解答例

STEP III 2015、第 12 問

確率・統計 ・ 確率母関数

STEP III 2015、問 12

先に進む前に、まず問題を読んでおこう。問題は STEP Support Programme の問題データベースにある：

step.maths.org/questions/15-s3-q12

鍵となる考え方

m で割った余り（remainder）は指数を m で割った余りにしか関係しないので、余りの母関数（generating function）では、x^m が現れるところはどこでも 1 に置き換えてよい。独立（independent）な試行の結果を足すことは母関数を掛けることにあたり、そのあとで再び x の冪を簡約すればよい。この規則を使うと、計算全体は $x \cdot y$ や y^2 が y の定数倍につぶれてしまう単純な多項式の計算になる。

解答

以下を通して、$X_1, X_2, \ldots$ をさいころを投げた結果とする。これらは独立で、それぞれ $\{1, \ldots, 6\}$ 上の一様分布（uniform）に従う。

簡約の規則。 m を正の整数とする。U と V が独立で $\{0, 1, \ldots, m-1\}$ の値をとるとき、$U+V$ の確率母関数（pgf, probability generating function）は $\mathrm{G}_U(x)\mathrm{G}_V(x)$ であり、これは x^k の項が $U+V=k$ となる確率をもつ多項式である。$U+V$ を m で割った余りが j となるのは、$U+V$ が j または $j+m$ のときちょうどである。したがって、その余りの確率母関数は、$k \geq m$ に対してすべての x^k を x^{k-m} に置き換えることで、言い換えれば $x^m = 1$ とおくことで得られる。S_n の余りは（S_{n-1} の余り）＋（X_n の余り）の余りであり、この二つは独立であるから、各余りの確率母関数は、一つ前のものに掛け算をしてから $x^m = 1$ とおくことで得られる。「$x^m = 1$ を用いると等しい」ことを $\equiv$ で表す。

小問 (i)

1,...,5 の目は余り 1,...,5 を与え、6 の目は余り 0 を与える。それぞれ確率 $\frac{1}{6}$ で起こるので、

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

$x^6 = 1$ のもとでは、z に x を掛けることは各項を一つずつ巡回的にずらすだけである：$xz = x + x^2 + \cdots + x^5 + x^6 \equiv z$。よって、すべての k について $x^k z \equiv z$ であり、

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

したがって R_2 の確率母関数は

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

となり、示すべきことが示された。

同じ手順がすべての段階で成り立つ：R_{n-1} の確率母関数が $\mathrm{G}(x)$ ならば、R_n の確率母関数は $\mathrm{G}(x)^2 \equiv \mathrm{G}(x)$ である。数学的帰納法（induction）により、すべての R_n の確率母関数は $\mathrm{G}(x) = \frac{1}{6}z$ である。$6 \mid S_n$ となる確率は $\mathrm{P}(R_n = 0)$、すなわち $\mathrm{G}(x)$ の定数項であるから、

$$\mathrm{P}(S_n \text{ が次の数で割り切れる：} 6) = \tfrac{1}{6}.$$

小問 (ii)

今度は $m = 5$ である。1, 2, 3, 4 の目は余り 1, 2, 3, 4 を与え、5 の目は 0 を、6 の目は 1 を与える。よって余り 1 の確率は $\frac{2}{6}$、他はそれぞれ $\frac{1}{6}$ である：

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

小問 (i) とまったく同様に、$x^5 = 1$ のもとで $xy \equiv y$ であるから、すべての k について $x^k y \equiv y$ であり、

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

したがって

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

となり、これが求める結果である。（確認として $x = 1$ を代入すると $\frac{1}{36}(1 + 35) = 1$ となる。）

一般の確率母関数。 簡約の規則により、$G_n(x) \equiv G_1(x)^n = \frac{1}{6^n}(x+y)^n$ である。二項定理（binomial theorem）で展開すると

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

$k \geq 1$ のとき、$y^k \equiv 5^{k-1} y$（$y^2 \equiv 5y$ から帰納法で得られる）と、さらに $x^{n-k} y \equiv y$ を用いると、

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

よって

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

考えてみよう $(6^n - 1)/5$ はどこから出てきたのか？

和 $\sum_{k=0}^{n} \binom{n}{k} 5^k$ は二項定理により $(1+5)^n = 6^n$ である。ここでは $k = 0$ の項（1 である）が欠けており、さらに因子 $\frac{1}{5}$ が余分についている。したがって

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

ここで r は n を 5 で割った余りである（$x^n \equiv x^r$ であるため）。よって、どの余りも確率 $\dfrac{6^n - 1}{5 \cdot 6^n}$ をもつが、余り r だけは $\frac{1}{6^n}$ が上乗せされる。

5 で割り切れること。 必要なのは $P(T_n = 0)$、すなわち $G_n(x)$ の定数項である。y の定数項は 1 である。

- $5 \nmid n$ のとき、$r \neq 0$ であり x^r は定数項に寄与しないので、

$$P(S_n \text{ が次の数で割り切れる：} 5) = \frac{6^n - 1}{5 \cdot 6^n} = \frac{1}{5}\left(1 - \frac{1}{6^n}\right),$$

  となり、示すべきことが示された。

- $5 \mid n$ のとき、$r = 0$ であり $x^r = 1$ が $\frac{1}{6^n}$ を加えるので、

$$P(S_n \text{ が次の数で割り切れる：} 5) = \frac{6^n - 1}{5 \cdot 6^n} + \frac{1}{6^n} = \frac{6^n + 4}{5 \cdot 6^n} = \frac{1}{5}\left(1 + \frac{4}{6^n}\right).$$

検算

- $n = 1$：公式は $\frac{1}{5} \cdot \frac{5}{6} = \frac{1}{6}$ を与え、実際 5 で割り切れるのは 5 の目だけである。

- $n = 2$：公式は $\frac{1}{5} \cdot \frac{35}{36} = \frac{7}{36}$ を与える。直接数えると、和が 5（4 通り）と 10（3 通り）で $\frac{7}{36}$ となり、$\frac{1}{36}(x^2 + 7y)$ の定数項と一致する。
- $n = 5$：答えは $\frac{6^5+4}{5 \cdot 6^5} = \frac{389}{1944} \approx 0.2001$ であり、$\frac{1}{5}$ よりわずかに大きい。$n \leq 8$ についてコンピュータで 6^n 通りの結果をすべて列挙すると、確率母関数 $G_n(x)$ 全体と両方の場合が確かめられる。
- $n \to \infty$ のとき、どちらの答えも $\frac{1}{5}$ に収束（converge）する：余りは一様分布に近づく。

よくある間違い

- 6 の目は 5 で割ると余り 1 を残すことを忘れ、G_1 の x の係数が $\frac{2}{6}$ になることを見落とす。
- すべての n について x^n を x^0 に簡約してしまう：項 x^n は n の余りを r として x^r に簡約されるのであり、まさにこのために $5 \mid n$ の場合が異なるのである。
- $G_n(x) = G_1(x)^n$ を「=」で書き、$x^5 = 1$ を法とした簡約をせずに係数を読み取ってしまう。

STEP のその先へ

$x^m = 1$ とおくことは、$x^m - 1$ を法とする多項式環（ring）、すなわち位数 m の巡回群（cyclic group）の群環（group algebra）の中で計算することにあたる。同等の道具として 1 の冪根フィルター（roots-of-unity filter）がある：$P(m \mid S_n) = \frac{1}{m} \sum_{\omega^m=1} G_S(\omega)$ であり、これは離散フーリエ変換（discrete Fourier transform）のはたらきそのものである。この見方は、巡回群上のランダムな歩みの和がなぜ一様分布に近づくのかも説明し、マルコフ連鎖（Markov chains）や群上のランダムウォーク（random walks）の理論の出発点となる。Grimmett と Welsh による *Probability: An Introduction*（確率論入門）は、母関数とランダムウォークをちょうどよい水準で扱っている。

Beyond STEP 解答集：https://beyondstep.keithmcnulty.org/ja/。解答本文は CC0 1.0 である。問題そのものは © Cambridge University Press & Assessment に帰属し、ここには掲載していない。英語版から機械翻訳したものであり、まだ校閲を経ていない。