详细解答

STEP III 2015，第 12 题

概率与统计 · 概率生成函数

> **STEP III 2015，第 12 题**
>
> 继续阅读之前，请先看题目（原题为英文）。题目载于 STEP Support Programme 的试题资料库：
>
> step.maths.org/questions/15-s3-q12

关键思路

除以 m 的余数（remainder）只取决于指数模 m 的值，所以在余数的生成函数（generating function）中，凡是出现 x^m 的地方都可以换成 1。把独立（independent）的投掷结果相加，相当于把生成函数相乘，之后再把 x 的幂次约简一次。有了这条规则，整个计算就变成简单的多项式代数，其中 $x \cdot y$ 和 y^2 都会化为 y 的倍数。

解答

全文中，设 $X_1, X_2, \ldots$ 为各次投掷的结果，它们互相独立，且各自在 $\{1, \ldots, 6\}$ 上服从均匀分布（uniform）。

约简规则。 设 m 为正整数。若 U 与 V 互相独立，且取值于 $\{0, 1, \ldots, m-1\}$，则 $U+V$ 的概率生成函数（probability generating function, pgf）是 $\mathrm{G}_U(x)\mathrm{G}_V(x)$，这是一个多项式，其中 x^k 项的系数就是 $U+V=k$ 的概率。$U+V$ 除以 m 的余数等于 j，当且仅当 $U+V$ 等于 j 或 $j+m$。因此，只要对 $k \geq m$ 把每个 x^k 换成 x^{k-m}，换言之令 $x^m = 1$，便得到该余数的 pgf。由于 S_n 的余数就是（S_{n-1} 的余数）+（X_n 的余数）的余数，而这两者互相独立，所以每个余数的 pgf 都可由前一个相乘再令 $x^m = 1$ 得到。我们以 $\equiv$ 表示“在使用 $x^m = 1$ 后相等”。

第 (i) 部分

掷出 $1, \ldots, 5$ 的余数分别是 $1, \ldots, 5$，而掷出 6 的余数是 0。每种情况的概率都是 $\frac{1}{6}$，所以

$$\mathrm{G}(x) = \tfrac{1}{6}\left(1 + x + x^2 + x^3 + x^4 + x^5\right) = \tfrac{1}{6}z, \qquad \text{其中} z = 1 + x + \cdots + x^5.$$

在 $x^6 = 1$ 之下，把 z 乘以 x 只是把每一项往前转一格：$xz = x + x^2 + \cdots + x^5 + x^6 \equiv z$。因此对每个 k 都有 $x^k z \equiv z$，而且

$$z^2 = \sum_{k=0}^{5} x^k z \equiv 6z.$$

所以 R_2 的 pgf 是

$$\tfrac{1}{36} z^2 \equiv \tfrac{1}{36} \cdot 6z = \tfrac{1}{6} z = \mathrm{G}(x),$$

正如所求。

同样的步骤在每一步都适用：若 R_{n-1} 的 pgf 是 $\mathrm{G}(x)$，则 R_n 的 pgf 是 $\mathrm{G}(x)^2 \equiv \mathrm{G}(x)$。由归纳法（induction），每个 R_n 的 pgf 都是 $\mathrm{G}(x) = \frac{1}{6} z$。$6 \mid S_n$ 的概率就是 $\mathrm{P}(R_n = 0)$，即 $\mathrm{G}(x)$ 的常数项（constant term）：

$$\mathrm{P}(S_n \text{ 可被整除，除数为6}) = \tfrac{1}{6}.$$

第 (ii) 部分

现在 $m = 5$。掷出 $1, 2, 3, 4$ 的余数是 $1, 2, 3, 4$；掷出 5 的余数是 0；掷出 6 的余数是 1。所以余数为 1 的概率是 $\frac{2}{6}$，其余各为 $\frac{1}{6}$：

$$\mathrm{G}_1(x) = \tfrac{1}{6}\left(1 + 2x + x^2 + x^3 + x^4\right) = \tfrac{1}{6}(x + y), \qquad y = 1 + x + x^2 + x^3 + x^4.$$

与第 (i) 部分完全一样，在 $x^5 = 1$ 之下有 $xy \equiv y$，所以对所有 k 都有 $x^k y \equiv y$，而且

$$y^2 = \sum_{k=0}^{4} x^k y \equiv 5y.$$

因此

$$\begin{aligned} \mathrm{G}_2(x) &\equiv \tfrac{1}{36}(x + y)^2 = \tfrac{1}{36}\left(x^2 + 2xy + y^2\right) \\ &\equiv \tfrac{1}{36}\left(x^2 + 2y + 5y\right) = \tfrac{1}{36}\left(x^2 + 7y\right), \end{aligned}$$

这就是所求的结果。（作为合理性检查，代入 $x = 1$ 得 $\frac{1}{36}(1 + 35) = 1$。）

一般的 pgf。 由约简规则，$\mathrm{G}_n(x) \equiv \mathrm{G}_1(x)^n = \frac{1}{6^n}(x + y)^n$。用二项式定理（binomial theorem）展开：

$$(x + y)^n = x^n + \sum_{k=1}^{n} \binom{n}{k} x^{n-k} y^k.$$

对 $k \geq 1$，利用 $y^k \equiv 5^{k-1} y$（由 $y^2 \equiv 5y$ 用归纳法得出），再利用 $x^{n-k} y \equiv y$，得

$$x^{n-k} y^k \equiv 5^{k-1} y.$$

所以

$$(x+y)^n \equiv x^n + y\sum_{k=1}^{n}\binom{n}{k}5^{k-1} = x^n + \frac{y}{5}\left[(1+5)^n - 1\right] = x^n + \frac{6^n-1}{5}y.$$

想一想 $(6^n-1)/5$ 是从哪里来的?

由二项式定理，和 $\sum_{k=0}^{n}\binom{n}{k}5^k$ 等于 $(1+5)^n = 6^n$；我们少了 $k=0$ 那一项（其值为 1），又多了一个因子 $\frac{1}{5}$。因此

$$G_n(x) = \frac{1}{6^n}\left(x^r + \frac{6^n-1}{5}y\right),$$

其中 r 是 n 除以 5 的余数（因为 $x^n \equiv x^r$）。所以每个余数的概率都是 $\dfrac{6^n-1}{5\cdot 6^n}$，唯独余数 r 额外多了 $\frac{1}{6^n}$。

被 5 整除。 我们需要 $P(T_n = 0)$，即 $G_n(x)$ 的常数项。y 的常数项是 1。

- 若 $5 \nmid n$，则 $r \neq 0$，x^r 对常数项没有贡献，所以

$$P(S_n \text{ 可被整除，除数为5}) = \frac{6^n-1}{5\cdot 6^n} = \frac{1}{5}\left(1 - \frac{1}{6^n}\right),$$

  正如所求。

- 若 $5 \mid n$，则 $r = 0$，$x^r = 1$ 会加上 $\frac{1}{6^n}$:

$$P(S_n \text{ 可被整除，除数为5}) = \frac{6^n-1}{5\cdot 6^n} + \frac{1}{6^n} = \frac{6^n+4}{5\cdot 6^n} = \frac{1}{5}\left(1 + \frac{4}{6^n}\right).$$

验算

- $n=1$: 公式给出 $\frac{1}{5}\cdot\frac{5}{6} = \frac{1}{6}$，而事实上只有掷出 5 才能被 5 整除。
- $n=2$: 公式给出 $\frac{1}{5}\cdot\frac{35}{36} = \frac{7}{36}$。直接计算，和为 5（四种方法）及 10（三种方法）共得 $\frac{7}{36}$，与 $\frac{1}{36}(x^2+7y)$ 的常数项吻合。
- $n=5$: 答案是 $\frac{6^5+4}{5\cdot 6^5} = \frac{389}{1944} \approx 0.2001$，略高于 $\frac{1}{5}$。用电脑对 $n \le 8$ 穷举全部 6^n 种结果，证实了整个 pgf $G_n(x)$ 以及两种情况。
- 当 $n \to \infty$ 时，两个答案都趋向 $\frac{1}{5}$: 余数变成均匀分布。

常见错误

- 忘记掷出 6 除以 5 的余数是 1，因此 G_1 中 x 的系数是 $\frac{2}{6}$。

- 对所有 n 都把 x^n 约简为 x^0：其实 x^n 约简为 x^r，其中 r 是 n 的余数，这正是 $5 \mid n$ 的情况与别不同的原因。
- 用“=”写出 $G_n(x) = G_1(x)^n$，然后没有按 $x^5 = 1$ 约简就直接读取系数。

STEP 之外

令 $x^m = 1$ 相当于在模 $x^m - 1$ 的多项式环（ring）中运算，即 m 阶循环群（cyclic group）的群代数（group algebra）。一个等价的工具是单位根滤波（roots-of-unity filter）：$P(m \mid S_n) = \frac{1}{m} \sum_{\omega^m=1} G_S(\omega)$，这正是离散傅里叶变换（discrete Fourier transform）在发挥作用。这个观点亦解释了为何循环上随机步的总和会趋于均匀分布，而这正是马尔可夫链（Markov chains）与群上随机漫步（random walks）理论的起点。Grimmett 与 Welsh 的 *Probability: An Introduction*（《概率导论》）以合适的程度介绍了生成函数与随机漫步。

Beyond STEP 详细解答：https://beyondstep.keithmcnulty.org/zh-hans/。解答文字采用 CC0 1.0；题目本身版权属 Cambridge University Press & Assessment 所有（©），本文件不予转载。由机器从英文翻译而成；尚未经审阅。