概率题目_百囚徒挑战

> 监狱决定给关押的100名囚徒一次特赦的机会，条件是囚徒通过一项挑战。所有囚徒被编号为1-100，对应他们编号的100个号码牌被打乱顺序放在了100个抽屉里。每个囚徒需要从所有抽屉里打开至多半数(50个)，并从中找出对应自己编号的号码牌。如果找到了则该名囚徒的任务成功。所有囚徒会依次单独进入挑战室完成任务，并且从第一个囚徒进入挑战室开始，直到所有囚徒结束挑战为止囚徒之间任何形式的交流都是禁止的。当一名囚徒完成任务后，挑战室会被恢复为他进入之前的样子（号码牌当然也放回原来的抽屉里）。在这100名囚徒中，任意一名囚徒的失败都会导致整个挑战失败，只有当所有囚徒全部成功完成任务时，他们才会统一得到特赦的机会。最后，在开始挑战之前，监狱给了所有囚徒一个月时间商量对策。那么，囚徒究竟有多大的几率得到释放？

A.小于0.0000000000000000000000000001%
B.大于0.0000000000000000000000000001%小于0.1%
C.大于0.1%小于30%
D.大于30%

> 假设囚徒的数量趋于无穷大，那么囚徒获得释放的几率趋于多少？

A.趋于0
B.趋于1
C.趋于(0,1)内的某个实数
D.在某个区间内振荡

之所以反直觉，是因为一眼看上去囚徒获胜的概率小的可怜，因为假如每个人的任务都是一次独立实验，那么他完成任务的概率只有 $1/2$ ，再乘以基数 100 人最终的成功概率约等于 10^{-30} ，当人数趋于无穷时这个数值还会继续缩小直到无限趋于0.这样才对。

但是实际上，这个题目并不是单纯的概率题。注意最后一句话，监狱给了所有囚徒一个月时间商量对策。比如考虑最简单的情况，囚徒只有两人，那么他们每人只能从两个抽屉里选择一个抽屉打开，这时他们被释放的概率是1/4吗？不是。如果两个囚徒打开不同的抽屉，那么他们被释放的概率是1/2，反之如果两个囚徒打开同一个抽屉，那么他们被释放的概率是0。

将盒子与号码的关系看作有向图 G：如果盒子 i 内放有号码 j，那么就存在一条从 i 指向 j 的有向边。不难发现，G 有一个重要特点：所有点的入度与出度均为 1，这说明 G一定由一些（意思是至少一个）互不连通有向环组成（如果不明白可以仔细想一想，这和欧拉回路有些像，区别只是 G 不一定连通）。

于是我们的策略也就呼之欲出了：沿着环依次查找即可。换句话说，囚徒 i 应从与自己编号相同的盒子 i 开始，如果盒子 i 内放有号码 j，那么接下来就应该打开盒子 j，以此类推，直到找到自己的号码或次数达到上限为止。按照这一策略，所有囚徒被释放的充要条件是所有的环的长度都小于 ⌊n/2⌋，不过这个概率可不容易计算，我们从相反的角度入手。

不妨假设抽屉里的号码牌是随机放置的（否则，囚徒可以自己在脑内打乱所有抽屉的位置以达到同样的效果※），之后囚徒首先为抽屉编号，例如从左上到右下依次编号。而每个囚徒的策略，就是首先打开与自己编号相同的抽屉，从中取出号码牌，并打开号码牌所对应的抽屉。之后，重复此过程，直到找到自己的号码牌，或者50个抽屉的机会用完。

例如，29号囚徒首先打开了29号抽屉，里面放着51号的号码牌，于是他打开51号抽屉，里面放着18号的号码牌，于是他打开18号的抽屉，里面放着29号的号码牌，他完成了任务。（只是随便举例）

为了计算成功概率，首先对这个游戏进行化简。将抽屉与号码牌的对应关系视为一个映射，例如 $f(29)=51$ ， $f(51)=18$ ，那么从任意一个数出发，不停地迭代计算，最终总能回到这个数。通过这种方法， $1\sim 100$ 的数字被分割为了一些“圆环”，而每个圆环的长度不一，比如 $3\to 3$ 的长度就是1，意味着3号抽屉里装着3号号码牌， $29\to 51\to 18\to 29$ 的长度是3；这时，我们发现，**所有囚徒能够通过挑战，当且仅当所有圆环的长度不超过50**，此时显然每个囚徒都能在50次以内找到自己的号码牌，反之如果有一个圆环长度超过50，那么这个圆环上的所有人都会失败。

接下来就是计算了。比起计算“所有圆环的长度不超过50”的概率，“有一个圆环长度超过50”的概率更容易计算。因为“有一个圆环的长度是51”和“有一个圆环的长度是52”之类的事件是彼此互斥的（圆环的长度总和是100），所以总概率就是它们的和。而对于 $m\geq 51$ ，只需先选出 m 个元素，将它们构成一个环，之后再将剩下的元素随机打乱即可唯一地得到一种分布。具体地说，所有形成长度为 m 环的映射种类为 $C_{100}^{m}\cdot(m-1)!\cdot(100-m)!=100!/m$ ，全排列个数为 $100!$ ，因此这个概率等于 $P(m)=1/m$

综上，所有圆环长度不超过50的概率等于 $P=1-\sum\limits_{m=51}^{100}\frac{1}{m}\approx 0.312$ ，这个概率就是囚徒被释放的概率。当囚徒人数趋于无穷大时，概率趋向于

$$P(N)=1-\sum_{m=N+1}^{2N}\frac{1}{m}\to 1-\ln 2$$

※否则，囚徒可以自己在脑内打乱所有抽屉的位置以达到同样的效果
因为在挑战开始之前有一个月时间商讨对策，所以囚徒可以在这段时间内约定好随机打乱抽屉的方式。另外，如果担心囚徒的策略被狱警知晓，也可以考虑迪菲赫尔曼密钥交换（前提是P≠NP），这是一种大声说悄悄话的方法，具体做法是利用非对称算法，使得两个没有任何共同知识的人知晓一个共同的关键词，并且任何窃听者无法通过两人的对话推理出这个关键词，之后这个关键词可以作为加密的秘钥使用。