) h_2(t)\big)\\
&\ge \sup_{t\in\mathbb{R}}\Big(\big((\lambda x + (1-\lambda)y\big)h_1(t) + \big(\lambda + (1-\lambda)\big)h_2(t)\Big)\\
&= f(\lambda x + (1-\lambda)y).
\end{aligned}$$

1) 即存在 $w_k \in W_k$, $k = 1, 2, \ldots, 2n-1$, 使得诸 w_k 互不相同.—— 译注

反之亦真，即，每个凸函数 $f:\mathbb{R}\to\mathbb{R}$ 对于某两个 $h_1, h_2:\mathbb{R}\to\mathbb{R}$ 满足 (1)；事实上，我们断言，我们可以选取 h_1 和 h_2，使得它们满足更强一些的条件

$$f(x)=\max_{t\in\mathbb{R}}(xh_1(t)+h_2(t)). \tag{2}$$

事实上，因为 f 是凸的，我们知道：f 是一个连续函数，并且在每一点处具有左导数和右导数，它们对任意满足 $a<b$ 的 $a, b\in\mathbb{R}$，满足

$$f'_-(a)\le f'_+(a)\le\frac{f(b)-f(a)}{b-a}\le f'_-(b).$$

由此即得，对于每个 $t\in\mathbb{R}$ 有

$$f(x)\ge(x-t)f'_-(t)+f(t),$$

当 $t=x$ 时等号成立．立即得到，当

$$h_1(t)=f'_-(t),\quad h_2(t)=f(t)-tf'_-(t)$$

时 (2) 式成立．

令 $g_1, g_2:\mathbb{R}\to[1,\infty)$ 如问题的叙述中所述．在上面讨论的第 1 部分中，我们已经证明了

$$f(x)=\sup_{t\in\mathbb{R}}\big(x\log g_1(t)+\log g_2(t)\big)$$

定义了一个凸函数 $f:\mathbb{R}\to\mathbb{R}$，因为 $\log g_1, \log g_2:\mathbb{R}\to\mathbb{R}$ 是有界的．因而 $e^{f(x)}$ 也是凸的．这是众所周知的，并且从

$$\lambda e^{f(x)}+(1-\lambda)e^{f(y)}\ge e^{\lambda f(x)+(1-\lambda)f(y)}\ge e^{f(\lambda x+(1-\lambda)y}$$

也可得到，其中第 1 步利用了指数函数的凸性，第 2 步利用了函数 f 的凸性以及指数函数的单调性．由于 $e^{f(x)}$ 是一个凸函数，由 (2) 即得，对于某两个函数 $h_1, h_2:\mathbb{R}\to\mathbb{R}$，有

$$e^{f(x)}=\max_{t\in\mathbb{R}}\big(xh_1(t)+h_2(t)\big).$$

这等价于我们所要证明的．

B6 (15, 0, 0, 0, 0, 0, 0, 0, 3, 10, 33, 128)

解答 对于由 π 所固定的 3 类 0, 1 和 -1，考虑 $a\ne0,1,-1$．包含 a 的循环 (cycle) 与包含 $-a\ne a\,(\mathrm{mod}\,p)$ 的循环有相同的长度．这样，π 的奇偶性由包含 a 和 $-a$ 两者的那些循环所决定．类似地，包含 a 的循环与包含 $a^{-1}\ne a\,(\mathrm{mod}\,p)$ 的循环有相同的长度．这样，我们只剩下包含 a, $-a$ 和 a^{-1} 的循环了．那么，如果从 a 到 $-a$ 要应用 k 次 π，则此循环有长度 $2k$；另一方面，替代 $-a$，相同的论证也适用于 a^{-1}，因而 $-a\equiv a^{-1}\,(\mathrm{mod}\,p)$，即 $a^2\equiv-1\,(\mathrm{mod}\,p)$．对于这样的 a，$a^3\equiv-a\,(\mathrm{mod}\,p)$，因而 $k=1$．因为乘法群 $(\mathrm{mod}\,p)$ 是 $p-1$ 阶循环的，或者，由 Euler (欧拉) 准则，当 $p\equiv3\,(\mathrm{mod}\,4)$ 时不存在这样的 a，当 $p\equiv1\,(\mathrm{mod}\,4)$ 时有两个这样的 a 形成阶为 2 的循环．因而，在前一情形 π 是偶的，在后一情形 π 是奇的．

(陆柱家 译　　陆昱 校)