数学新星网 ※ 学生专栏
www.nsmath.cn/xszl

2020 年伊朗 TST (第二轮) 试题解答与评析

梁敬勋

(杭州学军中学, 310012)

指导教师: 边红平

伊朗数学奥林匹克国家队选拔一般有三轮共 18 个题. 伊朗的试题总体质量很高, 有些题目难度极大, 总是给我们的竞赛选手留下深刻的印象.

本文是 2020 年伊朗国家队选拔赛 (第二轮) 试题的解答. 由于能力有限, 难免有不当疏漏之处, 敬请读者批评指正.

I. 试 题

1. 称首一多项式 $p(x) \in \mathbb{Z}[x]$ 为"模 n 无平方因子的", 若不存在多项式 $Q(x), R(x) \in \mathbb{Z}[x]$, 且 Q 非常数, 使得 $P(x) = Q(x)^2 R(x) \pmod{n}$. 给定素数 p 及整数 $m \geq 2$, 求模 p 无平方因子的 m 次首一多项式 $P(x)$ 的个数, 其中 p 的系数取自 $\{0, 1, \cdots, p-1\}$.

2. 甲乙两人轮流对一个 2020×2020 的棋盘上的方格进行染色, 甲先开始每次操作可以选择一个未被着色的方格, 将它染黑并得到等同于此时它所在的行与列之并中黑格数目的分数. 当所有格均染黑时游戏结束, 得分高的人获胜. 问: 甲乙谁有必胜策略? 他至多可保证比另一方多得多少分?

3. 给定 $\triangle ABC$ 及外接圆 Γ, 点 E, F 分别为 $\angle B, \angle C$ 平分线与对边的交点, I 为内心, K 为 AI 与 EF 的交点. 设 T 为 Γ 中弧 BAC 上的中点. 设 Γ 与 $A-$ 中线和 $\odot(AEF)$ 的另一交点分别为 X, S, S' 为 S 关于 AI 的对称点. J 为 $\odot(AS'K)$ 与 AX 的另一交点. 证明: T, J, I, X 四点共圆.

4. 等腰 $\triangle ABC$ ($AB = AC$) 内心为 I. 圆 ω 过 C 且与 AI 切于 I, ω 与 $AC, \odot(ABC)$ 的另一交点分别为 Q, D, M, N 分别为 AB, CQ 的中点. 证明: AD, BC, MN 三线共点.

修订日期: **2020-12-01.**

5. 对每个 $k \in \mathbb{N}_+, k > 1$, 证明: 存在 $x \in \mathbb{R}$, 使得对任一正整数 $n < 1398$, 有

$$\{x^n\} > \{x^{n-1}\} \Leftrightarrow k|n.$$

6. p 为奇素数, 求所有 $\frac{p-1}{2}$ 元组 $(x_1, \cdots, x_{\frac{p-1}{2}}) \in \mathbb{Z}_p^{\frac{p-1}{2}}$, 使

$$\sum_{i=1}^{\frac{p-1}{2}} x_i \equiv \sum_{i=1}^{\frac{p-1}{2}} x_i^2 \equiv \cdots \equiv \sum_{i=1}^{\frac{p-1}{2}} x_i^{\frac{p-1}{2}} \pmod{p}.$$

Ⅱ. 解答与评注

1. 称首一多项式 $p(x) \in \mathbb{Z}[x]$ 为"模 n 无平方因子的", 若不存在多项式 $Q(x), R(x) \in \mathbb{Z}[x]$, 且 Q 非常数, 使得 $P(x) = Q(x)^2 R(x) \pmod{n}$. 给定素数 p 及整数 $m \geq 2$, 求模 p 无平方因子的 m 次首一多项式 $P(x)$ 的个数, 其中 p 的系数取自 $\{0, 1, \cdots, p-1\}$.

解 所求为 $p^m - p^{m-1}$.

固定素数 p, 用 $f(m)$ 表示满足条件的 m 次首-多项式的个数. 补充约定 $f(0) = 1, f(1) = p$, 在域 $\mathbb{Z}_p$ 上考察多项式.

对 $m \geq 2$, 每个 m 次首一多项式 $P(x)$ 可以在 $\mathbb{Z}_p$ 中唯一分解为 $\mathbb{Z}_p[x]$ 上的首一不可约多项式的积:

$$P(x) = P_1(x)^{\alpha_1} P_2(x)^{\alpha_2} \cdots P_k(x)^{\alpha_k} \pmod{p},$$

$\alpha_1, \alpha_2, \cdots, \alpha_k \in \mathbb{N}^+, p_1, p_2, \cdots, p_k$ 为互异的首一不可约多项式.

令

$$Q(x) = p_1(x)^{\left[\frac{\alpha_1}{2}\right]} p_2(x)^{\left[\frac{\alpha_2}{2}\right]} \cdots p_k(x)^{\left[\frac{\alpha_k}{2}\right]},$$

$$R(x) = p_1(x)^{\alpha_1 - 2\left[\frac{\alpha_1}{2}\right]} p_2(x)^{\alpha_2 - 2\left[\frac{\alpha_2}{2}\right]} \cdots p_k(x)^{\alpha_k - 2\left[\frac{\alpha_k}{2}\right]},$$

则

$$P(x) = Q(x)^2 R(x) \pmod{p}.$$

我们称在 $\mathbb{Z}_p$ 上 p 对应于 (Q, R).

易见 R 为模 p 无平方因子的多项式, 且对任一这样的 R 及模 p 首一多项式 Q. 若

$$\deg R + 2 \deg Q = m,$$

则 $\mathbb{Z}_p$ 上有唯一的 p 对应于 (Q,R). ($\mathbb{Z}_p[x]$ 的唯一分解定理起了巨大作用)

由于 P 共有 p^m 个, 对每个 $0\le R\le \frac{m}{2}$, 使 $\deg Q=R$ 的 (Q,R) 有 $p^R f(m-2k)$ 个. 由上述双射, 有

$$p^m=\sum_{k=0}^{[\frac{m}{2}]}p^k f(m-2k),\forall m\ge 2 \tag{1}$$

下归纳证明: $f(m)=p^m-p^{m-1},m\ge 2$.

由 $p^2=f(2)+pf(0)$ 知 $f(2)=p^2-p$. 假设命题对小于 m 的正整数均成立, 等于 m 时由 (1),

$$\begin{aligned}
f(m)&=p^m-\sum_{k=1}^{\left[\frac{m}{2}\right]}p^k f(m-2k)\\
&=p^m-\sum_{k=1}^{\left[\frac{m}{2}\right]-1}p^{m-k-1}(p-1)-p^{[\frac{m}{2}]}f\left(m-2\left[\frac{m}{2}\right]\right)\\
&=p^m-(p-1)p^{m-[\frac{m}{2}]}\frac{1-p^{\left[\frac{m}{2}\right]-1}}{1-p}-p^{\lceil\frac{m}{2}\rceil}\\
&=p^m+p^{\lceil\frac{m}{2}\rceil}-p^{m-1}-p^{\lceil\frac{m}{2}\rceil}=p^m-p^{m-1}.
\end{aligned}$$

由归纳原理, 结论成立. 故所求 m 次首一多项式有 p^m-p^{m-1} 个. □

评注 通常考虑多项式的重因式是要通过研究 $(f(x),f'(x))$ 来处理的. 但本题中 $(f'(x),f(x))=1$ 这一刻画使 $f(x)$ 比较孤立不利于计数, 因此要回到定义上. 本题的关键是 $\mathbb{Z}_p[x]$ 上的唯一分解定理. 因为 $\mathbb{Z}_p[x]$ 为域, 故 $\mathbb{Z}_p[x]$ 可建立带余除法, 从而有与 $Q[x],R[x]$ 类似的唯一分解定理. 本题较为简单.

2. 甲乙两人轮流对一个 2020×2020 的棋盘上的方格进行染色, 甲先开始每次操作可以选择一个未被着色的方格, 将它染黑并得到等同于此时它所在的行与列之并中黑格数目的分数. 当所有格均染黑时游戏结束, 得分高的人获胜. 问: 甲乙谁有必胜策略? 他至多可保证比另一方多得多少分?

解 乙必胜, 且至多可保证比甲多 $\frac{1}{2}\times 2020\times 2020=2040200$ 分.

一方面, 乙采取如下策略可保证比甲多 2040200 分: 易见从左到右第 1010 列的右边界 l 为整个方格表的对称轴, 每个方格在关于 l 的对称下有唯一的像.

甲每次染色后, 乙就染黑甲染的格在关于 l 的对称下的像, 则:

- 只要甲可染, 则乙的操作就是可进行的.
- 乙每轮得分恰比甲多 1. 这是因为甲该轮染的格计入乙的得分.

由于共进行 $\frac{1}{2}\times 2020\times 2020$ 轮, 故乙至少可比甲多 2040200 分.

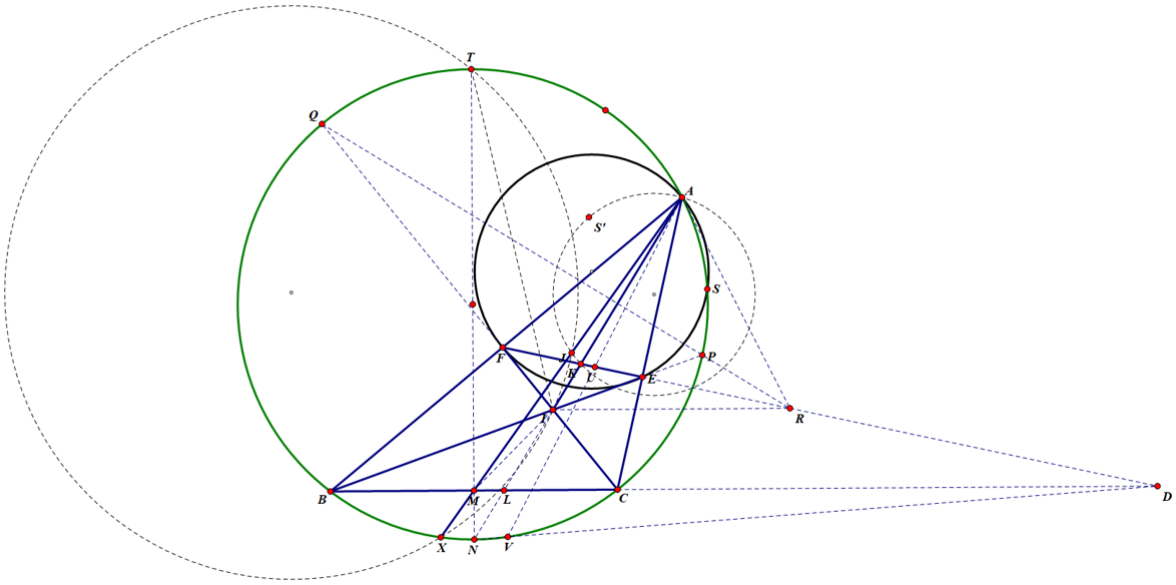
另一方面, 甲采取如下策略可使乙至多比甲多 2040200 分.

每次轮到甲染色时, 甲染黑格 a, 使得在剩下的可染色的格中, 染黑格 a 得分最高. 这时, 无论乙如何染色, 其除格 a 之外的得分不超过 a, 连同格 a 至多比甲多一分. 从而每轮乙至多比甲多一分, 共多至多 2040200 分.

综上, 乙至多可保证比甲多 2040200 分. □

评注 通常"中心对称"型配对可立刻说明乙不败, 从而乙必然是必胜一方. 由于总共操作次数为偶数, 从而可看成若干个"甲, 乙"的轮. 每一轮中甲先乙后, 甲先手可以抢占有利位置, 乙后手可以借助甲新染的格, 在这样的分析下可以很容易构造两者的策略.

3. 给定 $\triangle ABC$ 及外接圆 Γ, 点 E, F 分别为 $\angle B, \angle C$ 平分线与对边的交点, I 为内心, K 为 AI 与 EF 的交点. 设 T 为 Γ 中弧 BAC 上的中点. 设 Γ 与 $A-$ 中线和 $\odot(AEF)$ 的另一交点分别为 X, S, S' 为 S 关于 AI 的对称点. J 为 $\odot(AS'K)$ 与 AX 的另一交点. 证明: T, J, I, X 四点共圆.



证明 设 BC 中点为 M, T 在 Γ 中对径点为 N. 设 $AT \cap BC = D$, 则由角平分线及外角平分线定理知

$$\frac{AF}{FB} \cdot \frac{BD}{DC} \cdot \frac{CE}{EA} = \frac{AC}{CB} \frac{AB}{AC} \cdot \frac{BC}{AB} = 1.$$

由梅氏定理之逆即有 D, E, F 共线.

设 AX 关于 $\angle BAC$ 的等角线 (共轭中线) 与 EF 交于 U, 与 Γ 交于另一点 V. 熟知四边形 $ABVC$ 为调和四边形.

断言 1 A,S,U,K 共圆.

证明 设 $AI\cap BC=L$, 则

$$\frac{BL}{LC}=\frac{BA}{AC}=\frac{BD}{DC}\Rightarrow N(BC;LD)=-1=N(BC;AV)$$

又 N,L,A 共线, 故 N,V,D 共线. 而

$$\sphericalangle(SF,FD)=\sphericalangle(SA,AE)=\sphericalangle(SB,BC)\Rightarrow B,F,S,D\text{共圆},$$

$$\sphericalangle(SV,VA)=\sphericalangle(SV,VD)=\sphericalangle(SA,AK)\leftrightarrow S,U,V,D\text{共圆},$$

从而

$$\sphericalangle(SU,UD)=\sphericalangle(SV,VD)=\sphericalangle(SA,AK)\Rightarrow S,A,K,U\text{共圆}.$$

由断言 1, $\odot(AKS)$ 与 $\odot(AKS')$ 关于 AN 对称, AU 与 AX 关于 AN 对称, 故 J 与 U 关于 AN 对称.

断言 2 M,I,U 共线.

证明 设 BI,CI 为 Γ 另一交点为 P,Q.PQ 与过 A 的 Γ 切线交于 R. 对圆内接六边形 $AACQPB$, 用 Pascal 定理:

$$AA\cap QP=R,AC\cap PB=E,CQ\cap BA=F,$$

故 F,E,R 共线.

又熟知 $PA=PI,QA=QI$, 故 PQ 为 AI 中垂线. 故 $RA=RI$. 从而

$$\begin{aligned}\sphericalangle(AI,IR)=\sphericalangle(AR,AI)&=\sphericalangle(AR,AC)+\sphericalangle(AC,AI)\\&=\sphericalangle(AB,BC)+\sphericalangle(AI,AB)\\&=\sphericalangle(AI,BC).\end{aligned}$$

故 $IR\parallel BC$. 从而

$$I(CB;MR)=-1=A(BC;VA)=(FE;UR)=I(FE;UR).$$

又 I,F,C 共线; I,B,E 共线; I,R,R 共线, 故 I,M,U 共线. 现在, 由

$$\begin{aligned}NM\cdot NT=NB^2=NI^2&\Rightarrow\triangle NIM\sim\triangle NTI\\&\Rightarrow\sphericalangle(IN,IT)=\sphericalangle(IM,MN).\end{aligned}$$

故

$$\begin{aligned}\sphericalangle(JI,IT)&=\sphericalangle(JI,AI)+\sphericalangle(AI,IT)\\&=\sphericalangle(AI,UI)+\sphericalangle(IM,MN)\\&=\sphericalangle(AI,MN)=\sphericalangle(AX,XT)\end{aligned}$$

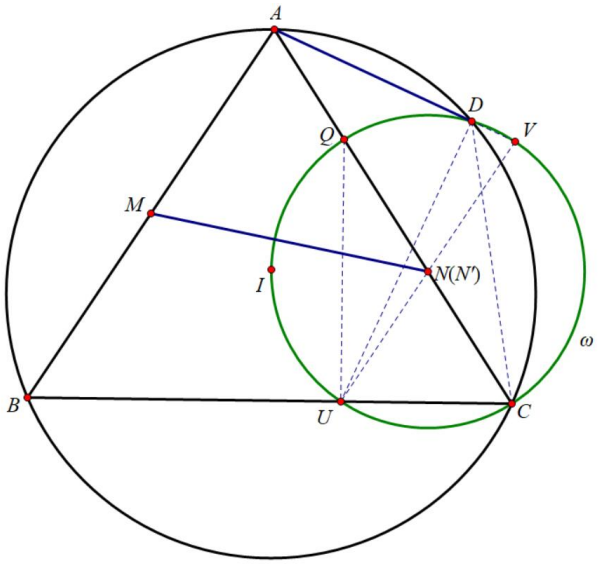
$$\Rightarrow J,I,X,T\text{共圆}.$$

故得证! □

评注 本题点的复杂度都比较高, J 处理起来非常困难. 点 J 用 $\angle AJK=\angle ASK$ 来定义显然是不好的, 需要消去 J 或改造 J 的定义. 在进行一系列的尝试性导角后, 如果作出了共轭中线, 则容易猜想 A,K,U,S 共圆, 但本题的困难之处在于 U,K 在图上很接近, (纸笔做图) 很难从图形中得到一些证据来确认 A,S,U,K 共圆; 而这一点又不容易证, U 的定义比较复杂, 使人对这一结论缺乏信心, 做到这很容易卡住. 幸好 U,J,M 共线是好证的 (与一个出现过的题: QE,PF,IM 共点做法完全相同), 从而只要 U 在 $\odot(ASK)$ 上, 这确信了这一结论.

总的来说, 本题点的定义较复杂, 能做的推理不多, 依赖于对结论的观察 (个人感觉 J 关于 AI 对称点为 U 这种清楚但不简单的点是很难事先预测的), 因此需要较多时间探索. 另外, 本题也可用反演法 (以 A 为中心的反演反射),(本质上区别不大), 这使 A,S,U,K 共圆的对应结论更清楚一点.

4. 等腰 $\triangle ABC$ $(AB=AC)$ 内心为 I. 圆 ω 过 C 且与 AI 切于 I, ω 与 $AC,\odot(ABC)$ 的另一交点分别为 Q,D, M,N 分别为 AB,CQ 的中点. 证明: AD,BC,MN 三线共点.



证明 设 ω 圆心为 N', 则由 ω 与 AI 相切知 $N'I\perp AI$, 即 $N'I\parallel BC$. 故

$$\sphericalangle(N'C,CI)=\sphericalangle(CI,IN')=\sphericalangle(CI,BC)=\sphericalangle(AC,CI)$$

$$\Rightarrow A,N',C\text{ 共线}.$$

即 CQ 过 N', 故 $N \equiv N'$.

设 ω 与 BC, AD 分别交于另一点 U, V, 则由直径 CQ 有 $QU \perp UC$. 从而

$$\sphericalangle(N'C, CI) = \sphericalangle(DC, CU) = \sphericalangle(DA, AB) \Rightarrow AB \parallel UV.$$

$$\begin{aligned}\sphericalangle(VD, DU) &= \sphericalangle(VD, DC) + \sphericalangle(DC, DU)\\ &= \sphericalangle(AB, BC) + \sphericalangle(QC, QU)\\ &= \sphericalangle(BC, AC) + \sphericalangle(QC, QU)\\ &= \sphericalangle(BC, QU) = \frac{\pi}{2}\end{aligned}$$

即 UV 为 ω 直径, 故 N 为 UV 中点.

令 $AB \parallel UV, M, N$ 分别为 AB, UV 中点, 故 AV, MN, BU 共点, 即 AD, MN, BC 共点. 故得证. □

评注 本题没有特别复杂的点, 只要作图时发现 N 为圆心, 各点的相关性质就很容易描述出来. 但证明三线共点是通过"线段位似"来证的, 不太常规, 需要对对图形进行一些探索. 本题较为简单.

5. 对每个 $k \in \mathbb{N}_+, k > 1$, 证明: 存在 $x \in \mathbb{R}$, 使得对任一正整数 $n < 1398$, 有

$$\{x^n\} > \{x^{n-1}\} \Leftrightarrow k \mid n.$$

证明 1 记 $m = 1397$.

引理 任取 a_n, b_n 使 $0 < a_n < b_n < 1$ $(1 \leq n \leq m)$, 存在 $M_1, M_2, \cdots, M_m \in \mathbb{N}_+$, 使得

$$\begin{aligned}\left((M_1 + a_1)^{\frac{1}{1}}, (M_1 + b_1)^{\frac{1}{1}}\right) \supseteq \left((M_2 + a_2)^{\frac{1}{2}}, (M_2 + b_2)^{\frac{1}{2}}\right) \supseteq \cdots\\ \supseteq \left((M_m + a_m)^{\frac{1}{m}}, (M_m + b_m)^{\frac{1}{m}}\right)\end{aligned} \tag{1}$$

证明 待定 M_1 (充分大), 递归地选取 M_k : 设 $M_1, \cdots, M_k$ 已取好, 要取 M_{k+1} 使

$$\left((M_k + a_k)^{\frac{1}{k}}, (M_k + b_k)^{\frac{1}{k}}\right) \supseteq \left((M_{k+1} + a_{k+1})^{\frac{1}{k+1}}, (M_{k+1} + b_{k+1})^{\frac{1}{k+1}}\right).$$

即

$$(M_k + a_k)^{\frac{k+1}{k}} - b_{k+1} > M_{k+1} > (M_k + a_k)^{\frac{k+1}{k}} - a_{k+1}$$

欲满足的 $M_{k+1} \in N_+$ 存在, 仅需

$$(M_k + a_k)^{\frac{k+1}{k}} - (M_k + a_k)^{\frac{k+1}{k}} > 2 \tag{2}$$

由取法,

$$(M_k+a_k)^{\frac{1}{k}}>M_1+a_1\Rightarrow M_k>M_1^k-1>\frac{1}{2}M_1^k,$$

从而

$$\begin{aligned}&(M_k+b_k)^{\frac{k+1}{k}}-(M_k+a_k)^{\frac{k+1}{k}}\\=&(M_k+a_k)^{\frac{k+1}{k}}\left(1+\frac{b_k-a_k}{M_k+a_k}\right)^{\frac{k+1}{k}}\geq M_k^{\frac{k+1}{k}}\left(1+\frac{k+1}{k}\frac{b_k-a_k}{M_k+a_k}\right)\\&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\text{(伯努利不等式)}\\\leq&\frac{k+1}{2k}(b_k-a_k)M_k^{\frac{1}{k}}>\frac{k+1}{2k}(b_k-a_k)\frac{1}{2}M_1.\end{aligned}$$

仅需

$$M_1>8k\frac{1}{(k+1)(b_k-a_k)}.$$

上式右边仅与 k,a_k,b_k 有关, 在 M_1 充分大时, 上式成立, 故 (2) 符合.

由归纳原理, 结论成立.

我们可以证明更强结论:

任取 $\{1,2,\cdots,m\}$ 的排列 σ, $\exists\, x\in\mathbb{R}$, 使

$$\{x^{\sigma(1)}\}<\{x^{\sigma(2)}\}<\cdots<\{x^{\sigma(m)}\}.$$

事实上, 记 $\tau\circ\sigma=id$, 则令 $\{x^i\}\in\left(\frac{\tau(i)-1}{m},\frac{\tau(i)}{m}\right)$ 即可.

由断言, 存在 $M_1,\cdots,M_m$, 使得

$$\begin{aligned}&\left(\left(M_i+\frac{\tau(i)-1}{m}\right)^{\frac{1}{i}},\left(M_i+\frac{\tau(i)}{m}\right)^{\frac{1}{i}}\right)\\&\qquad\supseteq\left(\left(M_{i+1}\frac{\tau(i+1)-1}{m}\right)^{\frac{1}{i+1}},\left(M_{i+1}\frac{\tau(i+1)}{m}\right)^{\frac{1}{i+1}}\right)\end{aligned}$$

这里 $1\leq i\leq m-1$.

取 $x\in\left(\left(M_m+\frac{\tau(m)-1}{m}\right)^{\frac{1}{m}},\left(M_m+\frac{\tau(m)}{m}\right)^{\frac{1}{m}}\right)$, 则由取法

$$\begin{aligned}&\left(M_n+\frac{\tau(n)-1}{m}\right)^{\frac{1}{n}}<x<\left(M_n+\frac{\tau(n)}{m}\right)^{\frac{1}{n}}\qquad 1\leq n\leq m\\\Rightarrow&\{x\}^{\frac{1}{n}}\in\left(\frac{\tau(n)-1}{m},\frac{\tau(n)}{m},\right),\end{aligned}$$

符合, 这个 x 即为所求. □

评注 本题的主要难点在于变量太少, 仅有一个 x. 虽然 $x\in\mathbb{R}$ 可连续变化, 蕴含无限的可能, 但实际操作中如果先取好 x, 则很难控制 $\{x^n\}$.

一种常见的方法是用递推数列保证 $x^n+\alpha^n+\beta^n\in\mathbb{Z},\forall n\in\mathbb{N}_+$, 其中

$\{\alpha\},\{\beta\}<1$. 再用 $\{x^n\}=\{-\alpha^n-\beta^n\}$ 来打开小数部分, 但这很难实现本题中吩咐按递增的分布.

本题的处理方法是扩充参数: 将 $\{x^n\}$ 的大小关系转化为具体的

$$M_k+a_K<x_k<M_k+b_k.$$

引入一个待取的参数 M_k, 降低单次选取的困难, 从而区间 $\left((M_k+a_k)^{\frac{1}{k}},(M_k+b_k)^{\frac{1}{k}}\right)$ 长度不断变短实现目的.

证明2 我们证明更强的结论: 对于 $1,2,\cdots,n$ 的任意排列 $\sigma(1),\sigma(2),\cdots,\sigma(n)$, 我们都能找到一个 x 使得 $\alpha_1\sim\alpha_n,\beta_1\sim\beta_n$.

(i). 取一个足够大的 M, 令

$$\alpha_1=M+(\gamma(1)-1)\cdot\frac{1}{n},\beta_1=M+\gamma(1)\cdot\frac{1}{n}\ (\alpha_1,\beta_1\in[m,m+1]),$$

则有

$$\beta_1-\alpha_1=\frac{1}{n}>2\left(\sqrt{m^2+1}-1\right).$$

(ii). 设 α_k,β_k 满足:

$$\beta_k-\alpha_k>2\left(\sqrt[k+1]{m^{k+1}}-1\right),\alpha_{k-1}\le\alpha_k<\beta_k\le\beta_{k-1}.\ (\alpha_0=M,\beta_0=M+1),$$

则必定存在一个 m_k, 满足 $\sqrt[k]{m_k},\sqrt[k]{m^k+1}$ 均在区间 (α_k,β_k) 中. $(m_k\in\mathbb{N}_+)$ (这是因为当 $m>M^k$ 时, $\sqrt[k]{m_k+1}-\sqrt[k]{m_k}<\sqrt[k]{M_k+1}-M<\frac{1}{2}(\beta_k-\alpha_k)$, 由区间的长度可知, 上面的结论成立).

我们令

$$\alpha_{k+1}=\sqrt[k+1]{m_k+(\gamma(k+1)-1)\cdot\frac{1}{n}},\beta_{k+1}=\sqrt[k+1]{M_k+\gamma(k+1)\cdot\frac{1}{n}},$$

则

$$\begin{aligned}\beta_{k+1}-\alpha_{k+1}&>(M+1)-\sqrt[k+1]{(M+1)^{k+1}-\frac{1}{n}}\\&=\frac{1}{n}\frac{1}{(M+1)^k\cdots\left[(M+1)^{k+1}-\frac{1}{n}\right]^{\frac{k}{k+1}}}.\end{aligned}$$

而

$$2\left(\sqrt[k+2]{M^{k+2}+1}-M\right)=2\cdot\frac{1}{M^{k+1}\cdots(M^{k+2}+1)^{\frac{k+1}{k+2}}}.$$

M 充分大时下式 $<$ 上式, 故

$$\beta_{k+1}-\alpha_{k+1}>2\left(\sqrt[k+2]{M^{k+2}+1}-M\right),\alpha_k\le\alpha_{k+1}<\beta_{k+1}\le\beta_k$$

成立.

依次类推可得到 $\alpha_1\sim\alpha_n,\beta_1\sim\beta_n$, 则我们考虑在 (α_t,β_t) 中取一个数

$x, \{x^t\} \in \left((\gamma(t)-1)\cdot\frac{1}{n}, \gamma(t)\cdot\frac{1}{n}\right)$.

故我们在 (α_n, β_n) 中取 x_0. (同样地, $x_0 \in (\alpha_i, \beta_i), i = 1, 2, \cdots, n-1$).

$$\Rightarrow \{x_0^i\} \in \left((\gamma(t)-1)\cdot\frac{1}{n}, \gamma(t)\cdot\frac{1}{n}\right) \text{成立}, \forall \in [1, n].$$

所以 $\{x^{\sigma(1)}\} < \{x^{\sigma(2)}\} < \cdots < \{x^{\sigma(n)}\}$ 成立.

故原命题随之成立. □

6. p 为奇素数, 求所有 $\frac{p-1}{2}$ 元组 $(x_1, \cdots, x_{\frac{p-1}{2}}) \in \mathbb{Z}_p^{\frac{p-1}{2}}$, 使

$$\sum_{i=1}^{\frac{p-1}{2}} x_i \equiv \sum_{i=1}^{\frac{p-1}{2}} x_i^2 \equiv \cdots \equiv \sum_{i=1}^{\frac{p-1}{2}} x_i^{\frac{p-1}{2}} \pmod{p}.$$

解法 1 $p > 3$ 时, 所求为全体 $(x_1, \cdots, x_{\frac{p-1}{2}}) \in \{0, 1\}^{\frac{p-1}{2}} \pmod{p}$; $p = 3$ 时所求为 0,1 或 2.

一方面, 显然所给的 $x_1, \cdots, x_{\frac{p-1}{2}}$ 符合.

另一方面, 下设 $r = \frac{p-1}{2}$; $x_1, \cdots, x_n$ 满足:

$$\begin{cases} x_1 + x_2 + \cdots + x_r \equiv a \pmod{p} \\ x_1^2 + x_2^2 + \cdots + x_r^2 \equiv a \pmod{p} \\ \qquad\vdots \\ x_1^r + x_2^r + \cdots + x_r^r \equiv a \pmod{p}, \end{cases} \tag{1}$$

下证 $(x_1, \cdots, x_r)$ 一定具有上述形式. 我们仅需考虑 $p > 3$ 的情况. 事实上, 任取 $t \in \{2, 3, \cdots, p-1\}$, 令 $\lambda \in \{1, \cdots, p-1\}$, 使得 $1 + \lambda \equiv t^2 \pmod{p}$, 则

$$\begin{aligned} \sum_{i=1}^{r}(\lambda x_i + 1)^r =& \sum_{i=1}^{r}\sum_{k=0}^{r}\binom{r}{k}x_i^k\lambda^k \\ =& r + \sum_{k=1}^{r}\sum_{i=1}^{r}\binom{r}{k}x_i^k\lambda^k \\ =& r + \sum_{k=1}^{r} a\binom{r}{k}\lambda^k \\ =& r + a\left((\lambda+1)^r - 1\right) \pmod{p} \end{aligned} \tag{2}$$

而

$$1 = \left(\frac{1+\lambda}{p}\right) \equiv (1+\lambda)^r \pmod{p} \Rightarrow p|(\lambda+1)^r - 1$$

这里 $\left(\frac{a}{p}\right)$ 为勒让德符号. 故

$$\sum_{i=1}^{r}(\lambda x_i + 1)^r \equiv r \pmod{p}.$$

即

$$\sum_{i=1}^{r}\left(\frac{\lambda x_i+1}{p}\right)^r\equiv r\pmod p.$$

即

$$\sum_{i=1}^{r}\left(\frac{x_i\cdot\lambda+1}{p}\right)\equiv r\pmod p.$$

又

$$-p+r<-r\le\sum_{i=1}^{r}\left(\frac{x_i\lambda+1}{p}\right)\le r,$$

故必须

$$\left(\frac{x_i\lambda+1}{p}\right)=1\qquad(1\le i\le r)$$

即

$$\left(\frac{x_i(t^2-1)+1}{p}\right)=1,\forall t\in\{2,3,\cdots,p-1\}\qquad(1\le i\le r)$$

又由于

$$\sum_{t=1}^{p-1}t^k\equiv\begin{cases}0, & p-1\nmid k\\ -1, & p-1|k\end{cases}\pmod p$$

故

$$\begin{aligned}p-1+\left(\frac{1-x_i}{p}\right)=&\sum_{t=0}^{p-1}\left(\frac{x_i(t^2-1)+1}{p}\right)\\ \equiv&\sum_{t=1}^{p}(x_it^2+(1-x_i))^r\\ \equiv&\sum_{t=1}^{p}\sum_{l=0}^{r}\binom{r}{l}(x_it^2)^l(1-x_i)^{r-l}\\ =&\sum_{t=1}^{p}(1-x_i)^r+\sum_{l=1}^{r-1}\binom{r}{l}(1-x_i)^{r-l}x_i^l\sum_{t=1}^{p}t^{2l}+\sum_{t=1}^{p}x_i^rt^{p-1}\\ \equiv&-x_i^r\equiv-\left(\frac{x_i}{p}\right)\pmod p.\end{aligned}$$

即

$$-1+\left(\frac{1-x_i}{p}\right)+\left(\frac{x_i}{p}\right)\equiv0\pmod p,\quad(1\le i\le r)$$

又 $p>3$, 故必须

$$-1+\left(\frac{1-x_i}{p}\right)+\left(\frac{x_i}{p}\right)=0,\quad(1\le i\le r)$$

这表明 $\left(\frac{1-x_i}{p}\right)=0$ 与 $\left(\frac{x_i}{p}\right)=0$ 至少有一个成立, 否则上式左边为奇数, 矛盾!

从而

$$x_i \equiv 0 \text{ 或 } 1 \pmod{p}, (1 \le i \le r)$$

故得证! 从而所求数组即为开头所列的. □

评注 本题很容易想到计算 σ_k, 由此导出 $x_1, \cdots, x_{\frac{p-1}{2}}$ 为 $\sum_{k=0}^{r} \binom{a}{k} x^{r-k}(-1)^k$ 的 r 个根, 说明每个 a 在轮换意义下仅一组 $(x_1, \cdots, x_r)$. 但用这种方法对"有 r 个根"体现较弱, 不容易对 $r < a < p$ 的情况进行排除.

另一角度是不等式: $x^r \equiv 0, \pm 1 \pmod{p}$, 其对根的个数体现很强. 但可惜 (1) 中 $\sum_{i=1}^{r} x_i^r \equiv a \pmod{p}$ 夹不出等号, 并且一般情况其算出余 $\pm n$ 的概率很低, 本题中 (2) 的出现不得不说是一个奇迹. 发现 (2) 基于考察平移变换 $y_i = x_i + \lambda$ 下方程 (1) 的变化, 但主要是巧合性居多, 本题也需要广大的尝试.

解法 2 $p = 3$ 同解法一. 下面仅考虑 $p > 3$ 的情形.

此时, $(x_1, x_2, \cdots, x_{\frac{p-1}{2}}) \in \{0, 1\}^{\frac{p-1}{2}}$. 即每项非 0 即 1.

一方面, 上述的 $2^{\frac{p-1}{2}}$ 个数组显然符合条件.

另一方面, 下证仅有这些数组符合条件.

设 $M \in \{0, 1, \cdots, p-1\}$ 且

$$M \equiv \sum_{i=1}^{\frac{p-1}{2}} x_i^t \pmod{p},\ t = 1, 2, \cdots, \frac{p-1}{2}.$$

则对于 mod$p$ 的一个新余类 a,

$$\sum_{i=1}^{\frac{p-1}{2}} (1 - ax_i)^{\frac{p-1}{2}} \equiv \frac{p-1}{2} + M \cdot \left[(1-a)^{\frac{p-1}{2}} - 1\right] \pmod{p}.$$

若 $\left(\frac{1-a}{p}\right) = 1$, 则

$$\sum_{i=1}^{\frac{p-1}{2}} (1 - ax_i)^{\frac{p-1}{2}} \equiv \frac{p-1}{2} \pmod{p} \Rightarrow \left(\frac{1-ax_i}{p}\right) = 1\ (i = 1, 2, \cdots, \frac{p-1}{2}).$$

也就是说, 如果 $1 - a$ 是 mod$p$ 的平方剩余, $1 - ax_i$ 也是. $(i = 1, 2, \cdots, \frac{p-1}{2})$.

所以记 $1 - a = a'$, 则 $1 - ax_i = 1 - (1 - a')x_i = 1 - x_i + x_i a'$. 所以

$$\sum_{\left(\frac{a'}{p}\right)=1} a' = \sum_{\left(\frac{a'}{p}\right)=1} 1 - x_i + x_i a'.$$

记左边 $= A$, 则

$$A = \frac{p-1}{2} \cdot (1 - x_i) + x_i \cdot A \Rightarrow \left(\frac{p-1}{2} - A\right) \cdot (1 - x_i) = 0 \pmod{p\text{意义}}.$$

又因为 $A \equiv 0 \pmod{p}$, 故必有 $x_i = 1$.

所以每个 x_i 非 0 即 1, 则原来的断言成立. □