2022 年秋季《离散数学》期中试卷

2022 年 11 月 5 日 $14:00-16:00$

本试卷共六道题, 分两页, 其中第 1, 6 题 $5+5+10$ 分, 第 2 题 10 分, 第 3 题 $5+10+5$ 分, 第 4 题 $5+5+5$ 分, 第 5 题 $5+10$ 分. 可利用前面小问的结论处理后面的小问.

1 (1) 设映射 $f:\{1,2,\ldots,100\}\to\{1,2,\ldots,50\}$ 是满射, 且满足 $f(1)\le f(2)\le\cdots\le f(100)$. 求满足上述条件的映射 f 的个数, 将结果用组合数表示即可.

(2) 将 $3\times n$ 方格纸 (共 3 行共 n 列的方格纸) 剖分成若干个 1×3 或 3×1 小条的并, 设方法总数为 a_n. 求 a_n 满足的递推关系式, 并说明理由.

(3) 一颗质地均匀的正方体骰子, 六个面上分别标有点数 $1,2,3,4,5,6$. 随机地掷该骰子三次 (各次掷骰子的结果互不影响), 将三次掷得的点数依次为 a_1,a_2,a_3, 求事件 $|a_1-a_2|+|a_2-a_3|+|a_3-a_1|=6$ 发生的概率.

解. (1) 设 $|f^{-1}(\{i\})|=n_i$, 则 $n_1,\ldots,n_{50}$ 都是正整数, 满足 $n_1+\cdots+n_{50}=100$. 条件表明 f 由有序组 $(n_1,\ldots,n_{50})$ 唯一确定, 有

$$f(x)=i \iff n_1+\cdots+n_{i-1}+1\le x\le n_1+\cdots+n_i.$$

讲义上我们证明了满足方程 $n_1+\cdots+n_{50}=100$ 的有序正整数解的数目为 C_{99}^{49}, 这也是所求 f 的数目.

(2) 考虑包含左上角小方格的小条, 有两种可能: 3×1 或 1×3. 若是前一种情形, 还需将除了第一列之外的 $3\times(n-1)$ 方格纸剖分, 方法数目为 a_{n-1}. 若是后一种情形, 则它下方必须是两个 1×3 的小条, 除此之外需将除了前 3 列之外的 $3\times(n-3)$ 方格纸剖分, 方法数目为 a_{n-3}.

利用加法原理可得 $a_n=a_{n-1}+a_{n-3}$.

(3) 所求概率为 $\frac{1}{4}$.

先确定 $|a_1-a_2|+|a_2-a_3|+|a_3-a_1|=6$ 的解. 若 a_1,a_2,a_3 中有两个相同, 则相同这两个与第三个的差为 3, 可得 $\{a_1,a_2,a_3\}=\{x,x,x+3\}$或$\{x,x+3,x+3\}$, 其中 $1\leq x\leq 3$. 计及排序, 这类 (a_1,a_2,a_3) 的数目为 $3\times 2\times C_3^1=18$.

若 a_1,a_2,a_3 两两不同, 设排序为 $a<b<c$, 则 $2(c-a)=6$, 可得 $\{a_1,a_2,a_3\}=\{a,a+1,a+3\}$或$\{a,a+2,a+3\}$, 其中 $a\leq 3$. 计及排序, 这类 (a_1,a_2,a_3) 的数目为 $3\times 2\times 3!=36$.

结合这两类, 满足条件的 (a_1,a_2,a_3) 的总数为 $18+36=54$, 由此可得所求的概率为 $\frac{54}{6^3}=\frac{1}{4}$.

□

2 给定正整数 m 以及整数 a,b,c,d, 满足 $ad-bc\equiv 1 \pmod m$. 求解如下线性同余方程组:

$$\begin{cases} ax+by\equiv 1 \pmod m \\ cx+dy\equiv 2 \pmod m. \end{cases}$$

解. 第一个方程乘以 d 减去第二个方程乘以 b, 得到

$$(ad-bc)x\equiv d-2b \pmod m,$$

利用条件 $ad-bc\equiv 1 \pmod m$ 可知上式为 $x\equiv d-2b \pmod m$.

第二个方程乘以 a 减去第一个方程乘以 c, 得到

$$(ad-bc)y\equiv 2a-c \pmod m,$$

得到 $y\equiv 2a-c \pmod m$.

最后易验证 $\begin{cases} x\equiv d-2b \pmod m \\ y\equiv 2a-c \pmod m \end{cases}$ 是原同余方程组的解. □

3 (1) 叙述容斥原理.

(2) 给定正整数 n, 设其素因子分解式为 $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, 其中 $p_1, \dots, p_k$ 是不同的素数, $\alpha_1, \dots, \alpha_k$ 是正整数. 对正整数 m, 定义 $f(m)$ 为 $1, 2, \dots, m$ 中与 n 互素的数的个数, 即

$$f(m) = \#\{x \in \mathbb{Z} | 1 \le x \le m 且 \gcd(x, n) = 1\}.$$

利用容斥原理计算 $f(m)$, 请用 m 与 $p_1, \dots, p_k$ 表示.

(3) 利用 (2) 的计算结果, 结合不等式 $y - 1 < [y] \le y$(其中 $[y]$ 表示不超过 y 的最大整数), 请证明如下不等式:

$$f(m) < m(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k}) + 2^{k-1}.$$

解. (1) 容斥原理为: 设 $A_1, \dots, A_n$ 是有限集合, 则有

$$|A_1 \cup \cdots \cup A_n| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \cdots + (-1)^{n-1} |A_1 \cap \cdots \cap A_n|.$$

(2) 令 $A_i = \{x \in \mathbb{Z} | 1 \le x \le m, p_i \mid x\}$, 则对 $i_1 < \ldots < i_r$, 有

$$A_{i_1} \cap \cdots \cap A_{i_l} = \{x \le m : p_{i_1} \cdots p_{i_l} \mid x\} = \{x = p_{i_1} \cdots p_{i_l} y | y \in \mathbb{Z}_+, y \le [\frac{m}{p_{i_1} \cdots p_{i_l}}]\},$$

可得 $|A_{i_1} \cap \cdots \cap A_{i_l}| = [\frac{m}{p_{i_1} \cdots p_{i_l}}]$. 这样, 利用容斥原理可得

$$\begin{aligned}
f(m) &= |(A_1 \cup \cdots \cup A_k)^c| \\
&= m - |A_1 \cup \cdots \cup A_k| \\
&= m - \sum_{l=1}^{k} (-1)^{l-1} \sum_{i_1 < \ldots < i_r} |A_{i_1} \cap \cdots \cap A_{i_l}| \\
&= m + \sum_{l=1}^{k} (-1)^{l} \sum_{i_1 < \ldots < i_r} [\frac{m}{p_{i_1} \cdots p_{i_l}}] \\
&= \sum_{l=0}^{k} (-1)^{l} \sum_{i_1 < \ldots < i_r} [\frac{m}{p_{i_1} \cdots p_{i_l}}].
\end{aligned}$$

(3) 利用 (2) 的结果以及提示中的不等式, 可得

$$
\begin{aligned}
f(m) &= \sum_{l\text{是偶数}} \sum_{i_1<\ldots<i_r} [\frac{m}{p_{i_1}\cdots p_{i_l}}] - \sum_{l\text{是奇数}} \sum_{i_1<\ldots<i_r} [\frac{m}{p_{i_1}\cdots p_{i_l}}] \\
&< \sum_{l\text{是偶数}} \sum_{i_1<\ldots<i_r} \frac{m}{p_{i_1}\cdots p_{i_l}} - \sum_{l\text{是奇数}} \sum_{i_1<\ldots<i_r} (\frac{m}{p_{i_1}\cdots p_{i_l}} - 1) \\
&= \sum_{l} (-1)^l \sum_{i_1<\ldots<i_r} \frac{m}{p_{i_1}\cdots p_{i_l}} + C_k^1 + C_k^3 + \cdots \\
&= m(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_k}) + 2^{k-1}.
\end{aligned}
$$

□

4 (1) 给定正整数 a, m. 证明: a 模 m 的倒数存在的充分必要条件是 a 与 m 互素. 换句话说, 即同余方程 $ax \equiv 1 \pmod m$ 有解的充分必要条件是 a 与 m 互素.

(2) 叙述并证明 Euler 定理.

(3) 设 p, q 是不同的素数, $N = pq$. 设 $d, e \in \{1, 2, \ldots, \varphi(N)\}$ 满足 $de \equiv 1 \pmod{\varphi(N)}$. 利用 Euler 定理证明: 对不超过 N 的非负整数 u, 令 v 为 u^e 除以 N 所得的余数, 则有

$$u \equiv v^d \pmod N.$$

证明: (1) 一方面, 若存在 x 使得 $ax \equiv 1 \pmod m$, 令 $d = (a, m)$, 则有 $ax \equiv 1 \pmod d$, 即 $d \mid ax + 1$, 结合 $d \mid a$ 可得 $d \mid 1$, 因而有 $d = 1$, 即 a 与 m 互素. 另一方面, 若 $(a, m) = 1$, 考虑 $F : \{0, 1, \ldots, m-1\} \to \{0, 1, \ldots, m-1\}$, $F(x) = ax \pmod m$, 其中 $ax \pmod m$ 表示 ax 除以 m 所得的余数. 若有 $x, y \in \{0, 1, \ldots, m-1\}$ 满足 $F(x) = F(y)$, 则有 $m \mid a(x-y)$, 由 a, m 互素可得 $m \mid x - y$. 由于 $x - y \in [-(m-1), (m-1)]$, 该区间中 m 只有 0 一个倍数, 可得 $x = y$. 这就证明了 F 是单射, 进而也是满射. 特别的, 存在 x 使得 $F(x) = 1$, 即 $ax \equiv 1 \pmod m$.

(2)Euler 定理为: 设 m 是正整数, 则对与 m 互素的整数 a, 有

$$a^{\varphi(m)} \equiv 1 \pmod m.$$

证明如下. 令 $C = \{1 \le x \le m | (x, m) = 1\}$, 则对 $x \in C$, 有 $F(x) = ax (\bmod\ m)$ 与 m 互素, 即 F 将 C 的元素映射到 C 中. 由 (1) 的证明可知 F 诱导 A 到 A 的双射, 换

句话说即 $\{F(x)|x\in C\}$ 是 C 的一个排列, 由此可得

$$\prod_{x\in C}(ax)\equiv\prod_{x\in C}F(x)=\prod_{x\in C}x\pmod m,$$

两边同消去与 m 互素的项 $\prod_{x\in C}x$, 即得到 $a^{|C|}\equiv 1\pmod m$.

(3) 设 $de=1+k\varphi(N)=1+k(p-1)(q-1)$. 当 $u=0,N$ 时所述命题显然成立, 以下假设 $0<u<N$.

当 u 与 N 互素时, 利用 Euler 定理可得 $u^{\varphi(N)}\equiv 1\pmod N$. 由此可得

$$v^d\equiv u^{de}=u^{1+k\varphi(N)}=u\cdot(u^{\varphi(N)})^k\equiv u\pmod N.$$

当 u 与 N 不互素时, 由 $0<u<N$ 可知 u 被 p,q 之一整除, 不妨设 $p\mid u, q\nmid u$. 由条件可知

$$v^d\equiv u^{de}=u^{1+k(p-1)(q-1)}\pmod{pq}.$$

结合 Euler 定理可得

$$v^d\equiv u\cdot(u^{q-1})^{k(p-1)}\equiv u\cdot 1\equiv u\pmod q.$$

由 $p\mid u$ 可知

$$v^d\equiv u^{1+k(p-1)(q-1)}\equiv 0\equiv u\pmod p.$$

设 v^d 模 pa 的余数为 r, 利用第 5 题中的映射 $F:\{0,1,\dots,pq-1\}\to\{0,1,\dots,p-1\}\times\{0,1,\dots,q-1\}$ 可知 $F(r)=F(u)$. 用第 5 题 (1) 的结论可得 $r=u$, 即有 $v^d\equiv u\pmod{pq}$. □

5 给定正整数 m,n, 定义映射 $F:\{0,1,\dots,mn-1\}\to\{0,1,\dots,m-1\}\times\{0,1,\dots,n-1\}$ 为: 若 a 除以 m 的余数为 b, a 除以 n 的余数为 c, 则定义 $F(a)=(b,c)$.

(1) 证明: 若 m 与 n 互素, 则上述定义的 F 是双射.

(2) 当 m 与 n 的最大公因子为 d 时, 求上述定义的 F 的像集的元素个数.

解. (1) 当 m,n 互素时, 我们来证明 F 是双射, 结合定义域与值域的元素个数相等即可得到 F 是双射. 为此, 设 $x,y\in\{0,1,\dots,mn-1\}$ 满足 $F(x)=F(y)$, 则有 $m\mid x-y, n\mid x-y$. 由 m,n 互素可得 $mn\mid x-y$. 注意到 $x-y\in[-(mn-1),mn-1]$, 0 是此区间内 mn 唯一的倍数, 因而有 $x=y$, 从而验证了 F 是单射.

(2) 我们来数每个像点 $F(x_0)$ 的原像点的个数, 即满足 $F(x)=F(x_0)$ 的 $x\in\{0,1,\dots,mn-1\}$ 的个数. 注意到,

$$F(x)=F(x_0)\iff m\mid x-x_0, n\mid x-x_0\iff x-x_0\text{是}m,n\text{的公倍数}\iff [m,n]\mid x-x_0.$$

课上我们证明了 $[m,n](m,n)=mn$, 从而有 $[m,n]=\frac{mn}{d}$. 这样, $F(x)=F(x_0)$ 当且仅当 $\frac{mn}{d}\mid x-x_0$, 也当且仅当存在整数 k 使得 $x=x_0+\frac{mn}{d}k$. 结合 x 的取值范围 $0\le x\le mn-1$, 可得 k 的取值范围为

$$\frac{-x_0}{mn/d}\le k\le\frac{mn-1-x_0}{mn/d}=d+\frac{-1-x_0}{mn/d}$$

设 $-1-x_0$ 关于 mn/d 的带余除法为 $-1-x_0=q(mn/d)+r$, 其中 $0\le r<mn/d$, 则上述关于 k 的约束可改写成

$$q+\frac{r+1}{mn/d}\le k\le d+q+\frac{r}{mn/d}\iff q+1\le k\le d+q,$$

由此可知满足条件的 k 共有 d 个. 这样, 对 F 的每个像点, 它都恰好 d 个原像点. 利用 Fubini 定理可得

$$mn=\sum_{y\in\mathrm{Im}(F)}\#F^{-1}(\{y\})=\sum_{y\in\mathrm{Im}(F)}d=d\cdot|\mathrm{Im}(F)|,$$

即有 $|\mathrm{Im}(F)|=\frac{mn}{d}$.

(2) 的另一种证法. 注意到,$(b,c)\in\mathrm{Im}(F)$ 当且仅当存在 $a\in\{0,1,\dots,mn-1\}$ 满足 $a\equiv b\pmod m, a\equiv c\pmod n$, 当且仅当仅当存在整数 a 满足 $a\equiv b\pmod m, a\equiv c$ $(\mathrm{mod}\ n)$(因为对满足此同余方程组的 a, 设 a 除以 mn 的余数为 $a_0\in\{0,1,\dots,mn-1\}$, 则 a_0 也满足前述同余方程组). 前一方程等价于 $a=b+mx$, 代入后一方程, 可知要求 $b+mx\equiv c\pmod n$, 此方程有解的充分必要条件为 $b\equiv c\pmod d$.

□

6 (1) 叙述 Markov 不等式.

(2) 设 Ω 是有限的概率空间, $X:\Omega\to\mathbb{R}$ 是 Ω 上的一个随机变量. 对给定的实数 t 定义随机变量 $Y:\Omega\to\mathbb{R}$ 为

$$Y(\omega)=e^{tX(\omega)},\quad\forall\omega\in\Omega.$$

证明: 当 t 是正数时, 对每个实数 λ 有

$$P(X \geq \lambda) \leq \frac{E[Y]}{e^{t\lambda}}.$$

(3) 设随机变量 X 取值在 $[-1,1]$ 中, 且 X 的期望为零. 设 $t \in [-1,1]$ 是给定的实数, 定义随机变量 $Y : \Omega \to \mathbb{R}$ 为 $Y(\omega) = e^{tX(\omega)}$. 利用不等式

$$e^y \leq 1 + y + y^2, \quad \forall y \in [-1,1]$$

证明: $E[Y] \leq e^{t^2 \mathrm{Var}(X)}$, 其中 Var(X) 表示 X 的方差.

证明: (1) Markov 不等式为如下定理: 设 X 是非负的随机变量, 则对任何正数 $\lambda > 0$, 有

$$P(X \geq \lambda) \leq \frac{E[X]}{\lambda}.$$

(2) 注意到, 对正数 t, 有 $X \geq \lambda$ 当且仅当 $Y \geq e^{\lambda t}$. 结合 Markov 不等式可得

$$P(X \geq \lambda) = P(Y \geq e^{\lambda} t) \leq \frac{E[Y]}{e^{\lambda t}}.$$

(3) 设 X 的所有取值为 $x_1, \ldots, x_n$, 相应的概率分别为 $p_1, \ldots, p_n$, 则有 $\sum_{i=1}^{n} p_i x_i = 0$, 且 $\mathrm{Var}(X) = E[X^2] - E[X]^2 = \sum_{i=1}^{n} p_i x_i^2$. 结合提示中的不等式, 可估计 $E[Y]$:

$$E[Y] = \sum_{i=1}^{n} p_i e^{t x_i} \leq \sum_{i=1}^{n} p_i (1 + t x_i + t^2 x_i^2) = 1 + t^2 \mathrm{Var}(X) \leq e^{t^2 \mathrm{Var}(X)},$$

其中最后一步用到了熟知的不等式: 对任何实数 x 都有 $1 + x \leq e^x$.

$\square$