第二届 AGMC 数学竞赛

答案 & 解析

【团队赛】

目录

（点击左侧红色超链接，快速跳转至目标页数）

第一部分【几何】

填空题.....2

简答题.....4

主题探究题.....5

第二部分【代数】

填空题.....11

简答题.....13

主题探究题.....15

第三部分【数论】

填空题.....27

简答题.....28

主题探究题.....30

第四部分【组合】

填空题.....50

简答题.....52

主题探究题.....54

题目来源&命题人员.....59

鸣谢.....60

第一部分【几何】

1. 填空题

已知一个三角形的三边长分别为 4，5，6，则其外接圆和内切圆的圆心之间的距离为 _____ .

答案：$\frac{2\sqrt{14}}{7}$

解析：

这道题其实就是一个结论题，不知道结论的话做起来确实比较费时间

可能会有巧妙的纯几何解法， 毕竟这是一场开卷考试嘛

为快速解决本题你最好需要知道四个公式/定理

（证明过程此处暂不赘述）

设一个三角形的三边长分别为a, b, c，其面积为S

（1） 外接圆半径公式

其外接圆半径$R = \frac{abc}{4S}$

（2） 内切圆半径公式

其内切圆半径为$r = \frac{2S}{a+b+c}$

（3） 海伦公式

设 $p = \frac{a+b+c}{2}$

则$S = \sqrt{p(p-a)(p-b)(p-c)}$

（4） 夏普尔定理

设外接圆和内切圆的圆心之间的距离为d

则有：$d^2 = R^2 - 2Rr$

接下来就是纯计算过程了

$$Rr = \frac{abc}{4S} \cdot \frac{2S}{a+b+c} = \frac{abc}{2(a+b+c)} = 4$$

$$p = \frac{a+b+c}{2} = \frac{15}{2}$$

$$S = \sqrt{p(p-a)(p-b)(p-c)} = \frac{15\sqrt{7}}{4}$$

$$R = \frac{abc}{4S} = \frac{8\sqrt{7}}{7}$$

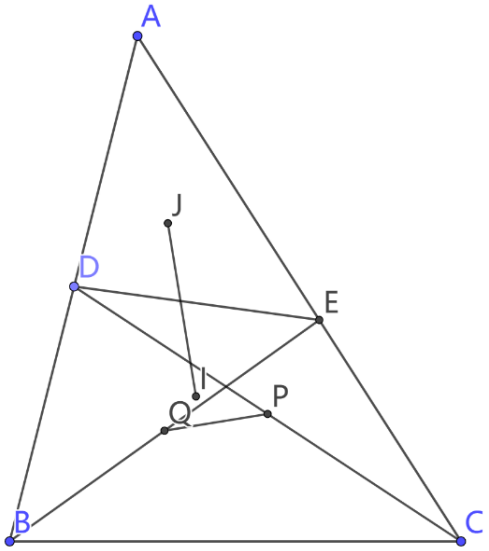
$$R^2 = \frac{64}{7}$$

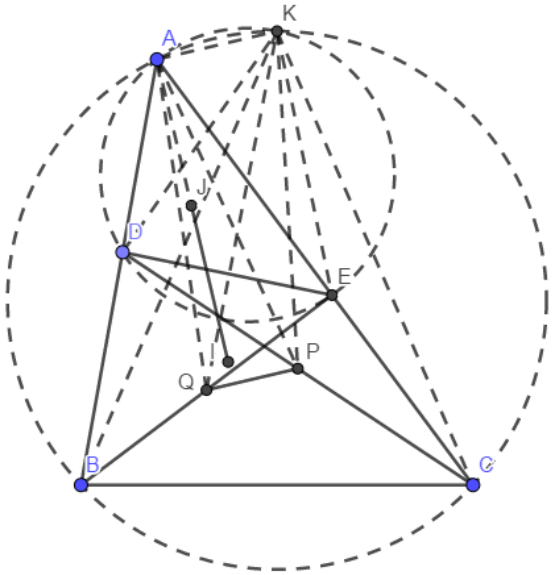
$$d^2 = R^2 - 2Rr = \frac{64}{7} - 2 \times 4 = \frac{8}{7}$$

$$d = \frac{2\sqrt{14}}{7}$$

2. 简答题

（1）如图，在△ABC 中，D，E 分别是 AB，AC 上两点，$BD=CE$，I，J 分别为△ABC，△ADE 内心，P，Q 分别为 CD，BE 中点，求证：$IJ\perp PQ$.（4 分）





（左图为原题的图，右图为解析专用图）

解析：由内心 I，J 都在∠BAC 的平分线上，

AIJ 共线取圆（ABC），圆（ADE）交于 K，

则 K 为四边形 BCED 密克点，易得△KDB≌△KEC

∠IAK=∠IAC+∠EAK=$\frac{1}{2}$∠BAC+∠KDE=$\frac{1}{2}$∠BAC+（90°$-\frac{1}{2}$∠BAC）=90°

那么证 PQ∥AK 即可

$$\mathrm{PQ}\parallel\mathrm{AK}\Leftrightarrow S_{\triangle\mathrm{AKQ}}=S_{\triangle\mathrm{AKC}}\Leftrightarrow\frac{S_{\triangle\mathrm{AKD}}+S_{\triangle\mathrm{AKC}}}{2}=\frac{S_{\triangle\mathrm{AKB}}+S_{\triangle\mathrm{AKE}}}{2}$$

$$\Leftrightarrow S_{\triangle\mathrm{AKC}}-S_{\triangle\mathrm{AKE}}=S_{\triangle\mathrm{AKB}}-S_{\triangle\mathrm{AKD}}\Leftrightarrow S_{\triangle\mathrm{KDB}}-S_{\triangle\mathrm{KEC}}$$

又因为△KDB≌△KEC

证毕.

3. 主题探究题

调和点列是几何世界中璀璨的明珠，散发着无尽的光芒。其规律简洁而优美：对于线段 AB 的内分点 C 和外分点 D，若 $\frac{AC}{BC}=\frac{AD}{BD}$，则称 A，B，C，D 为调和点列。

① 轻描淡写勾阿圆

我们曾学习过“阿波罗尼斯圆”这一特殊的几何图形，若 A，B，C，D 为调和点列，作以 CD 为直径的一个圆，则该圆上的动点 P，始终满足条件 $\frac{\mathrm{AP}}{\mathrm{BP}}=k\,(k\neq 1)$，该结论的逆命题依然成立。

给定非等边△ABC，作∠A 的内，外角平分线分别交直线 BC 于点 X，Y，作以 XY 为直径的圆，即阿波罗尼斯圆，记该圆为圆 a，接着同理过点 B，C 作出圆 b，圆 c，求证：圆 a，圆 b，圆 c 有且仅有两个公共点.（5 分）

② 信手执笔出调和

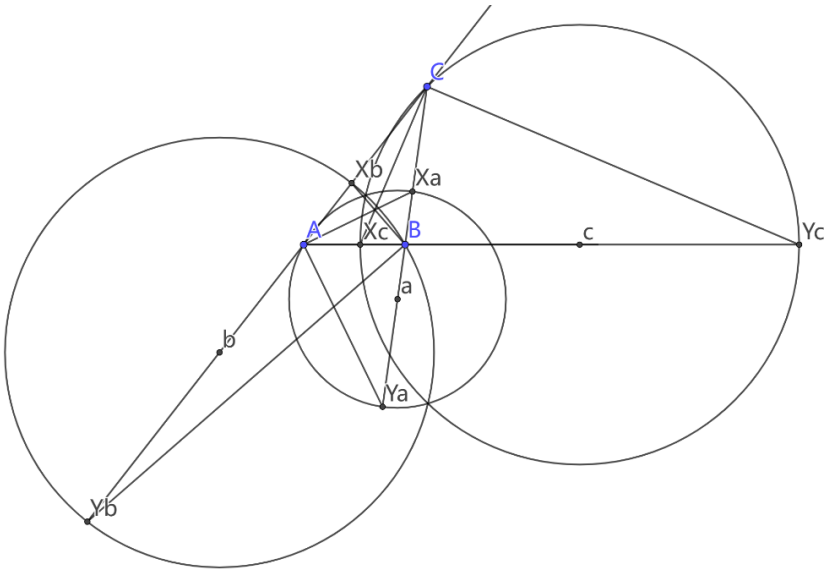
请尝试证明如下有关调和点列的结论：△ABC 的三个顶点在对应边上的射影分别为 D，E，F，其外心为 O，点 B，C 对应旁心为 I_b，I_c，EF，OD 交 I_bI_c 于点 X，Y，求证：I_b，X，Y，I_c 为调和点列.（5 分）

③ 重章叠唱藏瑰丽

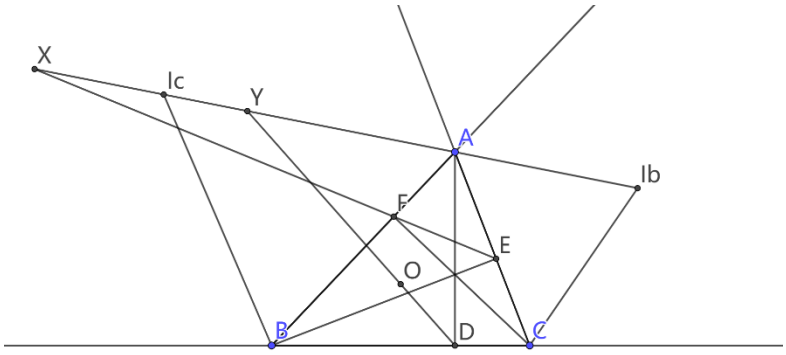
在②的条件下，设过点 B，Y，C 的圆 K 与 I_bI_c 的第二个交点为 T，则平面上存在一个点 S 使△TBC∽△SFE，且该点能通过只用圆规仅画一个圆的方式作出（所给图的所有条件均能使用），试找出该点并证明结论. （6 分）

作答上题时可能用到的图

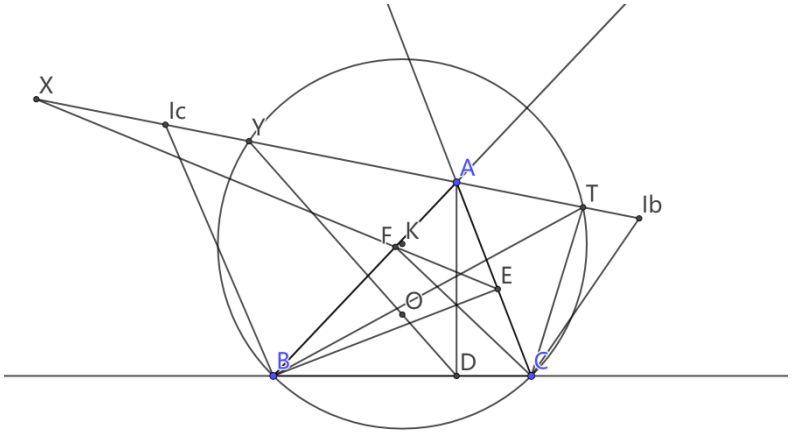
第①题图



第②题图



第③题图



（1）证明：

设圆a，圆b交点为 X，Y

则有

$$\begin{cases} \dfrac{BX}{CX} = \dfrac{AB}{AC} \\ \dfrac{CX}{AX} = \dfrac{BC}{AB} \end{cases}$$

因此有

$$\frac{BC}{AC} = \frac{BX}{AX}$$

则 X 在圆c上

同理可得 Y 也在圆c上

证毕.

（2）证明：

作圆 O 和弧 BAC 中点 N

注意到 IcC<IbC

设 T 为 BC 延长线上一点

又因为∠IbCA=∠IbCT

只需证明∠YCA=∠XCT

由∠CEX=∠AEF=∠ABC=∠CNX 可知 C，E，N，X 四点共圆

从而∠ACB+∠XCT=180°—∠ACX=∠ENX

故∠XCT=∠ENX-∠ACB=∠NEA+∠NAC-∠ACB=∠NEA+∠NCA

又因为∠YCA=∠NCA+∠NCY

只需证明∠NEA=∠NCY

过点 O 作 BC 平行线交 CY 于点 S

则△ADC 和△NOS 位似，位似中心为点 Y

又因为△COT~△BAE

设 NC 和 OS 交于点 P

则∠MPC=2∠CNM=∠BAE

因此△MXC~△BAE

从而∠SMP=∠SNP=∠SNO—∠CNM=90°—∠ACB—$\frac{1}{2}$∠BAC

=∠ABC—（90°—$\frac{1}{2}$∠BAC）=∠ABN

且∠NPO=90°—∠CNM=∠NAC

因此∠MPS=∠BAN

从而△BAN~△MPS

因此四边形 BANE~四边形 MPSC

最终∠NCY=∠NEA

证毕.

（3）

证明：

给定图中作以 O 为圆心，OB 为半径的圆与 TY 交于点 Q

即为所求.

即证明△QFE~△TCB

其中 Q 为弧 BAC 的中点

由（2）可知∠NEF=∠NEA+∠AEF=∠NCY+∠ABC

=∠CNY+∠NCY=180°—∠NYC

因此∠NEF=∠TBC

同理可得∠NFE=∠TCB

证毕.

第二部分【代数】

1. 填空题

[A] 设$a,b,c\in\mathbb{C}$，若$\begin{cases}a^2=b-c\\b^2=c-a\\c^2=a-b\end{cases}$，则$a+b+c=$_____.

答案：0 或 $\boldsymbol{i\sqrt{6}}$ 或 $\boldsymbol{-i\sqrt{6}}$

解析：

设$a+b+c=k$

将三式相加，可得$a^2+b^2+c^2=0$.

根据$(a+b+c)^2=k^2$，可以推得$ab+ac+bc=\frac{k^2}{2}$

将$a^2=b-c$两边同乘a，可得$a^3=ab-ac$

以此类推，可得$b^3=bc-ab$，$c^3=ac-bc$

将三式相加，可得$a^3+b^3+c^3=0$.

$$-3abc=a^3+b^3+c^3-3abc$$

$$=(a+b+c)(a^2+b^2+c^2-ab-ac-bc)=-\frac{k^3}{2}$$

因此 $abc=\frac{k^3}{6}$。

接着我们用 3 种方法表示$a^4+b^4+c^4$

方法①:

$$a^4+b^4+c^4=\sum_{cyc}(a-b)^2$$

$$= 2(a^2 + b^2 + c^2) - 2(ab + ac + bc)$$

$$= -k^2$$

方法②:

$$a^4 + b^4 + c^4 = \sum_{cyc} a(ka^2 - \frac{k^2 a}{2} + \frac{k^3}{6})$$

$$= \sum_{cyc} k(ka^2 - \frac{k^2 a}{2} + \frac{k^3}{6}) - \frac{k^2 a^2}{2} + \frac{k^3 a}{6}$$

$$= \sum_{cyc} k(ka^2 - \frac{k^2 a}{2} + \frac{k^3}{6}) - \frac{k^2 a^2}{2} + \frac{k^3 a}{6}$$

$$= \sum_{cyc} a^2 \cdot \frac{k^2}{2} - a \cdot \frac{k^3}{3} + \frac{k^4}{6}$$

$$= -\frac{k^4}{3} + \frac{k^4}{2}$$

$$= \frac{k^4}{6}$$

方法③:

$$a^4 + b^4 + c^4 = \sum_{cyc} a^2(b - c)$$

$$= (a - b)(b - c)(c - a)$$

$$= -a^2 b^2 c^2$$

$$= -\frac{k^6}{36}$$

使用其中两个列方程，可得$a + b + c = k = 0$ 或 $i\sqrt{6}$ 或 $-i\sqrt{6}$

2. 简答题

设 x, y, z 为实数，且 $xyz = 1$，存在函数 f：$\mathbb{R} \setminus \{0\} \to \mathbb{R}$ 使得

$$f(x)^2 - f(y)f(z) = x(x+y+z)(f(x)+f(y)+f(z))$$

求 $f(x)$ 的表达式.

解析：

$f(x) = 0$ 或 $f(x) = x^2 - \dfrac{1}{x}$

设 x, y, z 互不相等，且 $x+y+z \neq 0$，于是我们可以得到

$$f(x)^2 - f(y)f(z) = x(x+y+z)(f(x)+f(y)+f(z)) \quad ①$$

$$f(y)^2 - f(z)f(x) = y(x+y+z)(f(x)+f(y)+f(z)) \quad ②$$

$$f(z)^2 - f(x)f(y) = z(x+y+z)(f(x)+f(y)+f(z)) \quad ③$$

将 $①^2 - ② \cdot ③$ 得到

$$f(x)(f(x)^3 + f(y)^3 + f(z)^3 - 3f(x)f(y)f(z)) = (x^2 - yz)(x+y+z)^2(f(x)+f(y)+f(z))^2$$

不妨设三元函数

$$F(x, y, z) = f(x)^3 + f(y)^3 + f(z)^3$$

$$G(x, y, z) = (x+y+z)(f(x)+f(y)+f(z))$$

则可将原式化为

$$f(x)F(x,y,z)=(x^2-yz)G(x,y,z)^2$$

不妨设 $H(x,y,z)=\dfrac{G(x,y,z)^2}{F(x,y,z)}$

则可将原式化为

$$\frac{f(x)}{x^2-yz}=H(x,y,z)$$

$$f(x)=H(x,y,z)(x^2-yz)$$

同理可得

$$f(y)=H(x,y,z)(y^2-xz)$$

$$f(z)=H(x,y,z)(z^2-xy)$$

代入①可得

$$H(x,y,z)^2x(x^3+y^3+z^3-3xyz)=H(x,y,z)x(x^3+y^3+z^3-3xyz)$$

易得 $H(x,y,z)=0$ 或 $H(x,y,z)=1$

从而

$$f(x)=f(y)=f(z)=0$$

或

$$f(x)=x^2-yz,\ f(y)=y^2-xz,\ f(z)=z^2-xy$$

又因为 $xyz=1$

因此 $f(x)=0$ 或 $f(x)=x^2-\dfrac{1}{x}$

3. 主题探究题

我们称 $k[x]$ 为定义在数域 k 上的一元多项式环，$\forall f(x) \in k[x]$，$f(x) = \sum_{i=0}^{n} a_i x^i$，

称 n 为 $f(x)$ 的次数，记作 $n = \deg f(x)$，$n \in \mathbb{N}$，$a_i \in k$. 我们称一个 $f(x)$ 在 k 上

可约：当 $\exists\, g(x)$，$h(x) \in k[x]$，$g(x)$，$h(x)$ 的次数不为 0，且 $f(x) = g(x) \cdot h(x)$.

（**1**） 求证：$x^5 - x - 1$ 在 $Q[x]$ 上不可约，并进一步讨论，对于哪些 $n \in \mathbb{N}^+$，

$x^n - x - 1$ 在 $Q[x]$ 上不可约.（3 分）

（**2**） 设 p 是一个质数，p 的 b 进制展开式为 $p = \sum_{i=0}^{n} a_i b^i$，其中 a_i 表示各位数，

$0 \le a_i \le b - 1$，求证：多项式 $f(x) = \sum_{i=0}^{n} a_i x^i$ 在 $Q[x]$ 上不可约.（3 分）

（**3**） 设 p 是一个质数，存在 $f(x) \in Z[x]$，且 $f(x)$ 在 $Z[x]$ 上不可约，并使得

$[(-1)^{\deg f(x)} f(0)]^{\frac{1}{p}}$ 是无理数，求证：$f(x^p)$ 在 $Z[x]$ 上不可约.（6 分）

（**4**） 设 P，Q 为两个复系数多项式，$r \in R^+$，若在以原点为圆心，半径为 r

的圆周上任意一点 Z，都有 $|P(Z) - Q(Z)| < |Q(Z)|$，求证：P，Q 在此圆内有

相同数量的零点.（且计重数，即 $(Z - Z_0)^k$ 算 k 个）（8 分）

（**1**） 求证：x^5-x-1 在 $Q[x]$ 上不可约，并进一步讨论，对于哪些$n\in\mathbb{N}^+$，

x^n-x-1在 $Q[x]$ 上不可约.（3 分）

解析：

引理 1

$$2Re\left(z-\frac{1}{z}\right)>\frac{1}{|z|^2}-1$$

其中$Re(z)$指复数z的实部。

由引理 1

$$2Re\left(z_1-\frac{1}{z_1}\right)+2Re\left(z_2-\frac{1}{z_2}\right)+\cdots+2Re\left(z_s-\frac{1}{z_s}\right)$$
$$>\frac{1}{|z_1|^2}+\frac{1}{|z_2|^2}+\cdots+\frac{1}{|z_s|^2}-s\geq 0$$

根据均值不等式，因为$|z_i|$的积恰是$|f(0)|=1$，于是

$$Re\left(z_1-\frac{1}{z_1}\right)+Re\left(z_2-\frac{1}{z_2}\right)+\cdots+Re\left(z_s-\frac{1}{z_s}\right)>0$$

另一方面，因为f首项系数为 1 且为整系数

$$Re\left(z_1-\frac{1}{z_1}\right)+Re\left(z_2-\frac{1}{z_2}\right)+\cdots+Re\left(z_s-\frac{1}{z_s}\right)$$

是一个整数，所以至少是 1，对于g同理可推出

$$Re(z_1-\frac{1}{z_1}+z_2-\frac{1}{z_2}+\cdots+z_n-\frac{1}{z_n})\geq 2$$

其中z_1,z_2,z_n是x^n-x-1所有的根。

但是，这是不可能的。

因为根据$Viete$公式

$$z_1-\frac{1}{z_1}+z_2-\frac{1}{z_2}+\cdots+z_n-\frac{1}{z_n}=1$$

这表明任何这样的分解都是不可能的，所以x^n-x-1在$Z[x]$上不可约。

我们现在只需要应用高斯引理来获得一个完整的证明。

（**2**） 设 p 是一个质数，p 的 b 进制展开式为 $p=\sum_{i=0}^{n}a_ib^i$，其中 a_i 表示各位数，$0\le a_i\le b-1$，求证：多项式 $f(x)=\sum_{i=0}^{n}a_ix^i$ 在 $Q[x]$ 上不可约.（3 分）

解析：

显然$\gcd(a_0,a_1,\dots,a_n)=1$，所以由高斯引理足以证明$f$在 Z 上不可约。

首先，我们讨论$b>3$的情况，$b=2$的情况更难一点。

假设

$$f(x)=g(x)h(x)$$

是f的非平凡因式分解。

因为p是一个质数，数字$g(b)$和$h(b)$之一等于1或-1

令这个数字是$g(b)$，而$x_1, x_2, \dots, x_n$是f的零点，则存在$\{1,2,\dots,n\}$的一个子集A满足

$$g(x) = a\prod_{i\in A}(x - x_i)$$

我们现在证明了一个有用的结果。

引理 2　f的每个复零点都有非正实部或绝对值小于$\frac{1+\sqrt{4b-3}}{2}$

证明如下，

观察到，若$|z| > 1$且$Re(z) > 0$，则$Re(\frac{1}{z}) > 0$

根据三角不等式

$$\left|\frac{f(z)}{z^n}\right| \geq \left|a_n + \frac{a_{n-1}}{z}\right| - (b-1)(\frac{1}{|z|^2} + \cdots + \frac{1}{|z|^n})$$

$$> Re\left(a_n + \frac{a_{n-1}}{z}\right) - \frac{b-1}{|z|^2 - |z|}$$

$$\geq \frac{|z|^2 - |z| - (b-1)}{|z|^2 - |z|}$$

所以若$f(z) = 0$且$Re(z) > 0$，则

$$|z| \leq 1 \quad 或 \quad |z| < \frac{1+\sqrt{4b-3}}{2}$$

这就建立了引理。

现在仍然需要巧妙地应用这个引理。

我们断言对于f的任意零点x_i有$|b-x_i|>1$

事实上，若$Re(x_i)\le 0$，一切都清楚了。否则

$$|b-x_i|\ge b-|x_i|>b-\frac{1+\sqrt{4b-3}}{2}\ge 1$$

若$b\ge 3$则很容易地验证，故$|g(b)|>1$，矛盾。

现在来看更难的情况，当$b=2$时：

我们将提供一个非常漂亮的解决方案。

想法是要证明对于f的任意零点x_i有$|2-x_i|>|1-x_i|$

保留先前的符号，我们将推断

$$1=|g(2)|>|g(1)|$$

于是$g(1)=0$

这意味着$f(1)=0$，显然不可能。

现在取x为f的一个零点并观察到若$|2-x|>|1-x|$，

则$Re(x)>(\frac{3}{2})$

所以若$y=\frac{1}{x}$有$|y|<1$，且y满足关系式

$$y^n+\left(\frac{1}{2}\pm\frac{1}{2}\right)y^{n-1}+\cdots+\left(\frac{1}{2}\pm\frac{1}{2}\right)y+1=0$$

乘以y^{n+1}并把两个关系式相加，我们得到同一类型的关系式，（但是随着n的增加）

通过重复这个论述，我们推断

存在无穷多个N使得y满足关系式

$$y^N+\left(\frac{1}{2}\pm\frac{1}{2}\right)y^{N-1}+\cdots+\left(\frac{1}{2}\pm\frac{1}{2}\right)+1=0$$

或写作

$$1+\frac{1}{2}\cdot(y+y^2+\cdots+y^N)=\frac{1}{2}\cdot(\pm y\pm y^2\pm\cdots\pm y^N)$$

三角不等式意味着对无数个N有

$$\left|\frac{2-y-y^{N+1}}{2(1-y)}\right|\leq\frac{|y|-|y|^{N+1}}{2(1-|y|)}$$

考虑到$|y|<1$，由上面的不等式推出

$$\left|\frac{2-y}{1-y}\right|\leq\frac{|y|}{1-|y|}$$

最后一个不等式意味着

$$\left|\frac{2x-1}{x-1}\right|\leq\frac{1}{|x|-1}\leq 2$$

于是

$$|2x-1|\leq|2x-2|$$

这对于$Re(x)\geq\frac{3}{2}$是不可能的

至此我们完成了断言的证明，也解决了此题目。

（**3**）设 p 是一个质数，存在 $f(x) \in Z[x]$，且 $f(x)$ 在 $Z[x]$ 上不可约，并使得

$[(-1)^{\deg f(x)} f(0)]^{\frac{1}{p}}$ 是无理数，求证：$f(x^p)$ 在 $Z[x]$ 上不可约.（6 分）

解析：

考虑α为f的一个复零点，设

$$n = \deg f(x), \qquad g(x) = x^p$$

$h = g - \alpha$，应用前面的结果，可以证明h在$Q[\alpha][x]$上不可约。

因为$Q[\alpha] \in C$可以证明α不是$Q[\alpha]$的元素的p次方。

假设存在$u \in Q[x]$至多为$n-1$次，使得$\alpha = u^p(\alpha)$成立

设$\alpha_1, \alpha_2, \dots \alpha_n$是$f$的零点

因为f不可约且α是它的一个零点，f是α的最小多项式，

所以f一定可以整除$u^p(x) - x$，从而

$$\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_n = (u(\alpha_1) \cdot u(\alpha_2) \cdot \dots \cdot u(\alpha_n))^p$$

是有理数

但是

$$\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_n = (-1)^n f(0)$$

意味着$\sqrt[p]{(-1)^n f(0)} \in Q$，矛盾。

（**4**）设 P，Q 为两个复系数多项式，$r \in R^{+}$，若在以原点为圆心，半径为 r 的圆周上任意一点 Z，都有$|P(Z)-Q(Z)|<|Q(Z)|$，求证：P，Q 在此圆内有相同数量的零点.（且计重数，即 $(Z-Z_0)^k$ 算 k 个）（8 分）

证明：

这个定理的证明不是初等的，但是用一点微积分，就可以很优雅地证明它。

设L为所有可微的，具有连续导数的弧γ：$[0,2\pi] \to C$的集合，

满足$\gamma(0)=\gamma(2\pi)$和γ不会消失，$\gamma \in L$的指标定义为

$$I(\gamma)=\frac{1}{2\pi i}\cdot\int_0^{2\pi}\frac{\gamma'(t)}{\gamma(t)}dt$$

我们断言$I(\gamma)$是一个整数

事实上，考虑

$$K(t)=e^{\int_0^t \frac{\gamma'(t)}{\gamma(t)}dt}$$

并注意到K是可微的，以及

$$K'(t)=K(t)\cdot\frac{\gamma'(t)}{\gamma(t)}$$

则$\frac{K(t)}{I(\gamma)}$是一个连续函数。

所以，由$\gamma(0)=\gamma(2\pi)$

必有$K(0)=K(2\pi)$。

恰好说明$I(\gamma)$是一个整数。

下列结果对证明是必要的：

引理 3　在不包含原点的圆中弧$\gamma \in L$的指数是 0

证明.　设$B(x,r)$为以x为圆心，半径$r>0$的圆，假设γ含在不含原点在内的$B(\omega,s)$中（于是$s<|\omega|$），即对于所有t，$|\gamma(t)-\omega|<s$.

目的是做一个γ的连续变形，保持指数不变。在某一时刻，新曲线的指数可以被简单地计算出来，为此取$u \in [0,1]$，并考虑在$[0,\ 2\pi]$上应用

$$f_u(t)=u\gamma(t)+(1-u)\omega$$

不等式表明$f_u \in L$且这条弧在$B(\omega,s)$内。

另一方面，我们断言映射$\phi(u)=I(f_u)$是连续的。

因为它只取整数值（根据前面的标注），故必为常数。

因此，$I(\gamma)=I(f_1)=I(f_0)=0$

所以，让我们证明$I(f_u)$对于u是连续的。

事实上，注意到

$$\left|\frac{f_u'(t)}{f_u(t)}-\frac{f_v'(t)}{f_v(t)}\right|=\left|\frac{\omega(u-v)\gamma'(t)}{(u\gamma(t)+(1-u)\omega)(u\gamma(t)+(1-v)\omega)}\right|$$

$$\leq\frac{|\omega|\cdot|u-v|\cdot|\gamma'(t)|}{(|\omega|-s)^2}$$

因为

$$|u\gamma(t)+(1-u)\omega| \geq |\omega|-|u|\cdot|\gamma(t)-\omega| \geq |\omega|-s$$

对这个不等式应用积分推出$I(f_u)$满足

$$|I(f_u)-I(f_v)| \leq \frac{|\omega|}{2\pi(|\omega|-s)^2}\cdot\int_0^{2\pi}|\gamma'(t)|dt\cdot|u-v|$$

这就证明了$I(f_u)$连续，引理证毕。

这个引理意味着L中两条足够接近的曲线具有相等的指数。

事实上，假设γ_1和γ_2属于L且对于所有t满足

$$|\gamma_1(t)-\gamma_2(t)| < |\gamma_2(t)|$$

那么对于所有t圆弧$\gamma(t)=\frac{\gamma_1(t)}{\gamma_2(t)}$满足

$$|\gamma_1(t)-1| < 1$$

因为$|\gamma_1(t)-1|$在紧区间$[0,2\pi]$也连续，推出它的最大值小于 1，即存在一个不包含原点的圆包含γ。

由引理，γ有指数 0

但快速计算表明$I(\gamma)=I(\gamma_1)-I(\gamma_2)$

于是γ_1和γ_2具有相等的指数。

最后，让我们证明这个特殊的 Rouche 定理。

考虑弧$\gamma_1(t) = P(Re^{it})$和$\gamma_2(t) = Q(Re^{it})$

观察到不等式$|P(z) - Q(z)|$，

意味着γ_i不会在$[0, 2\pi]$消失。

于是γ_1, γ_2属于L且

$$|\gamma_1(t) - \gamma_2(t)| < |\gamma_2(t)|$$

这样两条弧有相同的指数。

但对于多项式P很容易计算出相关曲线的指数！

事实上，假设

$$P(z) = a(z - z_1)(z - z_2) \dots (z - z_n)$$

其中z_i不必不同，那么显而易见

$$\frac{P'(z)}{P(z)} = \sum_{i=1}^{n} \frac{1}{z - z_i}$$

这表明若$\gamma(t) = P(Re^{it})$，则

$$I(\gamma) = \frac{R}{2\pi} \cdot \sum_{j=1}^{n} \int_0^{2\pi} \frac{e^{it}}{Re^{it} - z_j} dt$$

现在我们看到$|z_j| \neq R$

假设$|z_j| < R$，那么

$$\int_0^{2\pi} \frac{e^{it}}{Re^{it} - z_j} dt = \frac{1}{R} \int_0^{2\pi} \frac{1}{1 - \frac{z_j e^{-it}}{R}} dt = \frac{2\pi}{R}$$

事实上，

$$\frac{1}{1 - \frac{z_j e^{-it}}{R}} = 1 + \sum_{m \geq 1} \frac{z_j^m e^{-imt}}{R^m}$$

和e^{-imt}对于所有$m \geq 1$在$[0, 2\pi]$上的平均值为 0

因为关于t的一致收敛性，

我们可以改变积分和求和的顺序，

可以看到

$$\frac{1}{R} \int_0^{2\pi} \frac{1}{1 - \frac{z_j e^{-it}}{R}} dt = \frac{2\pi}{R}$$

现在，同理可证

$$\int_0^{2\pi} \frac{e^{it}}{Re^{it} - z_j} dt = 0, \quad |z_j| > R$$

因此$I(\gamma)$恰好是以原点为中心的，半径为R的圆内P的零点个数

证毕.

第三部分【数论】

1. 填空题

[A] 设 n 为两位数，若 $2n+3 \mid 2^{n!}-1$，则 $n_{min}=$ _____.

答案：88

解析：首先我们证明结论：如果$n \geq 10$，那么当且仅当 $n+1$ 和

$2n+3$ 都是素数时，才有 $2n+3 \mid 2^{n!}-1$，

如果 $n+1$ 和 $2n+3$ 都是素数，则假设 $2n+3 \mid 2^{n!}-1$，根据费马小定理，有$2n+3 \mid 2^{2n+2}-1$，然而，由于 $n+1$ 是素数，$\gcd(2n+2, n!)=2$，因此 $2n+3 \mid 2^2-1=3$，产生矛盾。

接下来我们引入$\varphi(n)$的概念，$\varphi(n)$代表小于等于n且与n互质的正整数的个数。

如果 $2n+3$ 是合数，则$\varphi(2n+3)$是偶数且最多为$2n$，因此$\varphi(2n+3)|n!$

如果 $n+1$ 是合数但 $2n+3$ 是素数，则$2n+2|n!$，因此

$2n+3|\ 2^{n!}-1$，

100 以内的素数是 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53、59、61、67、71、73、79、83、89、97。设其中一个为 $n+1$，那么使得$2n+3$为素数的最大数字是 89，因此 n_{min}为 88。

2. 简答题

$v_p(n)$表示正整数n的素因子分解式中素数p的幂次. 设$a \in \mathbb{N}^+$，若存在至少 2 个奇素数p能够使不等式$\sum_{k=1}^{a}(-1)^{v_p(k!)} < 0$成立，求$a_{min}$

答案：229

解析：

设$t = a + 1$，题目中$\sum_{k=1}^{a}(-1)^{v_p(k!)}$即为$f(a+1) - 1 = f(t) - 1$，最小值只能取到$-1$，而且如果对于两个奇素数$p_1, p_2$同时使$f(p_1, t) = f(p_2, t) = 0$，假设在 1~250 之间存在这样的$t$.

对奇素数$p \geq 7$，由于$p^3 \geq 343$，在 1~250 之间的$f(p, t)$的零点只有$t = 2mp, 1 \leq m \leq \frac{p-1}{2}$

所以如果$p_1, p_2 \geq 7$，在 1~250 之间不会有$f(p_1, t)$和$f(p_2, t)$的公共零点t.

否则若$p_1 > p_2$，由零点的形式可知$t|2p_1p_2$，但$2p_1p_2 > 2p_2^2 > 2p_2(p_2-1)$不可能是$f(p_2,t)$的零点.

如果$p_2 = 3$，$f(3,t)$在 1~250 之间的零点分别是$2\times 3 = 6$,

$2\times 3^3 - 2\times 3 = 48$，$2\times 3^3 = 54$

如果$p_2 = 5$，$f(5,t)$在 1~250 之间的零点分别是$2\times 5 = 10$,

$4\times 5 = 20$，$2\times 5^3 - 4\times 5 = 230$，$2\times 5^3 = 250$.

$f(3,t)$和$f(5,t)$在 1~250 之间没有公共零点，那$p_1 \geq 7$，并且$t|2p_1$

$f(3,t)$的 3 个零点都没有大于 3 的素因子，$f(5,t)$的 5 个零点只有 230 有≥7 的素因子 23，且$230 = 2\times 5\times 23$是$f(23,t)$的零点

所以 在 1~250 之间仅有$t = 230$同时是两个奇素数$p_1 = 23$和$p_2 = 5$的$f(p,t)$公共零点.

对应的$a = t - 1 = 229$便是最小的满足题意的正整数.

3. 主题探究题

二次剩余是初等数论中的重要概念，为判断二次（甚至高次）同余方程组是否有解这一类问题提供了基础的理论依据. 在对于二次剩余的分析中，引入勒让德符号不仅将文字语言全部转为数学语言，同时大大简化了计算，更容易推导出一系列二次剩余的性质. 下面，我们首先给出两者定义：

二次剩余：给定 $m \in N,\ m \geq 2,\ a \in Z,\ \gcd(a, m) = 1$，若存在 $x \in Z$，使得 $x^2 \equiv a \pmod{m}$，则称 a 为模 m 的二次剩余；否则，则称 a 为模 m 的二次非剩余.

勒让德符号：给定素数 p， $a \in Z$，定义：

$$(\frac{a}{p}) = \begin{cases} 1 & \text{当 } a \text{ 为模 } m \text{ 的二次剩余} \\ -1 & \text{当 } a \text{ 为模 } m \text{ 的二次非剩余} \\ 0 & \text{当 } p \text{ 整除 } a \end{cases}$$

下面我们给出有关两个与二次剩余和勒让德符号相关的重要定理，在作答本题时可直接使用.

欧拉判别法则：设 p 为奇素数， $\gcd(a, p) = 1$.

若 $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$，则 a 为模 m 的二次剩余；

若 $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$，则 a 为模 m 的二次非剩余.

高斯引理：设 p 为奇素数， $\gcd(a, p) = 1$，则

$$(\frac{x}{p}) = (-1)^{|\{1 \leq k < \frac{p}{2} : \{kx\}_p > \frac{p}{2}\}|}$$

其中 $\{kx\}_p$ 代表 kx 模 p 后的余数.

下面，我们来证明如下命题：

（1） （4 分）设 p 为奇素数，$\gcd(a,p)=1$，$f(x)$ 为整系数多项式，当 x 遍历模 p 的完全剩余系时，

$$\sum_{x \pmod p} \left(\frac{ax+b}{p}\right)=0$$

（2） （4 分）由（**1**）的条件，若多项式 $f(x)$ 是奇函数，则

当 p 为 $4m+1$ 型素数时，有：

$$\sum_{x=1}^{p-1}\left(\frac{f(x)}{p}\right)=2\sum_{x=1}^{\frac{p-1}{2}}\left(\frac{f(x)}{p}\right)$$

当 p 为 $4m+3$ 型素数时，有：

$$\sum_{x=1}^{p-1}\left(\frac{f(x)}{p}\right)=0$$

（3） （6 分）当 p 为足够大的 $4m+3$ 型素数时，求证：存在 x，y，$z\in\{1,2,\ldots,p-1\}$，使得：

$$\begin{cases}\left(\frac{x}{p}\right)=\left(\frac{x+1}{p}\right)=1\\ -\left(\frac{y}{p}\right)=\left(\frac{y+1}{p}\right)=1\\ \left(\frac{z}{p}\right)=-\left(\frac{z+1}{p}\right)=1\end{cases}$$

（4） （6 分） 设 p 为奇素数，$\gcd(x(1-x),p)=1$，则有：

$$(-1)^{\left|\{1\le k<\frac{p}{2}:\{kx\}_p>p\}\right|}=\left(\frac{2x(1-x)}{p}\right)$$

（1）解析：

引理 1　因为$(a,p)=1$，所以当x遍历模p的完全剩余系时，

$ax+b$也遍历其完全剩余系

----------1 分

引理 2　若$a\equiv a'\ (mod\ \ p)$，则$\left(\frac{a}{p}\right)=\left(\frac{a\prime}{p}\right)$

证明：

$$a\equiv a'\ (mod\ \ p)$$

$$a^{\frac{p-1}{2}}\equiv a'^{\frac{p-1}{2}}\ \equiv 1(mod\ \ p)$$

因为p为奇素数，通过费马小定理，有：

$$a^{\frac{p-1}{2}}\equiv a'^{\frac{p-1}{2}}\ \equiv 1(mod\ \ p)\text{或者}$$

$$a^{\frac{p-1}{2}}\equiv a'^{\frac{p-1}{2}}\equiv -1\ (mod\ \ p)\text{成立}$$

由欧拉判别法则，a和a'同为模p的二次剩余，或模p的二次非剩

余，即$\left(\frac{a}{p}\right)=\left(\frac{a\prime}{p}\right)$

----------1 分

引理 3　p为奇素数，在$a\in\{1,2\dots p-1\}$中，有一半的a为模p的二次剩余，另一半的a为模p的二次非剩余.

考虑模p意义下的多项式$f(x)=x^p-x$

由费马小定理，对于$\forall a\in\{1,2\dots p-1\}$,

$a^{p-1}\equiv 1\ (mod\ \ p)$，$a^p-a\equiv 0\ (mod\ \ p)$

因此，$\forall a\in\{1,2\dots p-1\}$为$f(x)$的根$(mod\ \ p)$

$$f(x)=x(x^{p-1}-1)=x\left(x^{\frac{p-1}{2}}+1\right)\left(x^{\frac{p-1}{2}}-1\right)=xg(x)h(x)$$

$g(x)$的最高次项指数为$\frac{p-1}{2}$

因此由数论中的拉格朗日定理可知

$$g(x)=x^{\frac{p-1}{2}}+1\equiv 0(mod\ \ p)$$

至多有$\frac{p-1}{2}$个解；

同理，$h(x)=x^{\frac{p-1}{2}}-1\equiv 0(mod\ \ p)$

至多有$\frac{p-1}{2}$个解。

当$f(x)\equiv 0(mod\ \ p)$，且$x\in\{1,2\dots p-1\}$时，$\gcd(x,p)=1$

$f(x)\equiv 0(mod\ \ p)$，因此$g(x)h(x)\equiv 0(mod\ \ p)$

故$g(x)\equiv 0(mod\ \ p)$或$h(x)\equiv 0(mod\ \ p)$

现在已知$\{1,2\dots p-1\}$全为$f(x)$的解，

则$g(x)$和$h(x)$均恰有$\frac{p-1}{2}$个解。

由欧拉判别法则，有一半的$a\in\{1,2\dots p-1\}$为模p的二次剩余，

另一半为模p的二次非剩余。

----------1 分

回到原问题，

由引理 1，2，$\sum_{x\,(\mathrm{mod}\,p)}(\frac{ax+b}{p})=\sum_{x\,(\mathrm{mod}\,p)}(\frac{x}{p})$

$$\sum_{x=1}^{p-1}(\frac{x}{p})$$

由引理 3，$\sum_{x=1}^{p-1}(\frac{x}{p})=0$

因此 $\sum_{x\,(\mathrm{mod}\,p)}(\frac{ax+b}{p})=0$

----------1 分

（2）解析：

引理 4

若$\left(\frac{-1}{p}\right)=1$　则p为$4m+1$型素数

若$\left(\frac{-1}{p}\right)=-1$　则p为$4m+3$型素数

证明：

$p=4m+1$：$(-1)^{\frac{p-1}{2}}=(-1)^{\frac{4m+1-1}{2}}=(-1)^{2m}=1\ (mod\ \ p)$

由欧拉判别法则，-1为模p的二次剩余

$p=4m+3$：$(-1)^{\frac{p-1}{2}}=(-1)^{\frac{4m+2}{2}}=(-1)^{2m+1}=-1\ (mod\ \ p)$

由欧拉判别法则，-1为模p的二次非剩余

----------1 分

引理 5 $\left(\frac{mn}{p}\right)=\left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$

证明：由欧拉判别法则可知

a为模m的二次剩余，则$a^{\frac{p-1}{2}}\equiv 1=\left(\frac{a}{p}\right)\ \ (mod\ \ p)$

a为模m的二次非剩余，则$a^{\frac{p-1}{2}}\equiv -1=\left(\frac{a}{p}\right)\ \ (mod\ \ p)$

则$\left(\frac{mn}{p}\right)=(mn)^{\frac{p-1}{2}}\equiv m^{\frac{p-1}{2}}n^{\frac{p-1}{2}}\left(\frac{m}{p}\right)\left(\frac{n}{p}\right)\ \ (mod\ \ p)$

因为p为奇素数，且$\left|\left(\frac{mn}{p}\right)-\left(\frac{m}{p}\right)\left(\frac{n}{p}\right)\right|\leq 2$

所以，$\left(\frac{mn}{p}\right)=\left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$

----------1 分

回到原问题，由引理 2

$$\left(\frac{f(p-x)}{p}\right)=\left(\frac{f(-x)}{p}\right)$$

因为$f(x)$为奇函数，

$$\left(\frac{f(-x)}{p}\right)=\left(\frac{-f(x)}{p}\right)$$

由引理 5

$$\left(\frac{-f(x)}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{f(x)}{p}\right)$$

由引理 4

$$\left(\frac{f(p-x)}{p}\right)=\begin{cases}\left(\frac{f(x)}{p}\right) & p\text{为 }4m+1\text{ 型素数}\\ -\left(\frac{f(x)}{p}\right) & p\text{为 }4m+3\text{ 型素数}\end{cases}$$

----------1 分

$$\sum_{x=\frac{p+1}{2}}^{p-1}\left(\frac{f(x)}{p}\right)=\sum_{x=1}^{\frac{p-1}{2}}\left(\frac{f(p-x)}{p}\right)$$

则有

$$=\begin{cases}\sum\limits_{x=1}^{\frac{p-1}{2}}\left(\dfrac{f(x)}{p}\right) & p\text{为 }4m+1\text{ 型素数}\\ -\sum\limits_{x=1}^{\frac{p-1}{2}}\left(\dfrac{f(x)}{p}\right) & p\text{为 }4m+3\text{ 型素数}\end{cases}$$

故$\sum\limits_{x=1}^{p-1}\left(\frac{f(x)}{p}\right)=\sum\limits_{x=1}^{\frac{p-1}{2}}\left(\frac{f(x)}{p}\right)+\sum\limits_{x=\frac{p+1}{2}}^{p-1}\left(\frac{f(x)}{p}\right)$

$$=\begin{cases}2\sum\limits_{x=1}^{\frac{p-1}{2}}\left(\dfrac{f(x)}{p}\right) & p\text{为 }4m+1\text{ 型素数}\\ 0 & p\text{为 }4m+3\text{ 型素数}\end{cases}$$

----------1 分

（3）解析：

引理 6　若$(k,p)=1$，则当x遍历p的完全剩余系时，

kx^{p-2}也遍历p的完全剩余系。

证明：由费马小定理，x遍历p的完全剩余系时，

$$x^{p-1}\equiv x^{p-2}\cdot x\equiv 1\ \ (mod\ \ p)$$

则x和x^{p-2}为模p的数论倒数。

已知若a遍历p的完全剩余系，则a的模p数论倒数也遍历。

则x^{p-2}遍历，因为$\gcd(k,p)=1$，则kx^{p-2}也遍历。

----------1 分

引理 7　　若$(k,p)=1$，则$\sum\limits_{x\,(\mathrm{mod}\,p)}(\frac{x(x+k)}{p})=-1$

证明：$\sum\limits_{x\,(\mathrm{mod}\,p)}(\frac{x(x+k)}{p})=\sum\limits_{x=1}^{p-1}(\frac{x^{p-1}\cdot x(x+k)}{p})$

由引理 6　　$=\sum\limits_{x=1}^{p-1}(\frac{x^{p-1}\cdot x^{p-2}(x+k)}{p})$

$$=\sum_{x=1}^{p-1}(\frac{x^{2p-2}+kx^{2p-3}}{p})$$

$$=\sum_{x=1}^{p-1}(\frac{1+kx^{p-2}}{p})$$

$$=\sum_{x=1}^{p-1}(\frac{1+x}{p})$$

$$=\sum_{x=2}^{p}(\frac{x}{p})$$

$$=\sum_{p\,(mod\ p)}(\frac{x}{p})-1=-1$$

----------1 分

引理 8　　当$p \equiv 3\ (mod\ \ 4)$，　$p \geq 3$

$$\left|\{x \in \{1,2 \dots p-1\}: \left(\frac{x}{p}\right) = \left(\frac{x+1}{p}\right) = 1\}\right| = \frac{p-3}{4} > 0$$

证明：构造如下和式

$$\sum_{x=1}^{p-2} \frac{\left(\frac{x}{p}\right)+1}{2} \cdot \frac{\left(\frac{x+1}{p}\right)+1}{2}$$

----------1 分

可以知道

$$\left|\{x \in \{1,2 \dots p-1\}: \left(\frac{x}{p}\right) = \left(\frac{x+1}{p}\right) = 1\}\right|$$

$$= \sum_{x=1}^{p-2} \frac{\left(\frac{x}{p}\right)+1}{2} \cdot \frac{\left(\frac{x+1}{p}\right)+1}{2}$$

$$= \frac{1}{4}\sum_{x=1}^{p-2}[\left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right) + \left(\frac{x}{p}\right) + \left(\frac{x+1}{p}\right) + 1]$$

$$= \frac{1}{4}[\sum_{x=1}^{p-2}\left(\frac{x^2+x}{p}\right) + \sum_{x=1}^{p-2}\left(\frac{x}{p}\right) + \sum_{x=1}^{p-1}\left(\frac{x}{p}\right) + p-2]$$

由引理 7

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

当$x=p-1$时，

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

$$=\left(\frac{0}{p}\right)=0$$

则

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

由引理 3 可知

$$\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)=0$$

则

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

因为$p\equiv 3\ (mod\ \ 4)$时，$\left(\frac{p-1}{p}\right)=\left(\frac{-1}{p}\right)=-1$

则有

$$\sum_{x=1}^{p-2}\left(\frac{x}{p}\right)=-1$$

综上所述

$$\frac{1}{4}[\sum_{x=1}^{p-2}\left(\frac{x^2+x}{p}\right)+\sum_{x=1}^{p-2}\left(\frac{x}{p}\right)+\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)+\ p-2]$$

$$=\frac{1}{4}[-1+1-1+p-2]$$

$$=\frac{p-3}{4}>0$$

----------1 分

回到原问题：

$$\left|\{y\in\{1,2\dots p-2\}:-\left(\frac{y}{p}\right)=\left(\frac{y+1}{p}\right)=1\}\right|$$

$$=\left|\{y\in\{1,2\dots p-2\}:\left(\frac{y+1}{p}\right)=1\}\right|-\frac{p-3}{4}$$

$$=\frac{p-1}{2}-1-\frac{p-3}{4}$$

$$=\frac{p-3}{4}>0$$

且

$$\left|\{z \in \{1,2 \dots p-2\}: \left(\frac{z}{p}\right) = -\left(\frac{z+1}{p}\right) = 1\}\right|$$

$$= \left|\{z \in \{1,2 \dots p-2\}: \left(\frac{z}{p}\right) = 1\}\right| - \frac{p-3}{4}$$

$$= \frac{p-1}{2} - \frac{p-3}{4}$$

$$= \frac{p+1}{4} > 0$$

所以这样的x, y, z均存在。

----------1 分

（4）解析：

引理 9 $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ p为奇素数

证明：给定k，对$2k$作$mod\ p$的带余数除法

$$2k = pq_k + r_k$$

$$0 \le r_k < p-1 \qquad 其中q_k = [\frac{2k}{p}]$$

对k从 1 到$\frac{p-2}{2}$求和：

$$\sum_{k=1}^{\frac{p-2}{2}} 2k = \sum_{k=1}^{\frac{p-2}{2}} pq_k + \sum_{k=1}^{\frac{p-2}{2}} r_k$$

因为$k \leq \frac{p-1}{2}$

$$q_k = \left[\frac{2k}{p}\right] < \left[\frac{2 \cdot \frac{p}{2}}{p}\right] = 1$$

$$q_k = 0$$

因此

$$\sum_{k=1}^{\frac{p-2}{2}} 2k = \sum_{k=1}^{\frac{p-2}{2}} r_k$$

$$= 2 \cdot \frac{p^2 - 1}{8}$$

$$= \sum_{\{2k\}_p < \frac{p}{2}} \sum_{1 \leq k < \frac{p}{2}} r_k + \sum_{\{2k\}_p > \frac{p}{2}} \sum_{1 \leq k < \frac{p}{2}} r_k$$

$$= \sum_{\{2k\}_p < \frac{p}{2}} \sum_{1 \leq k < \frac{p}{2}} r_k + \left(\sum_{\{2k\}_p > \frac{p}{2}} \sum_{1 \leq k < \frac{p}{2}} (p - r_k) \right)$$

$$+2 \sum_{\{2k\}_p > \frac{p}{2}} \sum_{1 \leq k < \frac{p}{2}} r_k - \sum_{\{2k\}_p > \frac{p}{2}} \sum_{1 \leq k < \frac{p}{2}} p$$

因为

$$\sum_{\{2k\}_p<\frac{p}{2}\ 1\le k<\frac{p}{2}} r_k + \sum_{\{2k\}_p>\frac{p}{2}\ 1\le k<\frac{p}{2}} (p-r_k)$$

$$= \sum_{1\le k<\frac{p}{2}} 1 = \frac{p^2-1}{8}$$

所以

$$\frac{p^2-1}{8} = 2\sum_{\{2k\}_p>\frac{p}{2}\ 1\le k<\frac{p}{2}} r_k - \sum_{\{2k\}_p>\frac{p}{2}\ 1\le k<\frac{p}{2}} p$$

故

$$(-1)^{\frac{p^2-1}{8}} = (-1)^{\sum_{\{2k\}_p>\frac{p}{2}\ 1\le k<\frac{p}{2}} p}$$

$$= (-1)^{\sum_{\{2k\}_p>\frac{p}{2}\ 1\le k<\frac{p}{2}} 1}$$

$$= (-1)^{\left|\{1\le k<\frac{p}{2}:\{2x\}_p>\frac{p}{2}\}\right|}$$

----------2 分

由高斯引理

$$(-1)^{\frac{p^2-1}{8}} = \left(\frac{2}{p}\right)$$

回到原问题,

对于$\forall k=1,2\ldots\frac{p-1}{2}$，不难发现

$$\left[\frac{kx}{p}\right]-\left[\frac{k(x-1)}{p}\right]=\begin{cases}0 & \text{如果}\{kx\}_p>k\\ 1 & \text{如果}\{kx\}_p<k\end{cases}$$

因此

$$\left|\{1\le k<\frac{p}{2}:\{kx\}_p>k\}\right|$$

$$=\frac{p-1}{2}-\sum_{k=1}^{\frac{p-1}{2}}([\frac{kx}{p}]-\left[\frac{k(x-1)}{p}\right])$$

----------1 分

由高斯引理

$$\left(\frac{x}{p}\right)=(-1)^{\left|\{1\le k<\frac{p}{2}:\{kx\}_p>\frac{p}{2}\}\right|}$$

可得

$$\left(\frac{-1}{p}\right)=(-1)^{\left|\{1\le k<\frac{p}{2}:\{-x\}_p>\frac{p}{2}\}\right|}$$

$$=(-1)^{\frac{p-1}{2}}$$

则

$$(-1)^{\left|\{1\le k<\frac{p}{2}:\{kx\}_p>k\}\right|}\cdot\left(\frac{-1}{p}\right)$$

$$=(-1)^{\frac{p-1}{2}-\sum\limits_{k=1}^{\frac{p-1}{2}}([\frac{kx}{p}]-\left[\frac{k(x-1)}{p}\right]}\cdot\left(\frac{-1}{p}\right)$$

$$=(-1)^{\frac{p-1}{2}-\sum\limits_{k=1}^{\frac{p-1}{2}}([\frac{kx}{p}]-\left[\frac{k(x-1)}{p}\right])}\cdot(-1)^{\frac{p-1}{2}}$$

$$=(-1)^{\frac{p-1}{2}-\sum\limits_{k=1}^{\frac{p-1}{2}}[\frac{kx}{p}]+\sum\limits_{k=1}^{\frac{p-1}{2}}\left[\frac{k(x-1)}{p}\right]}\cdot(-1)^{\frac{p-1}{2}}$$

$$=(-1)^{(p-1)-\sum\limits_{k=1}^{\frac{p-1}{2}}[\frac{kx}{p}]+\sum\limits_{k=1}^{\frac{p-1}{2}}\left[\frac{k(x-1)}{p}\right]}$$

$$=(-1)^{\sum\limits_{k=1}^{\frac{p-1}{2}}[\frac{kx}{p}]+\sum\limits_{k=1}^{\frac{p-1}{2}}\left[\frac{k(x-1)}{p}\right]}$$

$$=(-1)^{\sum\limits_{k=1}^{\frac{p-1}{2}}\frac{kx-\{kx\}_p}{p}+\sum\limits_{k=1}^{\frac{p-1}{2}}\frac{k(x-1)-\{k(x-1)\}_p}{p}}$$

$$=(-1)^{\sum\limits_{k=1}^{\frac{p-1}{2}}(2x-1)k\cdot\frac{1}{p}-\sum\limits_{k=1}^{\frac{p-1}{2}}\frac{\{kx\}_p}{p}-\sum\limits_{k=1}^{\frac{p-1}{2}}\frac{\{k(x-1)\}_p}{p}}$$

$$=(-1)^{\sum\limits_{k=1}^{\frac{p-1}{2}}(2x-1)k}\cdot(-1)^{\sum\limits_{k=1}^{\frac{p-1}{2}}\{kx\}_p+\sum\limits_{k=1}^{\frac{p-1}{2}}\{k(x-1)\}_p}$$

$$=(-1)^{\sum\limits_{k=1}^{\frac{p-1}{2}}k}\cdot(-1)^{\sum\limits_{k=1}^{\frac{p-1}{2}}\{kx\}_p+\sum\limits_{k=1}^{\frac{p-1}{2}}\{k(x-1)\}_p}$$

$$=(-1)^{\frac{p^2-1}{8}}\cdot(-1)^{\sum\limits_{k=1}^{\frac{p-1}{2}}\{kx\}_p+\sum\limits_{k=1}^{\frac{p-1}{2}}\{k(x-1)\}_p}$$

$$=(-1)^{\frac{p^2-1}{8}}\cdot(-1)^{\sum\limits_{k=1}^{\frac{p-1}{2}}(\{kx\}_p+\{k(x-1)\}_p)}$$

----------1 分

因为p为奇素数

$$\{kx\}_p \equiv 1 + p - \{kx\}_p \ (mod\ \ 2)$$

$$\sum_{k=1}^{\frac{p-1}{2}} \{kx\}_p \equiv \sum_{\{kx\}_p < \frac{p}{2}} \sum_{k=1}^{\frac{p-1}{2}} \{kx\}_p + \sum_{\{kx\}_p > \frac{p}{2}} \sum_{k=1}^{\frac{p-1}{2}} (1 + p - \{kx\}_p)$$

$$= \sum_{\{kx\}_p > \frac{p}{2}} \sum_{k=1}^{\frac{p-1}{2}} 1 + \sum_{r=1}^{\frac{p-1}{2}} r$$

$$= \left|\{1 \le k < \frac{p}{2} : \{kx\}_p > \frac{p}{2}\}\right| + \frac{p^2 - 1}{8} \ (mod\ \ 2)$$

所以

由引理 9 和高斯引理

$$(-1)^{\sum_{k=1}^{\frac{p-1}{2}} \{kx\}_p} = \left(\frac{x}{p}\right)\left(\frac{2}{p}\right) = (\frac{2x}{p})$$

相似地，我们可以得到

$$(-1)^{\sum_{k=1}^{\frac{p-1}{2}} \{k(x-1)\}_p} = \left(\frac{x-1}{p}\right)\left(\frac{2}{p}\right) = (\frac{2(x-1)}{p})$$

根据之前的结果

$$(-1)^{\left|\{1\le k<\frac{p}{2}:\{kx\}_p>k\}\right|}\cdot\left(\frac{-1}{p}\right)$$

$$=(-1)^{\frac{p^2-1}{8}}\cdot(-1)^{\sum\limits_{k=1}^{\frac{p-1}{2}}(\{kx\}_p+\{k(x-1)\}_p)}$$

可以得到

$$(-1)^{\left|\{1\le k<\frac{p}{2}:\{kx\}_p>k\}\right|}\cdot(\frac{-1}{p})$$

$$=(-1)^{\frac{p^2-1}{8}}\cdot(\frac{2x}{p})(\frac{2(x-1)}{p})$$

$$=(\frac{2x(x-1)}{p})$$

则

$$(-1)^{\left|\{1\le k<\frac{p}{2}:\{kx\}_p>k\}\right|}$$

$$=\frac{(\frac{2x(x-1)}{p})}{(\frac{-1}{p})}$$

$$=(\frac{2x(1-x)}{p})$$

----------2 分

证毕.

第四部分【组合】

1. 填空题

[A] 你参加了俄罗斯转盘赌. 庄家在弹夹中的三个随机弹位里塞了子弹，你身旁的倒霉蛋连续开了两枪，第一枪没有射出子弹，第二枪送他上了西天. 接着手枪递到了你的手上，你_____［填“应该”/“不应该”］旋转弹仓（至一个随机弹位）后再开枪，此时你的存活概率为_____.（下图是使用的手枪——柯尔特蟒蛇，一击必杀，内含 6 个弹位，每次开枪后弹仓会逆时针旋转一个弹位）

答案：“应该”，$\frac{2}{3}$

解析：

如果转弹仓，那么弹仓里还有 2 颗子弹，又因为一共有 6 个弹位，因此存活概率一定是 $\frac{2}{3}$.

让我们分类讨论来计算不转弹舱的存活概率：

不妨设六个弹位逆时针排列依次分别为 1 号位，2 号位，3 号位，4 号位，5 号位和 6 号位。

首先讨论三颗子弹的位置情况（假设每个弹位的位数都加一算作同种情况，特别的，6 号弹位加 1 为 1 号弹位）

第 1 种，如果三颗子弹全部相邻：

不妨设三颗子弹在 1 号位，2 号位和 3 号位，那么倒霉蛋的第一枪必定在 6 号位，第二枪在 1 号位。那么，如果转弹仓，存活概率为 0%

第 2 种，如果三颗子弹分别在 1 号位，2 号位，4 号位，则易得存活概率为 50%

第 3 种，如果三颗子弹分别在 1 号位，2 号位，5 号位，则易得存活概率为 50%

第 4 种，如果三颗子弹分别在 1 号位，3 号位，5 号位，则易得存活概率为 100%

其余所有情况均与上述四种情况重合，

因此不转弹仓后的存活概率为 50%

综上所述，你应该转弹舱后再开枪，此时你的存活概率为 $\frac{2}{3}$

2. 简答题

在 100×100 的网格中，每行每列都有 3 个红色方格，即共有 300 个红色方格. 对于 $k\in\mathbb{N}^+$，我们总是可以删去 k 个红色方格后，使得任意 2×2 的网格内不全是红色方格，求 $k_{\min}$.

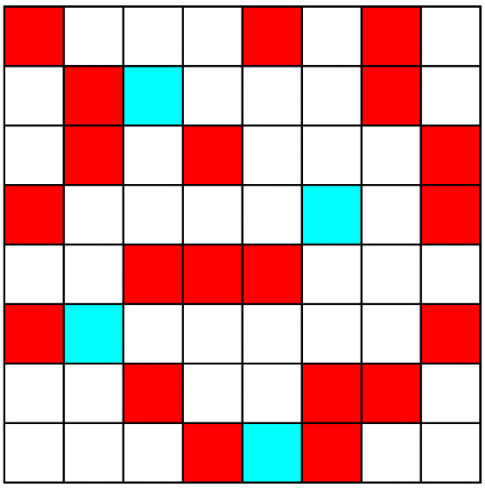
解析：

首先证明 $k=50$ 时能够使条件成立，再证明 $k=50$ 是最小值。

我们假设删去的红色方格为淡蓝色方格。

设从上到下依次为第 1 行，第 2 行…第 100 行。

我们删去偶数行的第二个红色方格，则可以确保任意 2×2 的网格内不全是红色方格，如下图所示：（删去奇数行同理）

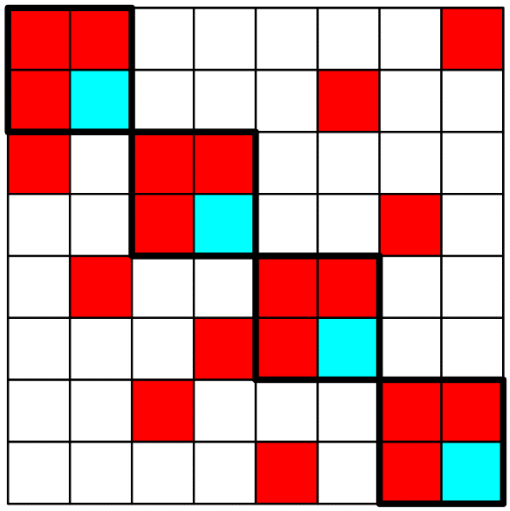


这是因为，每一个 2×2 的网格必定包含两个相邻的偶数行方格。

如果删去偶数行的第二个方格，则必定能确保不存在两个相邻的偶数行红色方格。

接下来证明 $k=50$ 是最小值：

由于有 300 个红色方格，考虑如下构造：



显然可以出现 50 个 2×2 的网格全部为红色方格，且 50 个为最大值。

因此如果 $k<50$，则不能确保任意 2×2 的网格内不全是红色方格

综上所述，最小值为 50.

3. 主题探究题

鸽笼原理是指，若$a_i \in R$，$m = \sum_{i=1}^{n} a_i$，则$\exists j,\ a_j \geq \frac{m}{n}$.

（**1**）设 A 是 Z_n 的子集，$Z_n = \{0, 1, 2 \ldots n-1\}$，且$|A| \leq \frac{\ln n}{1.7}$，求证：$\exists\, r \neq 0,\ r \in \mathbb{Z}$，

使得$\left|\sum_{S \in A} e^{\frac{2\pi i}{n} sr}\right| \geq \frac{|A|}{2}$.（4 分）

（**2**）设$1 \leq m < n, m, n \in Z,\quad a_{ij} \in \mathbb{N}$，其中$1 \leq i \leq n,\ 1 \leq j \leq m$，记 $A_j = \sum_{i=1}^{n} \left|a_{ij}\right|$，

且 $\forall\, 1 \leq j \leq m$，$A_j \neq 0$，求证：存在不全为零的整数$x_i\,(1 \leq i \leq n)$，且

$|x_i| \leq \prod_{i=1}^{m} A_j^{\frac{1}{n-m}}$，有 $\sum_{i=1}^{n} a_{ij} x_i = 0$.（5 分）

（**3**）求证：存在一个 $c > 0$，使得对于$\forall n \in N^+$，$\exists\, A \subseteq \{1, 2, 3 \ldots n\}$. $|A| \geq n e^{-c\sqrt{\ln N}}$，

且 A 中无三项成等差数列.（5 分）

（**4**） 对于 $n \geq 2$，设 A_n 是所有系数属于$\{-1, 0, 1\}$的 n 次多项式的因子集合，设

$C(n)$ 为属于 A_n 的整系数多项式的最大系数. 求证：对$\forall \varepsilon > 0$，$\exists\, k \in N^+$，

使得对所有$n > k$，有$2^{n^{\frac{1}{2}-\varepsilon}} < C(n) < 2^n$.（6 分）

（**1**）设 A 是 Z_n 的子集，$Z_n=\{0,1,2\ldots n-1\}$，且$|A|\le\frac{\ln n}{1.7}$，求证：$\exists\, r\ne 0,\ r\in\mathbb{Z}$，使得$\left|\sum\limits_{S\in A}e^{\frac{2\pi i}{n}sr}\right|\ge\frac{|A|}{2}$.（4 分）

解析：

设 $A=\{a_1,a_2,...,a_n\}$，定义 $g(t)=(e^{\frac{2i\pi}{n}a_1t},e^{\frac{2i\pi}{n}a_2t},...,e^{\frac{2i\pi}{n}a_nt})$，$0\le t\le n-1$，

将单位圆周分为 6 段相等的弧，那么这些 k 元组被分成 6^k 个等价类。

由于 $k\le\dfrac{\ln n}{1.7}$，故 $n>6^k$，则 $\exists t_1<t_2$，使 $g(t_1)$ 与 $g(t_2)$ 在同一个等价类，

若 $r=t_2-t_1$，则 $\mathrm{Re}(e^{\frac{2i\pi}{n}ra_j})=\cos(\dfrac{2a_j(t_2-t_1)\pi}{n})\ge\cos(\dfrac{\pi}{3})$

故 $|f(r)|\ge\mathrm{Re}|f(r)|\ge\dfrac{|A|}{2}$

（**2**）设$1\le m<n,m,n\in Z,\quad a_{ij}\in\mathbb{N}$，其中$1\le i\le n,\ 1\le j\le m$，记 $A_j=\sum\limits_{i=1}^{n}|a_{ij}|$，且 $\forall\,1\le j\le m$，$A_j\ne 0$，求证：存在不全为零的整数$x_i\,(1\le i\le n)$，且$|x_i|\le\prod\limits_{i=1}^{m}A_j^{\frac{1}{n-m}}$，有 $\sum\limits_{i=1}^{n}a_{ij}x_i=0$.（5 分）

解析：

记 $f(x_1,x_2,...,x_n)=(\sum\limits_{i=1}^{n}a_{i1}x_i,\sum\limits_{i=1}^{n}a_{i2}x_i,...,\sum\limits_{i=1}^{n}a_{im}x_i)$

显然对于 $\forall x_i\in[0,m],x_i\in\mathbb{N}$，设 $a_1\ge a_2\ge...\ge a_p\ge 0\ge a_{p+1}\ge...\ge a_n$

有：$[M](a_{p+1}+...+a_n)\le\sum\limits_{i=1}^{n}a_ix_i\le(a_1+...+a_p)[M]$

故 $\sum\limits_{i=1}^{n}a_ix_i$ 至多取 $[M](\sum\limits_{i=1}^{n}|a_i|)+1$ 个值.

故 f 的像至多 $\prod_{i=1}^{m}(1+[M]A_i)\le A_1A_2...A_m(1+[M])^m$

故取 $|M|=(A_1A_2..A_m)^{\frac{1}{n-m}}$ 知 $\exists f(x)=f(y)$

即可取 $v=x-y$，满足条件.

（3）求证：存在一个 $c>0$，使得对于 $\forall n\in N^+$，$\exists A\subseteq\{1,2,3\ldots n\}.\ |A|\ge ne^{-c\sqrt{\ln N}}$，

且 A 中无三项成等差数列.（5 分）

解析：

定义 $F(n,M,r)=\{x\mid x=(x_1,x_2,...,x_n),x_i\in\{1,2,...,M\},\sum_{i=1}^{n}x_i^2=r\}$

由抽屉原理，$\exists\sqrt{n}\le r\le M\sqrt{n}$，令 $|F(n,M,r)|\ge\frac{M^n}{n(M^2-1)}\ge\frac{M^{n-2}}{n}$ 个元素.

记 $f:F(n,M,r)\to\{1,2,...,N\}$，其中 $f(x_1,x_2,...,x_n)=\sum_{i=1}^{n}(2M)^{i-1}x_i$

若向量 x,y,z 的像 $f(x),f(y),f(z)$ 成等差.

则 $\sum_{i=1}^{n}(x_i+y_i-2z_i)(2M)^{i-1}=0\Longrightarrow x_i+y_i=2z_i$

而 x,y,z 同属 $F(n,M,r)$ 在 R^n 上为球面.

故 $x=y=z$，故 $|f(x_1,x_2,...,x_n)|\le M\cdot\frac{(2M)^n-1}{2M-1}\le(2M)^n$

故考虑 $M=[\frac{N^n}{2}]$，则 $f(F(n,M,r))\subseteq\{1,2,...,N\}$，且 $f(F(n,M,r))$ 无等差数列.

且 $\frac{M^{n-2}}{n}>\frac{N^{\frac{n-2}{n}}}{4^{n-2}n}$，取 $n=[\sqrt{\ln N}]$ 知 $f(F(n,M,r))$ 至少有 $Ne^{-c\sqrt{\ln N}}$ 个元素.

（**4**）对于 $n \geq 2$，设 A_n 是所有系数属于$\{-1, 0, 1\}$的 n 次多项式的因子集合，设 $C(n)$ 为属于 A_n 的整系数多项式的最大系数. 求证：对$\forall \varepsilon > 0$，$\exists\, k \in N^+$，使得对所有$n > k$，有$2^{n^{\frac{1}{2}-\varepsilon}} < C(n) < 2^n$.（6 分）

解析：

先证$C(n) > 2^{n^{\frac{1}{2}-\varepsilon}}$，

对于$\deg f \leq n$的多项式 f， $a_i = 0$ 或 1

记$\varphi(f) = (f(1), f'(1), \ldots, f^{N-1}(1))$， $f^{(j)} \leq (n+1)^{j+1}$

故φ的像至多$(1+n)^{1+2+\ldots+N} \leq (1+n)^{N^2}$

另一方面， f 的原像共2^{n+1}个，故$2^{n+1} > (1+n)^{N^2}$

由抽屉原理，存在 f, g 的的像$\varphi(f), \varphi(g)$相同，

且$(f-g)_k = -1$或 0 或 1，且$(x-1)^N \mid f-g$.

由于$(x-1)^N$ 中最大系数为C_{2N}^N且$C_{2N}^N > \dfrac{4^N}{2N+1} > 2^N$

故$C(n) > C_{2n}^n$.

取$N = [\sqrt{\dfrac{n}{\log_2(n+1)}}]$即有$(1+n)^{N^2} < 2^{N+1}$，

于是$N > n^{\frac{1}{2}-\varepsilon}$.

再证 $C(n)<2^n$，对 $f(x)=\sum_{k=0}^{n}a_kx^k, a_k\in\mathbb{R}$

定义 f 的 *Mahler* 度量 $M(f)=|a_n|\prod_{k=1}^{n}\max(1,|x_i|)$，其中 x_i 为 f 的根.

Landau 不等式：$M(f)\le\sqrt{a_0^2+a_1^2+...+a_n^2}$

证明：设 $z_1\sim z_n$ 为单位根，则 $|\sum_{j=1}^{N}f(z_j)|^2=\sum_{j=1}^{N}(\sum_{i=0}^{n}a_iz_j^i)(\sum_{i=0}^{n}a_iz_j^{-i})=N\sum_{i=0}^{n}a_i^2$

由 $AM-GM$ 即得 $\sum_{i=0}^{n}a_i^2\ge\sqrt{|f(z_1)f(z_2)...f(z_n)|^2}$

而 $(x-z_1)(x-z_2)...(x-z_N)=x^N-1$

故 $|f(z_1)f(z_2)...f(z_n)|=|a_n|^N|1-x_1^N||1-x_2^N|...|1-x_n^N|$

$\Rightarrow\sqrt{\sum_{i=0}^{n}a_i^2}\ge|a_n|\prod_{i=1}^{n}\sqrt[N]{|1-x^N|}$，而 $\lim_{n\to\infty}\sqrt[n]{|1-z^n|}=\max(1,|z_n|)$

$\Rightarrow M(f)\le\sqrt{\sum_{i=0}^{n}a_i^2}$

Landau 不等式告诉我们，对于 f，$<f>_k=0$ 或-1 或 1，$M(f)\le\sqrt{n+1}$

设 g 为这样的多项式，$g(x)=f(x)p(x)$

则 $M(g)=M(f)M(p)\ge M(f)\Rightarrow M(f)\le\sqrt{n+1}$

于是对于 $\forall x_i$ 为 f 根，$|x_{i1}x_{i2}...x_{i\varepsilon}|\le M(f)$

$\Rightarrow C_n^{[\frac{n}{2}]}M(f)\le\sqrt{n+1}$，$C_n^{[\frac{n}{2}]}<2^n$.

$\Rightarrow C(n)<2^n$

题目来源 & 命题人员

（纯原创题分值占比为 86%，所有题目来源均可查证）

带下划线的题号为非原创题，已进行改编

第一部分【几何】

1. 填空题 Prushka（风吻流光）原创题

2. 简答题 改编题

3. 主题探究题 芒 原创题

第二部分【代数】

1. 填空题 HMMT – 2024 年 February – Algebra and Number Theory – 第 9 题

2. 简答题 **黄教授 原创题**

3. 主题探究题 **（1）~（3）**Beez ~喵 原创题 **（4）**Beez ~喵 改编自某论文

第三部分【数论】

1. 填空题 AIME 改编题

2. 简答题 **A5（修）** 原创题

3. 主题探究题 黄教授 原创题

第四部分【组合】

1. 填空题 Prushka（风吻流光）原创题

2. 简答题 JHMT 改编题

3. 主题探究题 Beez ~喵 原创题

鸣谢

试题卷文档/解析文档制作

Prushka（风吻流光），A5

命题人员

Prushka（风吻流光），beez ~喵，黄教授（小黄），芒，A5

审核人员

李明，beez ~喵，黄教授（小黄），Prushka（风吻流光）

顾问

黄教授（小黄），愚集，beez ~喵

后台工作人员

Hatsune

默默供题的竞赛（均为国外竞赛）

AIME，HMMT，JHMT