数学新星网 ※ 学生专栏
www.nsmath.cn/xszl

数论问题中的整合思想

解尧平
(天津市实验中学, 300074)

在平时做题的过程中, 我们经常会遇到这样的一类数论题, 题目中包含着繁多的变量或每个变量都对应着繁多的取值, 并且这些变量被一个或若干个约束条件束缚着. 这类题往往以难著称, 因为题目中大多会包含各式各样的情形, 这样分门别类地讨论起来会十分麻烦, 而要想完整地刻画出变量的结构特征更是如同大海捞针一般困难. 这时整合思想往往可以派上大用场. 它的核心思想是设法寻找一个媒介, 使其能够将若干变量的某个共性的性质整合统一起来, 这时问题往往便会转化为一个和媒介有关的结论, 而如果我们可以利用某些整体或局部的处理方式来刻画出这个结论, 问题就可以解决了. 那么这样的媒介有哪些呢? 首先我们来列举一些常用的媒介, 大家可以先思考一下这些媒介究竟可以在哪些实际的题目中起到什么作用.

媒介 1 (费马小定理) 设 p 为素数, a为整数, 则

$$a^{p-1}\equiv\begin{cases}1\pmod p, & p\nmid a\\ 0\pmod p, & p\mid a\end{cases}.$$

媒介 2 设 ε 为 n 次本原单位根, 则

$$1+\varepsilon^x+\varepsilon^{2x}+\cdots+\varepsilon^{(n-1)x}=\begin{cases}0, & n\nmid x\\ n, & n\mid x\end{cases}.$$

媒介 3 设 p 为素数, 则

$$1^n+2^n+\cdots+(p-1)^n\equiv\begin{cases}0\pmod p, & p-1\nmid n\\ -1\pmod p, & p-1\mid n\end{cases}.$$

收稿日期: **2018-03-30;** 修订日期: **2018-07-08.**

媒介 4 设 p 为素数, 则有

$$\left(\frac{a}{p}\right)=\begin{cases}-1, & a \text{ 为模 } p \text{ 的非二次剩余};\\ 0, & p \mid a;\\ 1, & a \text{ 为模 } p \text{ 的二次剩余}\end{cases} \quad \text{及} \quad \left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod p.$$

特别地, $(\frac{a}{p})+1$ 可以表示为模 p 意义下方程 $x^2\equiv a \pmod p$ 解的个数.

以上便是一些常见的媒介. 这些媒介可能看起来平淡无奇, 但在某些实际问题中适当地运用可以起到神奇的作用. 合理地选取或构造媒介往往是利用整合思想解决问题的关键, 下面我们以例题的形式来分析整合思想在解题过程中发挥的作用.

例 1 (Erdös-Ginzburg-Ziv[1]) 证明: 任意 $2n-1$ 个整数中,一定存在 n 个整数和为 n 的倍数.

分析与证明 先考虑 n 为素数的情形.

利用反证法, 假设存在整数 $x_1, x_2, \cdots, x_{2n-1}$, 使得其中任意 n 个数和不为 n 的倍数, 那么这时我们可以利用媒介 1 将该性质整合起来.

这样, 条件就可以转化为: 对于任意 $1\le i_1<i_2<\cdots<i_n\le 2n-1$, 均有

$$(x_{i_1}+x_{i_2}+\cdots+x_{i_n})^{n-1}\equiv 1 \pmod n.$$

为保持对称性, 我们对其进行整体化累和处理, 则有

$$S=\sum_{1\le i_1<\cdots<i_n\le 2n-1}(x_{i_1}+x_{i_2}+\cdots+x_{i_n})^{n-1}\equiv \mathrm{C}_{2n-1}^{n}\equiv 1 \pmod n.$$

而 S 的同余性质我们是可以处理的, 对上式进行换序配对, 即可得到:

$$\begin{aligned}
S &= \sum_{1\le i_1<\cdots<i_n\le 2n-1}\ \sum_{\substack{\alpha_1+\cdots+\alpha_n=n-1\\ \alpha_1,\cdots,\alpha_n\in\mathbb{N}}} x_{i_1}^{\alpha_1}x_{i_2}^{\alpha_2}\cdots x_{i_n}^{\alpha_n}\frac{(n-1)!}{\alpha_1!\cdots\alpha_n!}\\
&= \sum_{1\le i_1<\cdots<i_n\le 2n-1}\ \sum_{1\le j_1<\cdots<j_k\le 2n-1}\ \sum_{\substack{\alpha_1+\cdots+\alpha_k=n-1\\ \alpha_1,\cdots,\alpha_k\in\mathbb{N}^+}} x_{i_{j_1}}^{\alpha_1}x_{i_{j_2}}^{\alpha_2}\cdots x_{i_{j_k}}^{\alpha_k}\frac{(n-1)!}{\alpha_1!\cdots\alpha_k!}\\
&= \sum_{\substack{\alpha_1+\cdots+\alpha_k=n-1\\ \alpha_1,\cdots,\alpha_k\in\mathbb{N}^+\\ k\in\mathbb{N}^+}}\ \sum_{1\le i_1<\cdots<i_k\le 2n-1} x_{i_1}^{\alpha_1}x_{i_2}^{\alpha_2}\cdots x_{i_k}^{\alpha_k}\frac{(n-1)!}{\alpha_1!\cdots\alpha_k!}\mathrm{C}_{2n-1-k}^{n-k}\\
&= \sum_{\substack{\alpha_1+\cdots+\alpha_k=n-1\\ \alpha_1,\cdots,\alpha_k\in\mathbb{N}^+\\ k\in\mathbb{N}^+}}\mathrm{C}_{2n-1-k}^{n-k}\frac{(n-1)!}{\alpha_1!\cdots\alpha_k!}\sum_{1\le i_1<\cdots<i_k\le 2n-1} x_{i_1}^{\alpha_1}x_{i_2}^{\alpha_2}\cdots x_{i_k}^{\alpha_k}\\
&\equiv 0 \pmod n,
\end{aligned}$$

其中用到: 当 $k=1,2,\cdots,n-1$, 均有 $n\mid \mathrm{C}_{2n-1-k}^{n-1}$. 矛盾!

这样我们证明了 n 为素数的情形.

对于一般情形, 我们利用归纳法只需证明若 n 时结论成立, 则 pn 时结论成立, 其中 p 为素数. 对于任意 $2pn-1$ 个整数 $x_1, x_2, \cdots, x_{2pn-1}$, 由归纳假设知可以从中选取 $2p-1$ 个 n 元整数组, 使得任意两个数组不存在下标相同的数, 且每个 n 元数组中的数和为 n 的倍数. 又由前面已证的素数时的情形可得, 可以从这 $2p-1$ 个 n 元整数组中选出 p 个数组, 使得 p 个数组中所有数之和为 np 的倍数, 这样, 这 p 个数组中包含的 np 个数满足条件. □

评析 例 1 是运用整合思想的一个很具有代表性的问题, 同时也不失为一个很优美的结论.

例 2 (第 33 届伊朗国家队选拔考试[2]) *已知素数 $p \neq 13$, $p \equiv 5 \pmod 8$, 且 39 不为模 p 的二次剩余. 证明: 方程*

$$x_1^4 + x_2^4 + x_3^4 + x_4^4 \equiv 0 \pmod p$$

有一个正整数解满足 $p \nmid x_1x_2x_3x_4$.

证明 与例 1 类似的思路, 若不然, 则有

$$p \nmid x_1x_2x_3x_4 \Rightarrow p \nmid x_1^4 + x_2^4 + x_3^4 + x_4^4 \Rightarrow (x_1^4 + x_2^4 + x_3^4 + x_4^4)^{p-1} \equiv 1 \pmod p,$$

再对其进行整体化处理, 则有

$$S = \sum_{x_1,x_2,x_3,x_4 \in \{1,2,\cdots,p-1\}} (x_1^4 + x_2^4 + x_3^4 + x_4^4)^{p-1} \equiv 1 \pmod p.$$

而这里 S 的同余性质我们也是可以处理的.

注意到 S 的表达式中出现了四个变量, 这样直接展开处理会很麻烦, 于是我们选择将 x_2, x_3, x_4 作为常数, 单独对 x_1 进行整体化处理, 这样即有

$$\begin{aligned} S &= \sum_{x_2,x_3,x_4 \in \{1,2,\cdots,p-1\}} \sum_{x_1 \in \{1,2,\cdots,p-1\}} (x_1^4 + x_2^4 + x_3^4 + x_4^4)^{p-1} \\ &= \sum_{x_2,x_3,x_4 \in \{1,2,\cdots,p-1\}} \sum_{x_1=1}^{p-1} \sum_{i=0}^{p-1} x_1^{4i} (x_2^4 + x_3^4 + x_4^4)^{p-1-i} \mathrm{C}_{p-1}^i \\ &= \sum_{x_2,x_3,x_4 \in \{1,2,\cdots,p-1\}} \sum_{i=0}^{p-1} (x_2^4 + x_3^4 + x_4^4)^{p-1-i} \left(\sum_{x_1=1}^{p-1} x_1^{4i} \right) \mathrm{C}_{p-1}^i. \end{aligned}$$

此时, 对于不同的 i, 我们可以借助媒介 3 对 $\sum\limits_{x_1=1}^{p-1} x_1^{4i}$ 的性质进行整合, 即得

$$\sum_{x_1=1}^{p-1} x_1^{4i} \equiv \begin{cases} 0, & \frac{p-1}{4} \mid i \\ -1, & \frac{p-1}{4} \nmid i \end{cases}.$$

于是我们得到一个重要的结论: S 中所有形如 $x_1^{4i}x_2^{4j}x_3^{4k}x_4^{4l}$ $(\frac{p-1}{4}\nmid i)$ 的项均可通过分组来抵消. 又由 x_1,x_2,x_3,x_4 的并列关系进一步可知, 将 S 的表达式展开后只需考虑其中形如

$$x_1^{4\alpha_1}x_2^{4\alpha_2}x_3^{4\alpha_3}x_4^{4\alpha_4}\left(\frac{p-1}{4}\mid \alpha_1,\alpha_2,\alpha_3,\alpha_4;\alpha_1+\alpha_2+\alpha_3+\alpha_4=p-1\right)$$

的项, 于是

$$\begin{aligned}S\equiv&\sum_{x_1,x_2,x_3,x_4\in\{1,2,\cdots,p-1\}}(x_1^{4(p-1)}+x_2^{4(p-1)}+x_3^{4(p-1)}+x_4^{4(p-1)}\\&+\frac{(p-1)!}{((\frac{p-1}{4})!)^4}x_1^{p-1}x_2^{p-1}x_3^{p-1}x_4^{p-1}+\frac{(p-1)!}{((\frac{p-1}{2})!)^2}\sum_{1\le i<j\le 4}x_i^{2(p-1)}x_j^{2(p-1)}\\&+\frac{(p-1)!}{(\frac{p-1}{4})!(\frac{3(p-1)}{4})!}\sum_{1\le i\ne j\le 4}x_i^{(p-1)}x_j^{3(p-1)}\\&+\frac{(p-1)!}{(\frac{p-1}{2})!((\frac{p-1}{4})!)^2}\sum_{\substack{\{i,j,k\}\in\{1,2,3,4\}\\ i<j\\ i\ne j\ne k}}x_i^{(p-1)}x_j^{(p-1)}x_k^{2(p-1)})\\\equiv&(p-1)^4\left(4+\frac{(p-1)!}{((\frac{p-1}{4})!)^4}+\frac{6(p-1)!}{((\frac{p-1}{2})!)^2}+\frac{12(p-1)!}{(\frac{p-1}{4})!(\frac{3(p-1)}{4})!}+\frac{12(p-1)!}{(\frac{p-1}{2})!((\frac{(p-1)}{4})!)^2}\right),\end{aligned}$$

而由威尔逊定理不难推出

$$\begin{aligned}(p-1)!&\equiv -1\pmod p,\\\left((\frac{p-1}{2})!\right)^2&\equiv(p-1)!(-1)^{\frac{p-1}{2}}\equiv -1\ (\mathrm{mod\ p}),\\\left(\frac{3(p-1)}{4}\right)!&\equiv\frac{(p-1)!}{(\frac{p-1}{4})!(-1)^{\frac{p-1}{4}}}\equiv\frac{1}{(\frac{p-1}{4})!}\pmod p.\end{aligned}$$

于是

$$\begin{aligned}S\equiv&4+\frac{1}{[(\frac{p-1}{2})!((\frac{p-1}{4})!)^2]^2}-\frac{12}{(\frac{p-1}{2})!((\frac{p-1}{4})!)^2}+6-12\\\equiv&(\frac{1}{(\frac{p-1}{2})!((\frac{p-1}{4})!)^2}-6)^2-38\\\not\equiv&1\pmod p.\end{aligned}$$

这里用到的条件 $\left(\frac{39}{p}\right)\ne 1$, 矛盾! □

评析 我们发现例 1 和例 2 在处理手法上有很大的共性, 两者都是在寻找出一个适当的媒介后, 对媒介进行整体处理, 这种手法在以下的某些题目中也会有所体现. 而在整体处理的过程中, 我们往往也需要再次借助整合思想对目标进行进一步简化.

例 3 (2017 北大夏令营[3]) 设 p 是素数, 证明: 对任意整数 a , 同余方程 $y^2+x^3+a\equiv 0 \pmod p$ 一定有解.

证明 首先处理一些简单的情形: 当 $p=2$ 时, 显然成立.

当 $p\equiv 5 \pmod 6$ 时, 由 $\left(\frac{-3}{p}\right)=-1$ 可以推出 $1^3,2^3,\cdots,p^3$ 构成模 p 的完全剩余系, 于是结论显然成立.

这道题的难点是 $p\equiv 1 \pmod 6$ 的情形, 我们利用反证法. 假设整数 a 不满足条件, 即对任意 $x,y\in\mathbb{Z}$ 均有 $-(x^3+a)\not\equiv y^2 \pmod p$, 这时我们可以利用媒介 4 对该性质进行整合, 则条件可以转化为对任意 $x\in\mathbb{Z}$, 均有 $\left(\frac{-1}{p}\right)\left(\frac{x^3+a}{p}\right)=-1$,下面再次利用整体化处理方式 , 可得

$$S=\sum_{i=0}^{p-1}\left(\frac{x^3+a}{p}\right)\left(\frac{-1}{p}\right)=-p\equiv 0 \pmod p .$$

而另一方面 $\left(\frac{x^3+a}{p}\right)$ 的同余性质又可以利用媒介 4:

$$\left(\frac{x^3+a}{p}\right)\equiv\left(x^3+a\right)^{\frac{p-1}{2}} \pmod p.$$

进行整合, 这样

$$\begin{aligned}
S\equiv&\sum_{x=0}^{p-1}(x^3+a)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}\\
\equiv&(-1)^{\frac{p-1}{2}}\sum_{x=0}^{p-1}\sum_{i=0}^{\frac{p-1}{2}}x^{3i}a^{\frac{p-1}{2}-i}\mathrm{C}_{\frac{p-1}{2}}^{i}\\
\equiv&(-1)^{\frac{p-1}{2}}\sum_{i=0}^{\frac{p-1}{2}}a^{\frac{p-1}{2}-i}\mathrm{C}_{\frac{p-1}{2}}^{i}\left(\sum_{x=0}^{p-1}x^{3i}\right)\\
\equiv&(-1)^{\frac{p-1}{2}}(pa^{\frac{p-1}{2}}-\mathrm{C}_{\frac{p-1}{2}}^{\frac{p-1}{3}}a^{\frac{p-1}{6}})\\
\equiv&(-1)^{\frac{p-1}{2}}\mathrm{C}_{\frac{p-1}{2}}^{\frac{p-1}{3}}a^{\frac{p-1}{6}} \pmod p . \qquad (1)
\end{aligned}$$

其中倒数第二式又一次用到媒介 3. 于是 $a\equiv 0 \pmod p$.

而当 $a\equiv 0 \pmod p$ 时, 取 $x=y=0$ 即满足条件 , 矛盾! □

评析 回顾例 3 的解答过程: 我们首先选取勒让德符号作为媒介 , 然后将勒让德符号累和 , 并将其转化为多项式累和的形式, 这样我们便将一道复杂的存在性问题转化为一道相对简单的多项式同余问题. 这一连串的处理方式完美地凸显了整合思想处理这一类问题的强大之处. 笔者认为这种处理方式是值得我们去学习和掌握的. 在下面这道题中, 这种处理方式的神奇将体现得更加淋漓尽致.

例 4 (2018 韩国数学冬令营训练题[4]) 设 $p=4k+1$ 为质数, 集合 $S=\left\{x|x\equiv \frac{1}{2}\mathrm{C}_{2k}^{k}n^{k}\pmod p, n\in\mathbb{Z}, x\in\{0,1,\cdots,2k\}\right\}$, 证明: $\sum\limits_{x\in S}x^2=p$.

证明 这道题的困难之处在于 $\mathrm{C}_{2k}^{k}n^{k}=\mathrm{C}_{\frac{p-1}{2}}^{\frac{p-1}{4}}n^{\frac{p-1}{4}}$ 模 p 的余数如何处理. 我们发现 $\mathrm{C}_{\frac{p-1}{2}}^{\frac{p-1}{4}}$ 的同余性质是很难刻画的, 又注意到 $\mathrm{C}_{\frac{p-1}{2}}^{\frac{p-1}{4}}n^{\frac{p-1}{4}}$ 的形式与上题中 (1) 的右端形式十分类似, 这提示我们可以设法将 $\mathrm{C}_{2k}^{k}n^{k}$ 的同余性质整合为 p 个勒让德符号之和的形式.

经过简单的分析, 我们选定和式 $f(n)=-\sum\limits_{i=0}^{p-1}(\frac{i^3+ni}{p})$. 类似上题的处理方式, 可以得到

$$\begin{aligned}
f(n)\equiv&-\sum_{i=0}^{p-1}\left(i^3+ni\right)^{\frac{p-1}{2}}\\
\equiv&\sum_{i=0}^{p-1}\sum_{j=0}^{\frac{p-1}{2}}i^{3j}(ni)^{\frac{p-1}{2}-j}\mathrm{C}_{\frac{p-1}{2}}^{j}\\
\equiv&\sum_{i=0}^{p-1}\sum_{j=0}^{\frac{p-1}{2}}i^{2j+\frac{p-1}{2}}n^{\frac{p-1}{2}-j}\mathrm{C}_{\frac{p-1}{2}}^{j}\\
\equiv&\sum_{j=0}^{\frac{p-1}{2}}n^{\frac{p-1}{2}-j}\mathrm{C}_{\frac{p-1}{2}}^{j}\left(\sum_{i=0}^{p-1}i^{2j+\frac{p-1}{2}}\right)\\
\equiv&n^{\frac{p-1}{4}}\mathrm{C}_{\frac{p-1}{2}}^{\frac{p-1}{4}}.
\end{aligned}$$

这样, 我们达到了之前的目标, 于是接下来只需转换视角去研究 $f(n)$ 的同余性质. 我们从 $f(n)$ 的分布规律入手.

由 $f(n)\equiv n^{\frac{n-1}{4}}\mathrm{C}_{\frac{p-1}{2}}^{\frac{p-1}{4}}\pmod p$ 及 $f(n)\in[1-p,p-1]$ 可以推出除了 0 以外, $f(n)$ 仅可以取到形如 $x,-x,y,-y$ 的 4 个值, 并且其中每个值都恰好取 $\frac{p-1}{4}$ 次, 于是结论等价于证明

$$\sum_{n=0}^{p-1}f^2(n)=2p(p-1),$$

即

$$\sum_{n=0}^{p-1}\left(\sum_{i=0}^{p-1}\left(\frac{i^3+ni}{p}\right)\right)^2=2p(p-1). \tag{2}$$

我们将 (2) 式左端展开并利用勒让德符号的积性进行处理可得

$$\begin{aligned}
LHS(2)=&\sum_{n=0}^{p-1}\sum_{0\le i,j\le p-1}\left(\frac{ij}{p}\right)\left(\frac{i^2+n}{p}\right)\left(\frac{j^2+n}{p}\right)\\
=&\sum_{0\le i,j\le p-1}\left(\frac{ij}{p}\right)\sum_{n=0}^{p-1}\left(\frac{i^2j^2+n(i^2+j^2)+n^2}{p}\right).
\end{aligned}$$

于是下面我们只需求 $f(i,j)=\sum\limits_{n=0}^{p-1}\left(\frac{i^2j^2+n(i^2+j^2)+n^2}{p}\right)$ 的值.

还是利用类似处理方式处理, 可以得到

$$\begin{aligned}f(i,j)=&\sum_{n=0}^{p-1}(i^2j^2+n(i^2+j^2)+n^2)^{\frac{p-1}{2}}\\ \equiv&\sum_{n=0}^{p-1}\left(\left(i^2j^2\right)^{\frac{p-1}{2}}+n^{p-1}\right)\\ \equiv&-1\ (\mathrm{mod\ p}),\end{aligned}$$

而 $f(i,j)\in[-p,p]$, 故 $f(i,j)\in\{-1,p-1\}$. 再经过简单分析, 我们进一步推出

$$f(i,j)=\begin{cases}-1, & i^2\not\equiv j^2 \pmod p\\ p-1, & i^2\equiv j^2 \pmod p\end{cases}.$$

这样

$$\begin{aligned}LHS(2)=&p(2p-2)-\sum_{0\le i,j\le p-1}\left(\frac{ij}{p}\right)\\ =&p(2p-2)-\left(\sum_{i=0}^{p-1}\left(\frac{i}{p}\right)\right)^2\\ =&2p(p-1).\end{aligned}$$

□

评析 从这道题的过程中, 我们再次见识到勒让德符号累和这个方法的威力. 事实上, 本题的“整合思想”体现得并不十分典型 , 如果没有上一题作为铺垫, 我们很难想到可以将题目中 $\mathrm{C}_{2k}^{k}n^k$ 的同余性质整合为看似繁杂得多的 p 个勒让德符号累和的式子. 但是笔者仍将这道题选为例题, 一方面是因为这道题的解题过程简洁优美, 结论也十分深刻, 直接刻画方程 $x^2+y^2=p$ 中 x,y 的同余性质, 令我们拍手称绝. 另一方面, 笔者也希望让大家意识到, 将勒让德符号作为媒介处理起来是十分方便的, 这是因为勒让德符号集积性, 简洁的取值方式, 优美的同余性质于一身, 这样和其它媒介相比处理起来会更加灵活变通.下面, 我们再来看一个将勒让德符号作为媒介解决二次型同余方程问题的例子.

例 5 (2017 中国国家集训队[5]) 试求同时满足下列条件的有序数组 $(x_1,x_2,\cdots,x_{100})$ 的个数:

(1) $x_1,x_2,\cdots,x_{100}\in\{1,2,\cdots,2017\}$;

(2) $2017\mid x_1+x_2+\cdots+x_{100}$;

(3) $2017\mid x_1^2+x_2^2+\cdots+x_{100}^2$.

解 问题等价于求模 2017 的意义下, 同余方程组

$$\begin{cases} 2017 \mid x_1 + x_2 + \cdots + x_{100} \\ 2017 \mid x_1^2 + x_2^2 + \cdots + x_{100}^2 \end{cases}$$

的解数.

为简化条件, 首先将两个方程合并为一个方程, 我们可以令$a_i = x_1 + x_2 + \cdots + x_i$, 则题目条件等价于

$$2017 \mid (a_1 - a_2)^2 + \cdots + (a_{98} - a_{99})^2 + a_{99}^2 + a_1^2.$$

但此时该式右端的 100 个项数之间存在着约束关系, 仍难以处理, 于是我们需要对右式进行进一步变形

$$\begin{aligned} &(a_1 - a_2)^2 + \cdots + (a_{98} - a_{99})^2 + a_{99}^2 + a_1^2 \\ =&2\left(a_{99} - \frac{a_{98}}{2}\right)^2 + \frac{3}{2}\left(a_{98} - \frac{2a_{97}}{3}\right)^2 + \frac{4}{3}\left(a_{97} - \frac{3a_{96}}{4}\right)^2 \\ &+ \cdots + \frac{99}{98}\left(a_2 - \frac{98a_1}{99}\right)^2 + \frac{100}{99}a_1^2, \end{aligned}$$

并令

$$c_1 = 2, c_2 = \frac{3}{2}, \cdots, c_{98} = \frac{99}{98}, c_{99} = \frac{100}{99},$$

$$b_1 = a_{99} - \frac{a_{98}}{2}, \cdots, b_{98} = a_2 - \frac{98a_1}{99}, b_{99} = a_1,$$

则题目条件亦等价于

$$2017 \mid c_1 b_1^2 + c_2 b_2^2 + \cdots + c_{99} b_{99}^2. \tag{3}$$

此时 $c_1, c_2, \cdots, c_{99}$ 为常数, $b_1, b_2, \cdots, b_{99}$ 为自由变量, 我们达到了先前目标. 而我们所熟悉的问题是借助媒介 4 来整合方程 $x^2 \equiv a \pmod{p}$ 的解数, 于是我们选择再进一步将同余方程转化为下述形式

$$\begin{cases} 2017 \mid t_1 + t_2 + \cdots + t_{99} \\ 2017 \mid t_1 - c_1 b_1^2 \\ 2017 \mid t_2 - c_2 b_2^2 \\ \cdots \\ 2017 \mid t_{99} - c_{99} b_{99}^2 \end{cases}.$$

这样, 对于每组 $(t_1, t_2, \cdots, t_{99})$ 进行单独分析, 我们就可以利用媒介 4 将方程的解数整合为

$$\left(\left(\frac{t_1}{p}\right)\left(\frac{c_1}{p}\right) + 1\right)\left(\left(\frac{t_2}{p}\right)\left(\frac{c_2}{p}\right) + 1\right) \cdots \left(\left(\frac{t_{99}}{p}\right)\left(\frac{c_{99}}{p}\right) + 1\right),$$

这里记 $p=2017$. 于是 (3) 的解数可以表示为

$$S=\sum_{t_1+t_2+\cdots+t_{99}=0}\left(\left(\frac{t_1}{p}\right)\left(\frac{c_1}{p}\right)+1\right)\left(\left(\frac{t_2}{p}\right)\left(\frac{c_2}{p}\right)+1\right)\cdots\left(\left(\frac{t_{99}}{p}\right)\left(\frac{c_{99}}{p}\right)+1\right).$$

将 S 的表达式展开可得

$$\begin{aligned}S=&\sum_{t_1+t_2+\cdots+t_{99}=0}1+\sum_{t_1+t_2+\cdots+t_{99}=0}\left(\frac{c_1}{p}\right)\left(\frac{c_2}{p}\right)\cdots\left(\frac{c_{99}}{p}\right)\left(\frac{t_1}{p}\right)\left(\frac{t_2}{p}\right)\cdots\left(\frac{t_{99}}{p}\right)\\&+\sum_{t_1+t_2+\cdots+t_{99}=0}\sum_{\substack{1\le i_1<\cdots<i_k\le 99\\1\le k\le 98}}\left(\frac{c_{i_1}}{p}\right)\left(\frac{c_{i_2}}{p}\right)\cdots\left(\frac{c_{i_k}}{p}\right)\left(\frac{t_{i_1}}{p}\right)\left(\frac{t_{i_2}}{p}\right)\cdots\left(\frac{t_{i_k}}{p}\right).\end{aligned}$$

下面我们对上式右端的三个部分分别进行处理.

首先,

$$\sum_{t_1+t_2+\cdots+t_{99}=0}1=\sum_{0\le t_1,t_2,\cdots,t_{98}\le p-1}1=2017^{98},$$

其次, 第二个部分可以利用 99 为奇数这个特性进行正负配对, 得到

$$\begin{aligned}&\sum_{t_1+t_2+\cdots+t_{99}=0}\left(\frac{c_1}{p}\right)\left(\frac{c_2}{p}\right)\cdots\left(\frac{c_{99}}{p}\right)\left(\frac{t_1}{p}\right)\left(\frac{t_2}{p}\right)\cdots\left(\frac{t_{99}}{p}\right)\\&=\frac{1}{2}\sum_{t_1+t_2+\cdots+t_{99}=0}\left(\frac{c_1}{p}\right)\left(\frac{c_2}{p}\right)\cdots\left(\frac{c_{99}}{p}\right)\cdot\\&\qquad\left(\left(\frac{t_1}{p}\right)\left(\frac{t_2}{p}\right)\cdots\left(\frac{t_{99}}{p}\right)+\left(\frac{\lambda t_1}{p}\right)\left(\frac{\lambda t_2}{p}\right)\cdots\left(\frac{\lambda t_{99}}{p}\right)\right)\\&=\frac{1}{2}\left(\frac{c_1}{p}\right)\left(\frac{c_2}{p}\right)\cdots\left(\frac{c_{99}}{p}\right)\sum_{t_1+t_2+\cdots+t_{99}=0}\left(\frac{t_1}{p}\right)\left(\frac{t_2}{p}\right)\cdots\left(\frac{t_{99}}{p}\right)\left(1+\left(\frac{\lambda}{p}\right)^{99}\right)\\&=0,\end{aligned}$$

这里 λ 为模 2017 的任意非二次剩余.

而在第三个部分中, 注意到其中 $t_{i_1},t_{i_2},\cdots,t_{i_k}$ 均是自由变量, 并且每个单项 $\left(\frac{t_{i_1}}{p}\right)\left(\frac{t_{i_2}}{p}\right)\cdots\left(\frac{t_{i_k}}{p}\right)$ 均出现了 p^{98-t} 次, 于是

$$\begin{aligned}&\sum_{\substack{1\le i_1<\cdots<i_k\le 99\\1\le k\le 98}}\left(\frac{c_{i_1}}{p}\right)\left(\frac{c_{i_2}}{p}\right)\cdots\left(\frac{c_{i_k}}{p}\right)\left(\frac{t_{i_1}}{p}\right)\left(\frac{t_{i_2}}{p}\right)\cdots\left(\frac{t_{i_k}}{p}\right)\\&=\sum_{k=1}^{98}\sum_{1\le i_1<\cdots<i_k\le 99}\left(\frac{c_{i_1}}{p}\right)\left(\frac{c_{i_2}}{p}\right)\cdots\left(\frac{c_{i_k}}{p}\right)\cdot\\&\qquad\left(\sum_{0\le t_{i_1},t_{i_2},\cdots,t_{i_k}\le p-1}p^{98-t}\left(\frac{t_{i_1}}{p}\right)\left(\frac{t_{i_2}}{p}\right)\cdots\left(\frac{t_{i_k}}{p}\right)\right)\\&=\sum_{k=1}^{98}\sum_{1\le i_1<\cdots<i_k\le 99}\left(\frac{c_{i_1}}{p}\right)\left(\frac{c_{i_2}}{p}\right)\cdots\left(\frac{c_{i_k}}{p}\right)p^{98-t}\left(\sum_{i=0}^{p-1}\left(\frac{i}{p}\right)\right)^k\end{aligned}$$

$= 0,$

这样便推出: $S = 2017^{98}$. 于是原方程有 2017^{98} 组解. □

评析 例 3、例 6 都是与二次型同余方程的解相关的问题. 在解决这类问题的过程中, 将勒让德符号作为媒介来整合方程的某些性质往往也是十分有效的.

下面我们来看一个相对简单的题目.

例 6 (2011∼2012, 第 20 届伊朗数学奥林匹克[6]) 设 p 是一个奇素数, 若整系数多项式 $f(x) = \sum_{j=0}^{n} a_j x^j$ 满足

$$\sum_{p-1|j,\ j>0} a_j \equiv i \pmod{p},$$

则称 $f(x)$ 为 $i-$剩余的. 证明: $\{f(0), f(1), \cdots, f(p-1)\}$ 为模 p 的完全剩余系, 当且仅当多项式 $f(x), f^2(x), \cdots, f^{p-2}(x)$ 为 $0-$剩余, $f^{p-1}(x)$ 为 $1-$剩余.

证明 首先我们需要对 $\sum_{p-1|j,j>0} a_j$ 的同余性质进行整合. 而 $p-1 \mid j$ 这一约束条件对我们的提示已经很明显了, 因此不难想到利用媒介 3 , 即可得到

$$\sum_{p-1|j,j>0} a_j = -\sum_{j=0}^{p-1} a_j \left(0^j + 1^j + \cdots + (p-1)^j\right) \equiv -\sum_{i=0}^{p-1} f(i) \pmod{p}.$$

这样一方面, 若 $\{f(0), f(1), \cdots, f(p-1)\}$ 为模 p 完全剩余系, 则再次利用媒介 3, 可得

$$\sum_{i=0}^{p-1} f^{\alpha}(i) \equiv \begin{cases} 0 \text{ (mod p)}, & \alpha = 1, 2, \cdots, p-2 \\ -1 \text{ (mod p)}, & \alpha = p-1 \end{cases} \tag{4}$$

即 $f(x), f^2(x), \cdots, f^{p-2}(x)$ 为 $0-$剩余, $f^{p-1}(x)$ 为 $1-$剩余.

另一方面, 若 $f(x), f^2(x), \cdots, f^{p-2}(x)$ 为 $0-$剩余, $f^{p-1}(x)$ 为 $1-$剩余. 则由

$$\sum_{p-1|j,j>0} a_j \equiv -\sum_{i=0}^{p-1} f(i) \pmod{p}$$

可以反推出(4) 成立.

接下来考虑多项式

$$\begin{aligned} g(x) =& (x - f(0))(x - f(1)) \cdots (x - f(p-1)) \\ =& x^p + a_{p-1}x^{p-1} + \cdots + a_0 \,, \end{aligned}$$

则由牛顿恒等式, 易知

$$a_{p-1}, a_{p-2}, \cdots, a_2 \equiv 0 \pmod{p},$$

$$a_1 = -1 \pmod{p},\ a_0 = 0 \pmod{p},$$

于是

$$\begin{aligned} g(x) =& (x-f(0))\,(x-f(1))\cdots(x-f(p-1)) \\ \equiv& x\,(x-1)\cdots(x-(p-1)) \pmod p, \end{aligned}$$

即$\{f(0), f(1), \cdots, f(p-1)\}$为模 p 的完全剩余系. □

例 7[7] 设 p 为奇素数, $x_1, x_2, \cdots, x_k$ 模 p 互不同余, $y_1, y_2, \cdots, y_k$ 模 p 互不同余, 则存在一一对应的映射 $f: \{x_1, x_2, \cdots, x_k\} \to \{y_1, y_2, \cdots, y_k\}$, 使得 $x_i + f(x_i)$ $(1 \le i \le k)$ 模 p 互不同余.

证明 首先利用反证法, 若不然, 则存在整数 $x_1, x_2, \cdots, x_k,\ y_1, y_2, \cdots, y_k$, 使得对任意 k 个数 $z_1, z_2, \cdots, z_k$, 若 $\{z_1, z_2, \cdots, z_k\} = \{y_1, y_2, \cdots, y_k\}$, 则 $z_1 + x_1, z_2 + x_2, \cdots, z_k + x_k$ 这 k 个数中一定有两个模 p 同余, 这时我们可以该性质整合为下面这个同余式

$$\prod_{1\le i<j\le k} (x_i + z_i - x_j - z_j) \equiv 0 \pmod p. \tag{5}$$

但 $\{z_1, z_2, \cdots, z_k\} = \{y_1, y_2, \cdots, y_k\}$ 这种 k 元数组的取值方式是很难进行刻画的, 于是我们需要进一步将 (5) 式一般化为: 对于 $z_1, z_2, \cdots, z_k \in \{y_1, y_2, \cdots, y_k\}$, 均有

$$\prod_{1\le i<j\le k} (z_i - z_j) \prod_{1\le i<j\le k} (x_i + z_i - x_j - z_j) \equiv 0 \pmod p. \tag{6}$$

将 (6) 的左边记为 $f(z_1, z_2, \cdots, z_k)$. 观察 $z_1, z_2, \cdots, z_k$ 的取值方式及目标结论, 我们发现这恰恰是组合零点定理的形式.

于是我们取出 f 中的最高次项组成多项式 $\prod\limits_{1\le i<j\le k} (z_i - z_j)^2$, 然后考虑其中最具对称性的项 $z_1^{k-1} z_2^{k-1} \cdots z_k^{k-1}$ 的系数, 不难求得其系数为 $(-1)^{\mathrm{C}_k^2} k!$ 不是 p 的倍数. 而 $z_1, z_2, \cdots, z_k$ 均有 k 种取值方式, 于是由组合零点定理知, 存在一组 $z_1, z_2, \cdots, z_k$, 使得 $f(z_1, z_2, \cdots, z_k) \not\equiv 0 \pmod p$, 矛盾! □

下面补上组合零点定理的内容.

组合零点定理[7] 设 $\mathcal{F}$ 为一个域, $f \in \mathcal{F}[x_1, x_2, \cdots, x_n]$ 为域 $\mathcal{F}$ 上的一个 n 元多项式, 假设 f 有一个最高项 $x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$ 系数非零, 则对任意 $S_1, S_2, \cdots, S_n \subseteq \mathcal{F}$, $|S_i| > d_i$ $(1 \le i \le n)$, 存在 $s_i \in S_i$, 使得

$$f(s_1, s_2, \cdots, s_n) \neq 0.$$

常见的域有复数域 $\mathbb{C}$, 实数域 $\mathbb{R}$, 有理数域 $\mathbb{Q}$, 模素数 p 的素数域 $\mathbb{F}_p$.

评析 从这道题的解题过程中, 我们需要意识到在了解并掌握一些常用的媒介的基础上, 更多的题目需要我们去构造适当的媒介来对目标的某种性质进行整合. 在构造媒介的过程中, 如果条件允许, 我们最好让媒介满足下面两个要求: 1) 媒介与题目条件等价; 2) 媒介便于处理.

例 8[1] 设集合 $F_i=\{a_i+d_ix\mid x\in\mathbb{Z}\}\,(i=1,2,\cdots,k)$, 其中 $a_1,a_2,\cdots,a_k$, $d_1,d_2,\cdots,d_k$ 均为正整数, $1\leqslant d_1<\cdots<d_k$, 并设集合 $F=\bigcup\limits_{i=1}^{k}F_i$, 若 F 包含连续 2^k 个整数. 证明: $F=\mathbb{Z}$.

证明 不妨设 $x,x+1,\cdots,x+2^k-1$ 属于 F, 则结论等价于证明对于任意整数 t, $\frac{x+t-a_j}{d_j}\,(j=1,2,\cdots,k)$ 中至少有一个整数, 下面我们设法构造一个适当的媒介来整合 k 个数中至少有一个整数这个性质.

首先考虑只有一个数的情况, 我们显然可以利用媒介

$$e^{2\pi ix}\begin{cases}=1, & x\in\mathbb{Z}\\ \neq 1, & x\notin\mathbb{Z}\end{cases}$$

来整合全体整数的性质; 那么对于 k 个数的情况, 我们不难想到可以利用媒介

$$\prod_{1\leqslant j\leqslant k}\left(1-e^{\frac{2\pi i}{d_j}(x+t+a_j)}\right)=0 \tag{7}$$

来整合结论的性质.

于是接下来, 我们只需证明 (7) 即可. 将 (7) 式左端展开, 可得

$$LHS(7)=\sum_{I\subseteq\{1,2,\cdots,k\}}(-1)^{|I|}e^{-2\pi i\sum\limits_{j\in I}\frac{a_j}{d_j}-2\pi i\sum\limits_{j\in I}\frac{x+t}{d_j}}.$$

记

$$\alpha_I=\sum_{I\subseteq\{1,2,\cdots,k\}}(-1)^{|I|}e^{-2\pi i\sum\limits_{j\in I}\frac{a_j}{d_j}},\ Z_I=e^{-2\pi i\sum\limits_{j\in I}\frac{1}{d_j}},$$

则 α_I,Z_I 均为不依赖于 x 的常数. 于是 (7) 等价于

$$\sum_{I\subseteq\{1,2,\cdots,k\}}a_IZ_I^{x+t}=0.$$

而结合题目条件, 这是不难证明的.

设 $u_n=\sum\limits_{I\subseteq\{1,2,\cdots,k\}}a_IZ_I^n$, 则数列 $\{u_n\}$ 存在 2^k 阶线性递推关系

$$u_{n+2^k}+A_{2^k-1}u_{n+2^k-1}+\cdots+A_0u_n=0.$$

其中 $A_{2^k-1},\cdots,A_0$ 由下述方程确定

$$\prod_{I\subseteq\{1,2,\cdots,k\}}(x-a_IZ_I^n)=x^{2^k}+A_{2^k-1}x^{2^k-1}+\cdots+A_0,$$

又由条件可知 $\{u_n\}$ 中有连续 2^k 项均为 0 , 于是推出 $u_n \equiv 0$. □

例 9[1] 设 p 为素数, $f_k(x_1, x_2, \cdots, x_n) = a_{k_1}x_1 + \cdots + a_{k_n}x_n$ $(k = 1, 2, \cdots, p^n)$ 为 p^n 个整系数 n 元线性函数, 并且满足下列条件: 对于任意 n 元整数组 $(x_1, x_2, \cdots, x_n)$, 若 $x_1, x_2, \cdots, x_n$ 不全为 p 的余数, 则 $0, 1, \cdots, p-1$ 这 p 个数均在其中恰好出现了 p^{n-1} 次. 证明: 在模 p 的意义下, 有

$$\{(a_{k_1}, a_{k_2}, \cdots, a_{k_n}) \mid k = 1, 2, \cdots, p^n\} = \{(i_1, \cdots, i_n) \mid i_1, \cdots, i_n \in \{0, 1, \cdots, p-1\}\}.$$

证明 首先对条件进行处理. 简单分析一下这种特殊的取值方式, 不难想到可以利用媒介 2 将条件描述的性质整合为: 对于任意不均为 p 的倍数的 n 个数 $x_1, x_2, \cdots, x_n$, 一定有

$$\sum_{k=1}^{p^n} \varepsilon^{f_k(x_1, x_2, \cdots, x_n)} = 0. \tag{8}$$

事实上, 这个等式与原条件是等价的, 不过在这道题中我们不需要利用这一点.

接下来再对结论进行转化. 利用反证法, 我们可以将问题转化为只需对特定的一个 n 元数组进行具体分析: 若不然, 则存在一个 n 元数组 $(i_1, i_2, \cdots, i_n)$, 使得对任意 $k = 1, 2, \cdots, p^n$, 均有 $(i_1, i_2, \cdots, i_n) \neq (a_{k_1}, a_{k_2}, \cdots, a_{k_n})$ (这里的运算都是在模 p 的意义下进行的). 这时, 我们又可以借助媒介 2 的思想来整合这个条件, 即对任意 $k = 1, 2, \cdots, p^n$, 均有

$$\prod_{t=1}^{n} \left(\sum_{j=0}^{p-1} \varepsilon^{j(a_{k_t} - i_t)} \right) = 0. \tag{9}$$

下面我们将借助 (8), (9) 来推出矛盾. 首先将 (8) 向 (9) 的形式靠近,

$$\sum_{k=1}^{p^n} \varepsilon^{(a_{k_i} - i_1)x_1 + \cdots + (a_{k_n} - i_n)} = \begin{cases} 0, & x_1, x_2, \cdots, x_n \text{不全为 } p \text{ 的倍数}, \\ p^n, & x_1, x_2, \cdots, x_n \text{全为 } p \text{ 的倍数}. \end{cases}$$

再对上式进行整体处理: 让 $x_1, x_2, \cdots, x_n$ 取遍 $0, 1, \cdots, p-1$ 并对上式左端进行累和. 经一番计算可得

$$\sum_{k=1}^{p^n} \prod_{t=1}^{n} \left(\sum_{j=0}^{p-1} \varepsilon^{j(a_{k_t} - i_t)} \right) = p^n,$$

这显然与 (9) 式矛盾 **!** □

练习题

1 (2017 清华金秋营[3]**)** 给定奇素数 p , 求集合

$$\left\{(x, y) \mid x^2 + y^2 \equiv a \pmod{p},\ (x, y) \in \{0, 1, \cdots, p-1\}\right\}$$

的元素个数.

提示 根据媒介 4, 元素个数可以整合为 $\sum\limits_{i=1}^{p-1}\left(1+\left(\frac{a-i^2}{p}\right)\right)$, 再利用例 3 的处理方式即可.

2 (2007 年第 48 届 IMO 预选题[8]) 求所有 $n\in\mathbb{N}^+$, 使得集合 $S=\{1,2,\cdots,n\}$ 的元素可染成红蓝两色, 满足下述条件: 集合 $S\times S\times S$ 恰含 2007 个有序三元组 (x,y,z), 每组 x,y,z 同色, 且 $n\mid x+y+z$.

提示 利用媒介 2, 记红数组成的集合为 $\{x_1,x_2,\cdots,x_m\}$, 蓝数集合为 $\{y_1,y_2,\cdots,y_{n-m}\}$, 则满足 x,y,z 同色, 且 $n\mid x+y+z$的三元组 (x,y,z) 组数为

$$\sum_{i=0}^{n-1}(\varepsilon^{ix_1}+\cdots+\varepsilon^{ix_m})^3+(\varepsilon^{iy_1}+\cdots+\varepsilon^{iy_{n-m}})^3,$$

其中 ε 为 n 次本原单位根, 再对上式进行化简即可.

3 (1995 年第 36 届 IMO[8]) 设 p 为奇素数, 求集合 $\{1,2,\cdots,2p\}$ 中元素之和被 p 整除的 p 元子集的个数.

提示 利用媒介 2 ,可将 p 元子集数 S 整合为

$$\sum_{i=0}^{p-1}\left(\sum_{1\leq c_1<\cdots<c_p\leq 2p}\varepsilon^{i(c_1+c_2+\cdots+c_p)}\right),$$

其中 ε 为 p 次本原根, 再结合恒等式

$$(x+\varepsilon)(x+\varepsilon^2)\cdots(x+\varepsilon^{2p})=(x^p+1)^2,$$

不难求得

$$S=\frac{\mathrm{C}_{2p}^{p}+2p-2}{p}.$$

4[1] 设 p 为奇素数, m,n 为 p 的倍数, 且 n 为奇数, $m,n>1$, 对于所有满足 $\sum\limits_{k=1}^{m}f(k)\equiv 0\pmod p$ 的函数 $f:\{1,2,\cdots,m\}\to\{1,2,\cdots,n\}$, 考虑乘积 $\prod\limits_{k=1}^{m}f(k)$, 证明: 所有这样的乘积求和得到的数是 $(\frac{n}{p})^m$ 的倍数.

提示 考虑

$$S=\sum_{f}\prod_{k=1}^{m}f(k)\varepsilon^{f(k)}=\left(\sum_{i=1}^{n}i\varepsilon^i\right)^m=\frac{n^m}{(\varepsilon-1)^m},$$

由恒等式

$$\frac{1}{\varepsilon-1}=-\frac{1}{p}\left(\varepsilon^{p-2}+2\varepsilon^{p-3}+\cdots+(p-1)\right),$$

得

$$S=\left(-\frac{n}{p}\right)^m\left(\varepsilon^{p-2}+2\varepsilon^{p-3}+\cdots+(p-1)\right)^m.$$

设多项式 $P(x)=\left(x^{p-2}+2x^{p-3}+\cdots+(p-1)\right)^m$ 所有次数模 p 余 i 的项的系数之和为 $c_i(i=0,1,2,\cdots,p-1)$, 则

$$S=\left(-\frac{n}{p}\right)^m\left(c_0+c_1\varepsilon+\cdots+c_{p-1}\varepsilon^{p-1}\right).$$

记

$$y_i=\sum_{\sum\limits_{k=1}^{m}f(k)\equiv i\pmod p}\prod_{k=1}^{m}f(k)\quad(i=0,1,\cdots,p-1),$$

则

$$S=\sum_{i=0}^{p-1}y_i\varepsilon^i.$$

于是存在整数 r, 使得

$$y_i=r+\left(-\frac{n}{p}\right)^m c_i\quad(i=0,1,\cdots,p-1).$$

对其进行累和得到

$$pr+\left(-\frac{n}{p}\right)^m(c_0+\cdots+c_{p-1})=y_0+\cdots+y_{p-1}=(1+\cdots+u)^m.$$

再结合

$$c_0+\cdots+c_{p-1}=(1+\cdots+(p-1))^m,$$

即得

$$\left(\frac{n}{p}\right)^m\mid y_0\,.$$

5 (1999 年第 40 届 IMO 预选题[8]) 设 $p>3$ 为素数, 对于集合 $\{0,1,\cdots,p-1\}$ 的每个非空子集 T, 设 $E(T)$ 是所有 $p-1$ 元数组 $\{x_1,x_2,\cdots,x_{p-1}\}$ 组成的集合, 其中每一个 $x_i\in T$, 且 $x_1+2x_2+\cdots+(p-1)x_{p-1}$ 为 p 的倍数. 证明: $|E\{0,1,3\}|\geq|E\{0,1,2\}|$, 当且仅当 $p=5$ 时等号成立.

提示 利用媒介 2 , 设

$$f(x)=1+x+x^2,\ F(x)=f(x)f(x^2)\cdots f(x^{p-1}),\ \omega=e^{i\frac{2\pi}{p}},$$

则

$$E(\{0,1,2\})=\frac{F(1)+\cdots+F(\omega^{p-1})}{p}=\frac{3^{p-1}+p-1}{p}.$$

类似地, 设

$$g(x)=1+x+x^3,\ G(x)=g(x)g(x^2)\cdots g(x^{p-1}),$$

则

$$E(\{0,1,3\})=\frac{3^{p-1}+(p-1)G(\omega)}{p}.$$

设

$$g(x)=(x-\lambda)(x-\mu)(x-\gamma),$$

则

$$G(\omega)=\frac{\lambda^p-1}{\lambda-1}\frac{\mu^p-1}{\mu-1}\frac{\gamma^p-1}{\gamma-1}=\frac{-2+\lambda^p+\mu^p+\gamma^p-\lambda^p\mu^p-\mu^p\gamma^p-\lambda^p\gamma^p}{-3}.$$

接下来问题转化为一个纯代数问题. 我们可以先证明

$$g(\omega^j)g(\omega^{p-j})>0\Rightarrow G(\omega)>0\,;$$

再证明

$$G(\omega)=1\Rightarrow p=5\,;$$

最后证明

$$G(\omega)\geq 1\,.$$

6 (第 58 届美国国家队选拔考试[9]) 是否存在一个非常值整系数多项式 $Q(x)$, 使得对于每个正整数 $n>2$, $Q(0),Q(1),\cdots,Q(n-1)$ 模 n 最多有 $0.499n$ 个不同的剩余.

提示 存在. 我们证明多项式 $Q(x)=420(x^2-1)^2$ 满足条件, 只需考虑 $n=4$ 和 n 为奇素数的情形.

当 $n=3,4,5,7$ 时, 结论显然成立; 当 $n=p\geq 11$ (p 为素数) 时, 有

$$\left(1-\left(\frac{1-t}{p}\right)\right)\left(1-\left(\frac{1+t}{p}\right)\right)=\begin{cases}4, & t^2\notin\left\{\frac{Q(x)}{420}\mid x\in\mathbb{Z}\right\}\\ 0, & t^2\in\left\{\frac{Q(x)}{420}\mid x\in\mathbb{Z}\right\}\end{cases},$$

这里 $t\notin\{1,\,p-1\}$ 且这里的运算都是在模 p 的意义下进行的, 这样 $Q(x)$ 模 p 的剩余数为

$$\begin{aligned}S&=\frac{p+1}{2}-\frac{1}{2}\frac{\sum\limits_{t=2}^{p-2}\left(1-\left(\frac{1-t}{p}\right)\right)\left(1-\left(\frac{1+t}{p}\right)\right)}{4}\\&=\frac{p+1}{2}-\frac{\sum\limits_{t=0}^{p-1}\left(1-\left(\frac{1-t}{p}\right)\right)\left(1-\left(\frac{1+t}{p}\right)\right)-2+\left(\frac{2}{p}\right)+\left(\frac{-2}{p}\right)}{8}\\&\leq\frac{p}{2}+1-\frac{1}{8}\sum_{t=0}^{p-1}\left(1-\left(\frac{1-t}{p}\right)-\left(\frac{1+t}{p}\right)+\left(\frac{1-t^2}{p}\right)\right)\end{aligned}$$

$$= \frac{p}{2} + 1 - \frac{1}{8}\left(p + \sum_{t=0}^{p-1}\left(\frac{1-t^2}{p}\right)\right),$$

而利用例 3 的处理方法可以求得

$$\sum_{t=0}^{p-1}\left(\frac{1-t^2}{p}\right) = (-1)^{\frac{p+1}{2}},$$

于是

$$S \leq \frac{p}{2} + 1 - \frac{1}{8}(p-1) = \frac{3}{8}(p+3) < 0.499p.$$

7[1] 设 p 为素数, 设 $S_1, S_2, \cdots, S_k$ 是非负整数组成的集合, 其中每个集合均包括 0, 且每个集合元素模 p 两两不同余. 若 $\sum_{i=1}^{k}(|\ S_i\ | -1) \geq p$, 证明: 对任意 $a_1, a_2, \cdots, a_k \in \mathbb{Z}/p\mathbb{Z}$, 均存在 $(x_1, x_2, \cdots, x_k) \in S_1 \times \cdots \times S_k$, 使得 $(x_1, x_2, \cdots, x_k) \neq (0, 0, \cdots, 0)$, 且 $p \mid x_1a_1 + x_2a_2 + \cdots + x_ka_k$.

提示 借助媒介 1 的思想, 构造多项式:

$$p(x_1, x_2, \cdots, x_k) = (x_1a_1 + x_2a_2 + \cdots + x_ka_k)^{p-1} - 1 + c\prod_{0\neq s_1\in S_1}(x_1 - s_1)\prod_{0\neq s_2\in S_2}(x_2 - s_2)\cdots\prod_{0\neq s_k\in S_k}(x_k - s_k),$$

这里常数 c 满足 $p(0, 0, \cdots, 0) = 0$. 则该多项式最高次项 $x_1^{|s_1|-1}\cdots x_k^{|s_k|-1}$ 系数非零, 于是由组合零点定理, 存在 $x_1, x_2, \cdots, x_k$, 使得 $p(x_1, x_2, \cdots, x_k) \neq 0$, 此时数组 $(x_1, x_2, \cdots, x_k)$ 满足条件.

参考文献

[1] A. Titu, D. Gabriel, Problems from the Book [M], XYZ Press, 2010.

[2] 武炳杰译, 第 33 届伊朗国家队选拔考试 [J], 中等数学 2017 增刊 II.

[3] 孙孟越等, 2017 年北大清华金秋营试题简析 [J], 数学新星网*学生专栏, 2017.10.23.

[4] 2018 Korea Winter Program Practice Test [J/OL],https://artofproblemsolving.com/community/c6h1570700.

[5] 2017 年 IMO 中国国家集训队教练组. 走向 IMO: 数学奥林匹克试题集锦 (2017) [M]. 上海: 华东师范大学出版社, 2017. 09.

[6] 《中等数学》编辑部, 国内外数学奥林匹克试题精选 (2002-2012) 数论部分 [M], 浙江大学出版社, 2015.10.

[7] 瞿振华, Snevily 猜测和一道全国联赛加试题 [J], 中等数学, 2015.01.

[8] 数学奥林匹克题库编委会, 国际数学奥林匹克预选题解 [M], 浙江大学出版社, 2012.01.

[9] 冯祖鸣, 第 58 届美国国家队选拔考试 [J], 中等数学, 2017.09.