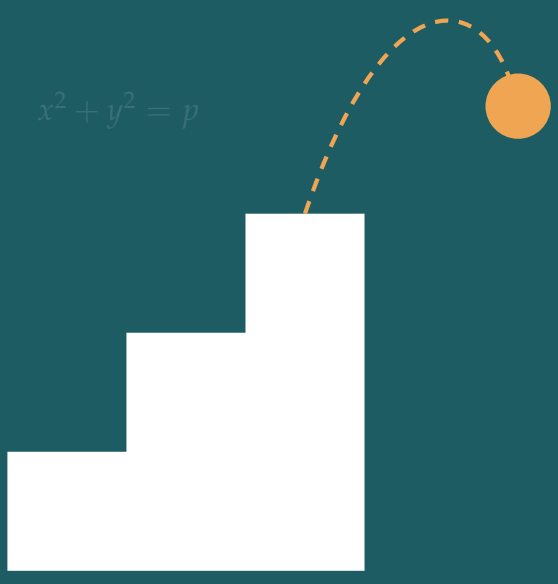
STEP 対策 · 大学の数学

Beyond STEP

第 9 章

数え上げと確率



KEITH McNULTY

Beyond STEP

大学数学への入り口としての
STEP 過去問

第 9 章

数え上げと確率

Keith McNulty

Beyond STEP：大学数学への入り口としての STEP 過去問

第 9 章：数え上げと確率

これは *Beyond STEP* 全 13 章のうちの第 9 章である。本書全体、各章単独の PDF、各節の印刷用ワークシート、そしてすべての STEP の問題の詳しい解答は、`beyondstep.keithmcnulty.org` で無料で閲覧・ダウンロードできる。

2026 年 11 月、オンラインにて初版発行。

本 PDF のうち著者自身の著作物（本文、解答、図、演習問題とその答えを含む）はすべて、クリエイティブ・コモンズ CC0 1.0 全世界（Creative Commons CC0 1.0 Universal）ライセンスのもとでパブリックドメインに提供されている。許可を求めることなく、いかなる目的でも複製、改変、共有してよい。詳しくは `creativecommons.org/publicdomain/zero/1.0` を参照のこと。

ここで扱う STEP の問題の著作権は Cambridge University Press & Assessment に帰属する。問題そのものは転載しておらず、各問題には公式の出典である STEP Support Programme の問題データベース、または OCR の過去問へのリンクを付している。

誤りの指摘は、`github.com/keithmcnulty/step_book_mcnulty` への issue として歓迎する。

章

9

数え上げと確率

数え上げは最も古い数学である。それを巧みに行うことは、今なお最も難しいことの一つである。

この章の内容

9.1	平面を分割する直線	STEP II 1990
9.2	ミニチュア版ラムゼーの定理	STEP I 1989
9.3	柵の杭を塗り分ける	STEP II 1995
9.4	関数としての数列	STEP I 2016
9.5	両替の仕方	STEP I 1997
9.6	奇妙なサイコロ	STEP I 1993
9.7	等しい累乗和	STEP I 1992
9.8	誰も自分のシャツを受け取らない	STEP II 2016
9.9	誕生日問題	STEP II 2007
9.10	いつでもおつりを渡せる	STEP I 2011
9.11	全種類を集める	STEP II 1994
9.12	ランダムな部分集合	STEP III 2019
9.13	いかさまサイコロ	STEP I 1999
A	演習問題の答え	p. 89

数え上げの技法

> 組合せ論は位相幾何学のスラム街である。
>
> — J. H. C. ホワイトヘッド（Whitehead）、1950 年代の言葉。今日この見方をとる者はいない。

誰でも数を数えることはできる。しかし、硬貨で £1 を作る方法は何通りあるか、10 人を誰も自分の席に座らないように座らせる方法は何通りあるか、地図を 4 色で塗り分ける方法は何通りあるか、と問われると、単純な数え上げはたちまち行き詰まる。場合が多すぎて書き出せないうえに、場合どうしが重なり合うからである。数え上げと配置の数学である**組合せ論**（combinatorics）とは、こうした問題を、書き出さずに解けるように整理する技法なのである。

ホワイトヘッドの言葉が示すように、組合せ論は長いあいだ、本格的な学問というより巧妙な小技の寄せ集めとみなされていた。それが変わったのは 20 世紀後半のことである。その原動力の一つは計算機科学であった。アルゴリズムが要する手順の数を数えることは、組合せ論の問題だからである。もう一つは、代数学、幾何学、確率論との深いつながりが発見されたことであった。今日、組合せ論は数学で最も活発な分野の一つである。2022 年、ジューン・フー（June Huh）は数学における最高の栄誉であるフィールズ賞（Fields Medal）を受賞したが、その受賞理由の一部は、Section 9.3 に登場する彩色多項式（chromatic polynomial）に関する 1968 年の予想を、代数幾何学の考え方を用いて証明したことであった。

なぜ数え上げが重要なのか

最も素朴な形の確率は、数え上げにほかならない。すべての結果が同様に確からしいとき、事象の確率は、その事象が起こる場合の数を全体の場合の数で割ったものである。したがって、トランプ、さいころ、くじに関する問題はすべて数え上げの問題であり、まさにこの理由から、本章の後半は確率分野の問題から採られている。しかし、数え上げが重要なのはゲームにとどまらない。計算機科学者は、アルゴリズムに必要な演算の回数や、アルゴリズムが失敗しうる仕方の数を数える。化学者は分子のとりうる構造を数える。生物学者は DNA 鎖の折りたたまれ方を数える。暗号学者は、攻撃者が試さなければならない鍵の数を数え、さらに Section 9.9 で見るように、何かが二つ一致するまでにいくつ必要かを数える。

大学で出会うこと

多くの大学では、1 年次または 2 年次に組合せ論あるいは離散数学の講義が開かれており、その主題は本章の主題と同じである。数え上げの基本原理（積の法則、全単射（bijection）、包除原理（inclusion–exclusion）、鳩の巣原理（pigeonhole principle））や、漸化式（recurrence relation）の立て方と解き方を学ぶ。数列を関数に、数え上げを代数に変える**母関数**（generating function）にも出会う。彩色からラムゼー理論（Ramsey theory）に至るまでのグラフ（graph）を学び、部分集合の束のような半順序集合（partially ordered set）を学ぶ。確率論の講義でも同じ道具が、期待値の線形性（linearity of expectation）とともに、ランダムな構造の解析に用いられる。さらに先へ進むと、組合せ論は代数学（対称関数、表現論）、整数論（分割、加法的組合せ論）、計算機科学（アルゴリズムの解析、計算量理論）とつながっていく。

本章を貫く問い

三つの大きな問い

1. **書き出さずにどう数えるか？**どのような構造（漸化式、全単射、母関数）を使えば、膨大な集まりを正確に数えられるか。
2. **何かが必ず起こるのはいつか？**大きさだけで、ある模様や一致や組み合わせが必然的に生じるのはどのようなときか。
3. **数え上げと確率は互いにどう助け合うのか？**確率を求めるのに数え上げが最適なのはどのようなときか。また、個数を求めるのに確率が最適なのはどのようなときか。

本章は前半と後半の二つに分かれる。最初の 7 つの節は純粋数学分野の問題から採られている。まず漸化式（平面を分割する直線、柵の支柱の塗り分け）と鳩の巣原理（ラムゼーの定理）から始め、次に母関数を展開して、それを用いて硬貨の組み合わせを数え、風変わりなさいころを設計し、べき乗和が等しくなるように数をチームに分ける。後半の 6 つの節は、確率分野の問題から採った古典的な数え上げの問題である。完全順列（derangement）と $1/e$ の出現、誕生日問題、投票問題（ballot problem）とその鏡像原理（reflection principle）、クーポン収集問題（coupon collector problem）、ランダムな部分集合、そして、どの合計も同様に確からしくなるようにさいころに細工することの不可能性を扱う。

本章に登場する考え方

§	話題	考え方
9.1	平面の領域	もう一つ加えると何が変わるか
9.2	ラムゼー理論	鳩の巣原理
9.3	グラフの彩色	連立漸化式、彩色多項式
9.4	母関数	数列が関数になる
9.5	分割	係数による数え上げ
9.6	シッヘルマンのさいころ（Sicherman dice）	多項式の因数分解
9.7	トゥエ–モース列（Thue–Morse sequence）	重根が釣り合った和を生む
9.8	完全順列	包除原理、$1/e$
9.9	偶然の一致	余事象、平方根の法則
9.10	投票問題	鏡像原理
9.11	クーポン収集問題	期待値の線形性、$n \ln n$
9.12	ランダムな部分集合	要素を一つずつ考える
9.13	細工したさいころ	相加・相乗平均の不等式（AM–GM）による不可能性の証明

本章の読み方

必ず小さな場合から始めること。直線を 3 本引いてみる、3 枚のカードの 6 通りの並べ方を書き出してみる、5p を作る方法を数えてみる。小さな場合は推測の手がかりとなるデータを与えてくれるし、最後には公式の検算にも役立つ。しかし、理由がわかるまでは規則性を信用してはならない。Section 9.1 には、$1, 2, 4, 8, 16, \ldots$ と続きながら次の項が 31 となる有名な数列が登場する。

9.1 平面を分割する直線

問題

STEP II 1990、問 4

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/90-s2-q4`

導入

ピースの大きさがそろっていなくてよいなら、n 回のまっすぐな切れ目でピザを何切れに分けられるだろうか。1 回切れば 2 切れ、2 回で 4 切れ、3 回で 7 切れ（8 ではない。実際に試してみよ）、4 回で 11 切れである。数列 $1, 2, 4, 7, 11, 16, \ldots$ は**怠惰な仕出し屋の数列**（lazy caterer's sequence）として知られており、この問題はその一般項を求めるものである。

この問題は、組合せ論（combinatorics）全体を貫く手法への最初の入門となる。すべてを一度に数えようとしてはならない。その代わりに、対象を一つ増やしたときに何が変わるかを問うのである。そして答えは、Section 7.9 でプラトンの立体とともに出会ったオイラー（Euler）の公式 $V - E + F = 2$ の特別な場合であることがわかる。

取りかかる前に

手を止めて、やってみよう 直線を一般の位置（general position）に保ちながら（どの 2 本も平行でなく、どの 3 本も 1 点を通らない）、$n = 1, 2, 3, 4$ の場合を丁寧に描け。それぞれの場合について、線分（segment）と領域（region）の個数を数えよ。規則性を推測できるだろうか。

次のようになるはずである。

n	0	1	2	3	4
線分	0	1	4	9	16
領域	1	2	4	7	11

線分の個数は n^2 のように見える。領域の個数は $1, 2, 3, 4$ ずつ増えている。つまり、階差が自然数になっている。

順を追って解く

段階 1　線分を数える

> **考えてみよう**　1 本の直線に注目せよ。他の直線のうち何本がそれと交わり、それを何個の部分に分けるか。

各直線は他の $n-1$ 本の直線のそれぞれと交わり（どれもその直線と平行ではない）、しかも交点は $n-1$ 個の相異なる点である（どの 3 本も 1 点で交わらない）。これら $n-1$ 個の点は、その直線を n 個の線分に分ける。両端にある 2 つの無限に伸びる部分と、その間にある $n-2$ 個の有限の線分である。直線が n 本あるので、全体では

$$n \times n = n^2 \text{ 個の線分.} \qquad \blacksquare$$

となる。これは直接的な数え上げであり、帰納法（induction）は必要ない。線分を直線ごとに数えたのである。

段階 2　直線を 1 本加えると何が起こるか

> **考えてみよう**　$n-1$ 本の直線が引かれているとし、そこに n 本目を加える。新しい直線は他の直線によって n 個の線分に分けられる。各線分は、それが通過する領域に対して何をするか。

新しい直線を引くと、その n 個の線分はそれぞれ既存の領域の一つを通り抜け、それを 2 つに分ける（図 9.1.1）。異なる線分は異なる領域にある。なぜなら、ある領域から別の領域へ移るには、新しい直線は既存の直線と交わらなければならないからである。したがって、n 本目の直線を加えると、領域の個数はちょうど n だけ増える。

$$R(n) = R(n-1) + n.$$

段階 3　漸化式を解く

$R(0) = 1$（直線がなければ領域は 1 つ）から出発すると、

$$R(n) = 1 + (1 + 2 + \cdots + n) = 1 + \frac{n(n+1)}{2} = \frac{n^2 + n + 2}{2}.$$

これを帰納法の形で述べると次のようになる。$\frac{1}{2}(1 + 1 + 2) = 2$ であるから、$n = 1$ のとき公式は成り立つ。また、$R(n-1) = \frac{1}{2}\big((n-1)^2 + (n-1) + 2\big) = \frac{1}{2}(n^2 - n + 2)$ ならば、$R(n) = \frac{1}{2}(n^2 - n + 2) + n = \frac{1}{2}(n^2 + n + 2)$ である。 ■

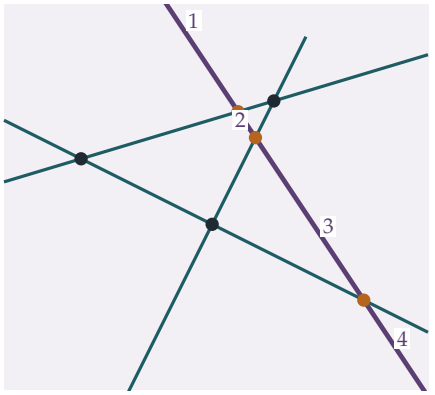


図 9.1.1　3 本の直線（ティール）は平面を 7 個の領域に分ける。4 本目の直線（プラム）は琥珀色の点で他の 3 本と交わり、それらの点によって 1 から 4 の番号をつけた 4 個の線分に分けられる。各線分は 1 つの領域を 2 つに分けるので、4 本目の直線によって領域は 4 個増え、11 個となる。

振り返り

- **一度に一つずつ数える。**線分は直線ごとに数え、領域は新しい直線 1 本が付け加えるものによって数えた。
- **幾何的な一歩を漸化式に変える。**「新しい線分はそれぞれ 1 つの領域を分ける」という観察が、$R(n) = R(n-1) + n$ になった。
- **一般の位置は重要である。**平行な直線や、1 点を通る 3 本の直線があると、領域の数は少なくなる。それぞれの仮定がどこで使われたかを確かめよ。

背後にある数学

姿を変えたオイラーの公式

ここでは第二の証明を示す。これは答えを単に導くだけでなく、その理由を説明するものである。直線の配置を地図とみなそう。交点を**頂点**（vertex）、線分を**辺**（edge）、

領域を**面**（face）とする。頂点は $V = \binom{n}{2}$ 個（直線の各組に 1 つ）、辺は $E = n^2$ 本ある。無限に伸びる線分には端が 1 つしかないので、それらがすべて集まる「無限遠」の頂点を 1 つ追加する。すると、図は球面上に描かれた地図になる（平面を球に巻きつけ、無限遠が頂上にくる様子を想像せよ）。Section 7.9 のオイラーの公式 $V - E + F = 2$ から

$$\left(\binom{n}{2} + 1\right) - n^2 + F = 2, \qquad \text{よって} \qquad F = n^2 - \frac{n(n-1)}{2} + 1 = \frac{n^2 + n + 2}{2}.$$

まったく異なる方向から、同じ数が得られた。領域はまた、種類によってきれいに分けられる。そのうち $2n$ 個は非有界であり（隣り合う無限半直線の各組の間に 1 つずつ）、残りの $\frac{1}{2}(n^2 + n + 2) - 2n = \binom{n-1}{2}$ 個は有界である。

二項係数と高次元

この公式は

$$R(n) = \binom{n}{0} + \binom{n}{1} + \binom{n}{2},$$

と書くことができ、これは偶然ではない。どの直線も水平にならないように図を回転させる。下に有界な領域には最低点があり、それは交点でなければならない。また、各交点はちょうど 1 つの領域（そのすぐ上にある領域）の最低点である。これにより、直線の各組に 1 つずつ、$\binom{n}{2}$ 個の領域が得られる。それ以外の領域はどこまでも下に伸びているので、すべての交点よりはるか下に引いた水平線と交わる。n 本の直線はその水平線を $n + 1$ 個の区間に分け、そのような領域のそれぞれに 1 つずつ区間がある。合計で $\binom{n}{2} + n + 1$ となる。3 次元では、一般の位置にある n 枚の平面は空間を

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} = \frac{n^3 + 5n + 6}{6}$$

個の部分に分け（**ケーキ数**（cake numbers）$1, 2, 4, 8, 15, 26, \ldots$）、この規則性はあらゆる次元で続く。証明は同じ帰納法である。新しい平面は他の平面によって、平面上の直線と同じ配置の領域に分けられ、それらの領域のそれぞれが空間の一部分を 2 つに分ける。

シュタイナーと超平面配置

直線や平面によって分けられる領域の個数の公式は、1826 年にヤコブ・シュタイナー（Jakob Steiner）によって発見された。今日、これは**超平面配置**（hyperplane arrangements）の理論の出発点となっている。この理論は、一般の位置にないものも含め、直線、平面、およびそれらの高次元版の任意の集まりが作る領域を数えるものである。1975 年の Thomas Zaslavsky による注目すべき定理は、どの超平面どうしが交わるかを記述する多項式を用いて、任意の配置の領域の個数を数える。同じ考え方は機械学習にも現れる。「ReLU」ユニットで構成されたニューラルネットワーク

は、超平面によって入力空間を領域に分け、その領域の個数は、ネットワークがどれほど複雑な関数を表現できるかの尺度となる。

思考のスキル

> **一つ増やしたときに何が変わるかを問う**
>
> n 個の対象からなる配置を数えるには、それを $n-1$ 個の配置と比べよ。全体よりも変化のほうがはるかに数えやすいことが多い。
>
> これは、証明のためだけでなく発見のための道具として帰納法を使うことである。組合せ論で最もよく使われる手の一つであり、幾何的な問題を解くことのできる漸化式に変えてくれる。

次の一歩

1. **円。** どの 2 つも 2 点で交わり、どの 3 つも 1 点を通らない n 個の円は、平面を $n^2 - n + 2$ 個の領域に分けることを示せ。

2. **平行な直線。** n 本の直線のうち k 本が互いにすべて平行である（それ以外は一般の位置にある）とき、領域はいくつあるか。

3. **ケーキ数。** 一般の位置にある n 枚の平面が空間を $\frac{1}{6}(n^3 + 5n + 6)$ 個の領域に分けることを、帰納法によって証明せよ。

4. **崩れる規則性。** 円周上に n 個の点をとり、すべての 2 点の組を弦で結ぶ。ただし、円の内部でどの 3 本の弦も 1 点を通らないものとする。$n = 1, 2, 3, 4, 5$ のとき、領域は $1, 2, 4, 8, 16$ 個になる。$n = 6$ のときの領域の個数を数えよ。（ヒント：オイラーの公式を用いよ。4 点の組それぞれから交点が 1 つできる。）その個数が $1 + \binom{n}{2} + \binom{n}{4}$ であることを示せ。

さらに学ぶために

- **Ronald Graham, Donald Knuth & Oren Patashnik, *Concrete Mathematics***（Addison-Wesley）、第 1 章。まさにこの問題と、その「ピザ」版および「ジグ」版から始まる。

- **Miklós Bóna, *A Walk Through Combinatorics***（World Scientific）。親しみやすい入門書で、帰納法、グラフ、オイラーの公式の章がある。
- **Richard Guy, "The strong law of small numbers"**、*American Mathematical Monthly* 95 (1988)。一見明らかに見えて実は誤りである規則性が数多く紹介されており、演習問題の円の問題も含まれている。

9.2 ミニチュア版ラムゼーの定理

問題

STEP I 1989、問 4

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/89-s1-q4`

導入

6 人が集まるパーティーでは、互いに全員が知り合いである 3 人か、互いに全員が見知らぬ者同士である 3 人が必ず存在する。これは 6 人が誰であっても保証される。5 人ではこれは保証されない。このささやかな事実は**ラムゼーの定理**（Ramsey's theorem）の最初の場合であり、現代の組合せ論（combinatorics）を貫く原理を捉えている。すなわち、**完全な無秩序は不可能である**。十分に大きな構造は、どのように色を塗られ、どのように配置されていようとも、高度に秩序立った部分を必ず含むのである。

証明はわずか 4 行で済む。しかし、自然に浮かぶ次の問い（互いに知り合いである 4 人か、互いに見知らぬ 4 人を保証するには何人必要か。5 人ならどうか）は、数学で最も難しい未解決問題のいくつかにつながっている。

取りかかる前に

考えてみよう 6 個の点が意味をもつのは、どの 2 点の組がどの色で結ばれているかという点だけであり、幾何学的な配置は目くらましにすぎない。線分は全部で何本あり、各点からは何本出ているか。

線分は $\binom{6}{2} = 15$ 本あり、各点からは 5 本ずつ出ている。（一般の位置（general position）にあるという条件は、どの 3 点も本物の三角形をなすことを保証しているにすぎない。この問題は実際には、6 頂点の**完全グラフ**（complete graph）K_6 の辺（edge）を 2 色で塗り分ける問題である。）

順を追って解く

段階 1　5 本の線分と 2 つの色

> **考えてみよう**　A からは 5 本の線分が出ており、それぞれ金色か銀色である。それらの色について確実にいえることは何か。

少なくとも 3 本は同じ色である。もし金色が高々 2 本、銀色も高々 2 本であれば、線分は高々 4 本しかないことになる。これが**鳩の巣原理**（pigeonhole principle）である。5 個の物を 2 つの箱に入れると、ある箱には少なくとも 3 個が入る。（必要なら色の名前を入れ替えて）AB、AC、AD がすべて金色であるとしよう。

段階 2　反対側の端に目を向ける

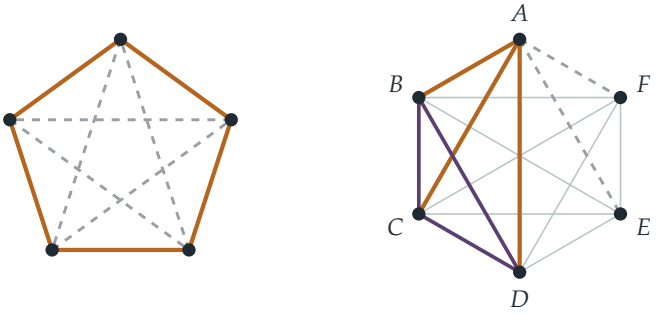
> **考えてみよう**　次に三角形 BCD を見よ。その辺のうちどれか 1 本でも金色であったらどうなるか。1 本も金色でなかったらどうなるか。

三角形 BCD のある辺、たとえば BC が金色であれば、ABC は 3 辺 AB、AC、BC がすべて金色となる。BCD のどの辺も金色でなければ、BC、CD、DB はすべて銀色であり、BCD は銀色の三角形となる。いずれにしても単色の三角形が存在する（図 9.2.1 右）。 ■

段階 3　5 点では足りない

> **考えてみよう**　5 点の場合、各点から出る線分は 4 本しかない。各点がちょうど 2 本ずつ各色の線分をもつように色を塗るにはどうすればよいか。

5 点を正五角形の頂点に置く（一般の位置にしたければ、平面から少しだけ持ち上げればよい）。五角形の 5 本の辺を金色に、5 本の対角線を銀色に塗る（図 9.2.1 左）。金色の辺は長さ 5 の閉路（5-cycle）をなし、三角形を含まない。銀色の辺は五芒星（pentagram）をなすが、これもまた長さ 5 の閉路であり、三角形を含まない。したがって単色の三角形は存在しない。 ■



5 点：単色の三角形はない　　6 点：BCD に注目する

図 9.2.1　左：五角形を金色（実線）、五芒星を銀色（破線）に塗った 5 点には単色の三角形がない。右：6 点の場合、A から出る 5 本の線分のうち 3 本は同じ色であり、たとえば B、C、D への線分が金色であるとする。このとき三角形 BCD（紫）がすべてを決める。金色の辺が 1 本でもあれば A とともに金色の三角形ができ、金色の辺が 1 本もなければ BCD が銀色の三角形となる。

振り返り

- **無関係なものを取り除く。**空間内の点は色付きのグラフになった。意味をもったのは辺の色だけである。
- **鳩の巣原理。**5 本の辺と 2 つの色から、同じ色の辺が 3 本あることが導かれた。
- **適切な対象での場合分け。**金色の辺が 3 本見つかれば、その反対側の端がなす三角形がすべてを決着させた。
- **最良性。**五角形の例は、6 という数をそれ以上小さくできないことを示している。よい定理には、それが最良であることを示す例が伴うものである。

背後にある数学

ラムゼー数

ラムゼー数（Ramsey number）$R(s,t)$ とは、K_N の辺を金色と銀色でどのように塗り分けても、金色の K_s（s 個の点からなる集合で、それらの間の辺がすべて金色であるもの）か銀色の K_t が必ず含まれるような最小の N のことである。この問題は $R(3,3) = 6$ を示したことになる。6 点では必ず成り立ち、五角形の例は 5 点では成り立たないことを示している。

フランク・ラムゼー（Frank Ramsey）は 1928 年に、これらの数が常に存在すること、

すなわち任意の s と t に対して条件を満たす N が存在することを証明した。その証明は上の議論を一般化した帰納法（induction）であり、$R(s,t) \le R(s-1,t) + R(s,t-1)$ を示すものである。しかし、正確な値を求めることは途方もなく難しい。

$$R(3,3) = 6, \qquad R(4,4) = 18, \qquad 43 \le R(5,5) \le 46.$$

$R(4,4)$ の値は 1955 年に求められた。膨大なコンピュータ探索にもかかわらず、$R(5,5)$ はいまだに分かっていない。上界（upper bound）46 が証明されたのは、ようやく 2024 年のことである。コンピュータで K_{43} のすべての塗り分けを単純に調べることはできない。塗り分けは 2^{903} 通りあり、宇宙に存在する原子の数よりはるかに多いのである。

エルデシュと宇宙人

ラムゼー理論の発展に誰よりも貢献したポール・エルデシュ（Paul Erdős）は、次のような話を好んで語った。宇宙人が地球に侵攻してきて、$R(5,5)$ の値を教えなければ地球を滅ぼすと脅したとしよう。そのときは、あらゆるコンピュータと数学者を総動員すべきであり、そうすれば値が見つかるかもしれない。しかし、もし彼らが $R(6,6)$ を求めてきたら、宇宙人を滅ぼすことを試みるべきだ、と。エルデシュはまた 1947 年に、驚くべき方法を用いて $R(k,k) > 2^{k/2}$ を証明した。彼は、$2^{k/2}$ 個未満の点の上で**ランダムに**色を塗ったグラフが単色の K_k を含まない確率が正であることを示したのである。したがって、どのように構成すればよいかは誰にも分からないにもかかわらず、条件を満たす塗り分けが存在しなければならない。この**確率的方法**（probabilistic method）は、今日では組合せ論における最も強力な道具の一つとなっている。

混沌からの秩序

ラムゼーの定理には多くの親戚があり、どれも同じ考え方、すなわち十分に大きな構造は秩序を避けられないという考え方を表している。**ファン・デル・ヴェルデンの定理**（van der Waerden's theorem）は、整数を有限個の色で塗り分けると、いくらでも長い単色の等差数列（arithmetic progression）が存在することを述べている。**エルデシュ–セケレシュの定理**（Erdős–Szekeres theorem）は、相異なる n^2+1 個の数からなる任意の数列が、長さ $n+1$ の増加部分列または減少部分列（subsequence）を含むことを述べている。そしてラムゼー自身は論理学の問題に関心をもっていた。彼はこの定理を、論理的な命題の真偽の判定に関する論文の中で、補題（lemma）として証明したのである。

思考のスキル

鳩の巣原理

kn 個より多くの物を n 個の箱に入れると、ある箱には k 個より多くの物が入る。

この原理は自明であるが、うまく使うのは一つの技芸である。腕の見せどころは、何を物とし、何を箱とするかの選び方にある。ここでは、1 点から出る 5 本の辺が物であり、2 つの色が箱であった。大学では、鳩の巣原理による議論は、整数論（無理数の分数による近似）、解析学（ボルツァーノ–ワイエルシュトラスの定理（Bolzano–Weierstrass theorem））、そして組合せ論の至るところに現れる。

次の一歩

1 **少なくとも 2 つ。** K_6 の任意の 2 色による塗り分けにおいて、実は単色の三角形が少なくとも 2 つ存在することを示せ。（**ヒント：**「二色の角」、すなわち共通の頂点で色の異なる 2 辺の組を数えよ。金色の辺を g 本、銀色の辺を $5-g$ 本もつ点は、このような角 $g(5-g) \leq 6$ 個の頂点となっている。単色でない三角形はそれぞれ、このような角をちょうど 2 つ含む。）

2 **3 色。** K_{17} の辺を 3 色で塗り分けると、単色の三角形が存在することを示せ。（**ヒント：**ある点は同じ色の辺を少なくとも 6 本もつ。）

3 **3 と 4。** $R(3,4) \leq 10$ を示せ。すなわち、K_{10} を金色と銀色でどのように塗り分けても、金色の三角形か銀色の K_4 が存在することを示せ。（**ヒント：**各点は、金色の辺を少なくとも 4 本もつか、銀色の辺を少なくとも 6 本もつかのいずれかである。）実際には $R(3,4) = 9$ である。

4 **単調部分列。** $n = 2$ の場合のエルデシュ–セケレシュの定理を証明せよ。すなわち、相異なる 5 個の数からなる任意の数列は、長さ 3 の増加部分列または減少部分列を含むことを示せ。また、どちらも含まない 4 個の数からなる数列を求めよ。

さらに学ぶために

- **Miklós Bóna, *A Walk Through Combinatorics***（World Scientific）。鳩の巣原理とラムゼー理論の章。

- **Ronald Graham & Joel Spencer,「Ramsey theory」**, *Scientific American*（1990 年 7 月）。第一線の研究者 2 人による一般向けの入門記事。
- **Noga Alon & Joel Spencer, *The Probabilistic Method***（Wiley）。エルデシュの方法に関する標準的な本。第 1 章は取り組みやすい。
- **Paul Hoffman, *The Man Who Loved Only Numbers***（Fourth Estate）。エルデシュの伝記（邦訳『放浪の天才数学者エルデシュ』）。

9.3 柵の杭を塗り分ける

問題

STEP II 1995、問 2

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/95-s2-q2`

導入

一列に並んだ柱を塗るのは簡単である。最初の柱は 3 通り、残りの柱はそれぞれ 2 通り（直前の柱の色以外なら何でもよい）であるから、$3 \times 2^{n-1}$ 通りとなる。ところが、この列を曲げて円にすると、意外なほど扱いにくくなる。最後の柱は隣の柱だけでなく最初の柱とも異なる色でなければならず、それによって使えない色が 1 つ減るのか、まったく減らないのかは、それまでの塗り方すべてに依存するからである。

この問題では、古典的な工夫によってこの困難を回避する。最後の柱の色によって数え上げを場合分けし、それぞれの場合が互いにどう結びつくかを調べるのである。答えの $2^n + 2(-1)^n$ は**彩色多項式**（chromatic polynomial）の最初の例であり、四色定理（four colour theorem）の背後にある数学の一部をなしている。

取りかかる前に

手を止めて、やってみよう 円形に並んだ 3 本の柱、4 本の柱の塗り方をそれぞれ数えよ。$3 \times 2^{n-1}$ は数えすぎになっているか。なっているとすれば、どれだけ多いか。

円形に並んだ 3 本の柱は互いにすべて隣り合っているので、3 つとも異なる色でなければならない。よって $3! = 6$ 通りである。円形に並んだ 4 本の柱では 18 通りである（最後に確かめられる）。一列の場合の $3 \times 2^2 = 12$ と $3 \times 2^3 = 24$ と比べると、円形の場合には、最後の柱が最初の柱と同じ色になる塗り方が除かれていることがわかる。

順を追って解く

段階 1　2 種類の塗り方

考えてみよう　$n+1$ 本の柱の塗り方で、最初と最後の柱が赤であるものを考える。最後の柱を取り除く。残った最初の n 本の柱の塗り方について、何がいえるか。

柱 n は赤である柱 $n+1$ の隣にあるので、柱 n は赤ではない。柱 $n+1$ を取り除くと、最初が赤で最後が赤でない n 本の柱の塗り方、すなわち s_n 通りの塗り方のうちの 1 つが残る。逆に、s_n 通りの塗り方のどれも、柱 $n+1$ を赤に塗ることで、ちょうど 1 通りに延長できる。したがって、この 2 つの集合はちょうど 1 対 1 に対応し、$r_{n+1} = s_n$ である。

考えてみよう　$r_n + s_n$ は何か。

最初の柱が赤である塗り方は、最後の柱が赤であるか赤でないかのどちらかであるから、$r_n + s_n$ は最初が赤である n 本の柱の塗り方すべての個数である。最初の柱より後の柱はそれぞれ 2 通りの選び方があるので、$r_n + s_n = 2^{n-1}$ となる。よって

$$r_{n+1} + r_n = s_n + r_n = 2^{n-1}. \qquad \blacksquare$$

段階 2　数学的帰納法による公式の証明

$n = 1$ のとき柱は 1 本で赤に塗られるので $r_1 = 1$ であり、公式は $\frac{1}{3}(1+2) = 1$ を与える。r_n について公式が成り立つと仮定する。このとき

$$r_{n+1} = 2^{n-1} - r_n = 2^{n-1} - \frac{2^{n-1} + 2(-1)^{n-1}}{3} = \frac{2 \cdot 2^{n-1} - 2(-1)^{n-1}}{3} = \frac{2^n + 2(-1)^n}{3},$$

となり、これは r_{n+1} に対する公式である。 $\blacksquare$

手を止めて、やってみよう　この公式はどこから来たのか。漸化式（recurrence）$r_{n+1} + r_n = 2^{n-1}$ は微分方程式に似ている。すなわち、「特殊解」（particular solution）$c \cdot 2^n$ に、$r_{n+1} + r_n = 0$ を満たす「余関数」（complementary function）$A(-1)^n$ を加えたものである。c と A を求めよ。

段階 3　円形の場合

考えてみよう n 本の柱が円形に並んでいるとき、柱 1 の色を固定し、たとえば赤とする。ここで柱 n と柱 1 の間で円を切り、まっすぐ一列に伸ばす。一列の塗り方のうち、円形の正しい塗り方に対応するのはどれか。

まっすぐに伸ばすと、円は赤から始まる n 本の柱の列になり、最後の柱は柱 1 とも異なる色でなければならない。つまり最後の柱は赤ではない。これらはちょうど s_n 通りの塗り方である。柱 1 は 3 色のどれでもよいので、円形の塗り方の総数は

$$3s_n = 3(2^{n-1} - r_n) = 3 \cdot 2^{n-1} - 2^{n-1} - 2(-1)^{n-1} = 2^n + 2(-1)^n. \qquad \blacksquare$$

確認：$n = 3$ のとき $8 - 2 = 6$、$n = 4$ のとき $16 + 2 = 18$ となる。

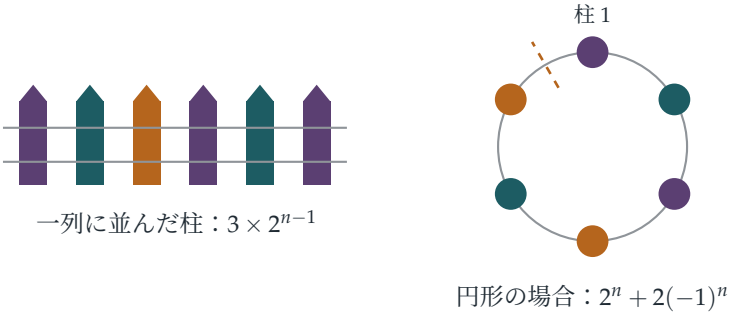


図 9.3.1 左：一列の場合、最初より後の各柱は直前の柱と異なる色であればよい。右：円形の場合、最後の柱は柱 1 とも異なる色でなければならない。破線のところで円を切ると、円形の塗り方は、最初と最後の柱の色が異なる一列の塗り方、すなわち問題で数えた s_n 通りの塗り方のうちの 1 つに変わる。

振り返り

- **互いに結びつく場合に分ける。**最後の柱が赤かどうかを記録することで、2 つの数列 r_n と s_n が得られ、それらは簡単な漸化式で結ばれていた。
- **全単射（bijection）。**$r_{n+1} = s_n$ は計算によってではなく、塗り方を 1 対 1 に対応させることで証明した。
- **円を切る。**循環的な問題が、両端に条件のついた一列の問題になった。

背後にある数学

彩色多項式

柱とその隣接関係は**グラフ**（graph）をなす。一列の場合は道（path）、円形の場合は閉路（cycle）である。**正しい彩色**（proper colouring）とは、隣り合う頂点に異なる色を塗る塗り方である。k 色による正しい彩色の個数は k の多項式であり、これをそのグラフの**彩色多項式**という。これは 1912 年にバーコフ（George Birkhoff）によって導入された。問題の議論を k 色で繰り返すと

$$\text{道：} k(k-1)^{n-1}, \qquad \text{閉路：} (k-1)^n + (-1)^n(k-1).$$

が得られる。$k = 3$ のとき、閉路の公式は $2^n + 2(-1)^n$ となる。バーコフは、あらゆる地図のグラフの彩色多項式が $k = 4$ で正であることを示すことによって、四色定理（どんな地図も、隣り合う国が異なる色になるように 4 色で塗り分けられる）を証明しようとした。この方法は結局成功しなかった。四色定理は 1976 年に Kenneth Appel と Wolfgang Haken によって、計算機を大規模に援用して最終的に証明された。彩色多項式は今なお活発な研究分野であり、統計物理学と意外なつながりをもっている。統計物理学では、彩色多項式は磁性の**ポッツ模型**（Potts model）として現れるのである。

行列による同じ数え上げ

第 7 章の線形代数を用いて、答えを別の見方で捉えることもできる。対角成分が 0 でそれ以外の成分が 1 である 3×3 行列を $\mathbf{M}$ とする。すなわち、(i, j) 成分は、色 i の次に色 j が来てよいとき 1 である。すると、$\mathbf{M}^{n-1}$ の (i, j) 成分は、色 i で始まり色 j で終わる一列の塗り方の個数を表すので、r_n は $\mathbf{M}^{n-1}$ の対角成分の 1 つである。円形の塗り方は、n ステップ後に出発点に戻る列であるから、円形の塗り方の個数は $\mathbf{M}^n$ の**トレース**（trace）である。$\mathbf{J}$ をすべての成分が 1 である行列として $\mathbf{M} = \mathbf{J} - \mathbf{I}$ であるから、$\mathbf{M}$ の固有値（eigenvalue）は $3 - 1 = 2$（固有ベクトル（eigenvector）$(1, 1, 1)$）と -1（重複度 2）であり、$\mathbf{M}^n$ のトレースは固有値の n 乗の和である：

$$\operatorname{tr} \mathbf{M}^n = 2^n + (-1)^n + (-1)^n = 2^n + 2(-1)^n.$$

この**転送行列**（transfer matrix）法は、1 ステップずつ組み立てられる配置を数えるために、組合せ論や統計物理学の至るところで用いられている。

思考のスキル

連立漸化式を立てる

1 つの数列だけでは簡単な漸化式を満たさないとき、少しだけ余分な情報（ここでは最後の柱の色）を記録し、場合どうしを結ぶ漸化式を求めよ。

これが状態（state）という考え方である。先へ進むために知る必要のあることだけを正確に記録し、それ以外は記録しない。これは計算機科学における動的計画法（dynamic programming）、確率論におけるマルコフ連鎖（Markov chain）（Section 12.16）、そして転送行列法の基礎となっている。

次の一歩

1 **k 色の場合。** この問題を k 色で考え直せ。$r_{n+1} = s_n$ が依然として成り立ち、$r_{n+1} + r_n = (k-1)^{n-1}$ となることを示し、r_n を求め、閉路の彩色多項式 $(k-1)^n + (-1)^n(k-1)$ を導け。

2 **赤が 2 つ続かない。** 一列に並んだ n 本の柱を赤または白に塗るとき、隣り合う 2 本の柱がともに赤にならない塗り方は何通りあるか。（フィボナッチ（Fibonacci）数が現れるはずである。）

3 **車輪。** 円形に並んだすべての柱に隣接する中心の柱を加える（これを「車輪」という）。これを 4 色で塗る方法は何通りあるか。（ヒント：中心は 1 色を使い、円は残りの 3 色を使わなければならない。）

4 **ネックレス。** 円形の 2 つの塗り方について、一方が他方を回転したものであるとき同じものとみなすことにすると、$n = 4$ のとき異なる塗り方は何通りあるか。$n = 5$ のときはどうか。（これがバーンサイド（*Burnside*）の補題の出発点である。）

さらに学ぶために

- **Robin Wilson, *Introduction to Graph Theory***（Pearson）。『グラフ理論入門』。定番の入門書であり、彩色と四色問題を扱っている。
- **Robin Wilson, *Four Colours Suffice***（Penguin）。『四色で十分』。一般読者向けの、四色定理の物語。
- **Herbert Wilf, *generatingfunctionology***（オンラインで無料公開）。『母関数学』。漸化

式とその解き方を、転送行列法も含めて解説している。

9.4 関数としての数列

問題

STEP I 2016、問 8

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/16-s1-q8`

導入

電卓で 1/89 を計算してみよう。0.011235955… となる。数字は 0, 1, 1, 2, 3, 5 と始まり、これはフィボナッチ数（Fibonacci numbers）である。これは偶然だろうか。偶然ではない。この問題はその理由を明らかにする。

ここで使う考え方は、組合せ論（combinatorics）で最も強力なものの一つである。無限数列をとり、その項を冪級数（power series）の係数として用いることで、数列全体を一つの関数にまとめてしまうのである。すると数列についての事実は関数についての事実となり、代数や微積分を使って扱えるようになる。ハーバート・ウィルフ（Herbert Wilf）はこれを印象的な言葉で表した。「母関数とは、数列を並べて見せるために吊るす物干しロープである。」

取りかかる前に

考えてみよう 母関数（generating function）が $\frac{1}{1-x}$ である数列は何か。$\frac{1}{1-2x}$ ではどうか。数列の母関数に x を掛けると、数列はどうなるか。

等比級数（geometric series）$\frac{1}{1-x} = 1 + x + x^2 + \cdots$ は数列 1, 1, 1, … の母関数であり、$\frac{1}{1-2x} = 1 + 2x + 4x^2 + \cdots$ は 2 の冪の母関数である。x を掛けると、すべての項が一つずつ後ろにずれる。$x \cdot \frac{1}{1-x} = x + x^2 + \cdots$ は 0, 1, 1, 1, … の母関数である。

順を追って解く

段階 1　自然数と三角数

考えてみよう　$(1-x)^{-2}$ を二項級数で展開せよ。x^n の係数は何か。

二項級数（binomial series）により

$$(1-x)^{-2} = 1 + 2x + 3x^2 + 4x^3 + \cdots = \sum_{n \ge 0} (n+1) x^n,$$

であるから、$x(1-x)^{-2} = x + 2x^2 + 3x^3 + \cdots = \sum n x^n$ となる。これは $u_n = n$ の母関数である。

同様に、$(1-x)^{-3}$ における x^n の係数は $\frac{(-3)(-4)\cdots(-3-n+1)}{n!}(-1)^n = \frac{(n+1)(n+2)}{2}$ であるから、

$$x(1-x)^{-3} = \sum_{n \ge 1} \frac{n(n+1)}{2} x^n = x + 3x^2 + 6x^3 + 10x^4 + \cdots,$$

となり、これは三角数（triangle numbers）$u_n = \frac{1}{2}n(n+1)$ の母関数である。

考えてみよう　n^2 を n と $\frac{1}{2}n(n+1)$ を用いて表すにはどうすればよいか。

$n^2 = 2 \cdot \frac{1}{2}n(n+1) - n$ であり、母関数は数列と同じように足し合わせられるので、

$$\sum n^2 x^n = \frac{2x}{(1-x)^3} - \frac{x}{(1-x)^2} = \frac{2x - x(1-x)}{(1-x)^3} = \frac{x(1+x)}{(1-x)^3}. \qquad \blacksquare$$

段階 2　漸化式が方程式になる

考えてみよう　$u_n = k u_{n-1}$ の両辺に x^n を掛け、$n \ge 1$ のすべての n について足し合わせよ。各辺は f を用いてどう表されるか。

左辺は $\sum_{n \ge 1} u_n x^n = \mathrm{f}(x) - u_0 = \mathrm{f}(x) - a$ である。右辺は $kx \sum_{n \ge 1} u_{n-1} x^{n-1} = kx\,\mathrm{f}(x)$ である。よって $\mathrm{f}(x) = a + kx\,\mathrm{f}(x)$ であり、

$$\mathrm{f}(x) = \frac{a}{1-kx}. \qquad \blacksquare$$

もちろん $u_n = a k^n$ である。$\frac{a}{1-kx}$ を等比級数として展開すれば、このことが確かめられる。

段階 3　フィボナッチ数

漸化式（recurrence）$u_n = u_{n-1} + u_{n-2}$（$n \geq 2$）にも同じことを行う。

$$\sum_{n\geq 2} u_n x^n = x \sum_{n\geq 2} u_{n-1} x^{n-1} + x^2 \sum_{n\geq 2} u_{n-2} x^{n-2},$$

すなわち

$$\mathrm{f}(x) - u_0 - u_1 x = x\big(\mathrm{f}(x) - u_0\big) + x^2\,\mathrm{f}(x).$$

$u_0 = 0$、$u_1 = 1$ とすると、これは $\mathrm{f}(x) - x = x\,\mathrm{f}(x) + x^2\,\mathrm{f}(x)$ を意味するので、

$$\mathrm{f}(x) = \frac{x}{1 - x - x^2}. \qquad \blacksquare$$

段階 4　1/89 の説明

> **手を止めて、やってみよう**　収束（convergence）の問題は無視して（ここでは問題ない。この級数は $|x| < 0.618$ で収束する）、f に $x = \frac{1}{10}$ を代入せよ。何が得られるか。

$$\frac{1}{10}F_1 + \frac{1}{100}F_2 + \frac{1}{1000}F_3 + \cdots = \mathrm{f}\Big(\frac{1}{10}\Big) = \frac{1/10}{1 - 1/10 - 1/100} = \frac{10}{89}.$$

10 で割ると $\frac{1}{89} = \sum F_n/10^{n+1}$ となる。フィボナッチ数が小数の各位に順に置かれ、9 より大きくなると互いに重なり合う（図 9.4.1）。1/89 の最初のほうの桁にはフィボナッチ数が現れるが、後のほうの桁は繰り上がりによってぼやけてしまう。

```
0.  1
0.    1
0.      2
0.        3
0.          5
0.            8
0.            1 3
0.              2 1
0.                3 4
0.                  5 5
 ⋮
0. 0 1 1 2 3 5 9 5 5 0 5
```

図 9.4.1　$n = 1, 2, 3, \ldots$ について $F_n/10^{n+1}$ を足し合わせる。各フィボナッチ数の末尾は、一つ前のものより小数点以下で一桁右にくる。2 桁になると互いに重なり、繰り上がりによって小数第 7 位以降の数字が変わる。$\frac{1}{89} = 0.01123595505\ldots$。

振り返り

- **数列を関数に変える。**無限数列全体が一つの有理関数（rational function）になった。
- **漸化式は方程式になる。**x^n を掛けて和をとることで、規則 $u_n = u_{n-1} + u_{n-2}$ が、代数的に解ける f についての方程式に変わった。
- **古いものから新しいものを作る。**母関数を足したり、ずらしたり、微分したりすることで、一から始めることなく新しい母関数が得られた。

背後にある数学

母関数から公式へ

母関数は数列を符号化するだけではない。数列を求めることもできる。分母は $1 - x - x^2 = (1 - \varphi x)(1 - \psi x)$ と因数分解される。ここで $\varphi = \frac{1+\sqrt{5}}{2}$ と $\psi = \frac{1-\sqrt{5}}{2}$ は $t^2 = t + 1$ の解である。部分分数分解（partial fractions）により

$$\frac{x}{1 - x - x^2} = \frac{1}{\sqrt{5}}\left(\frac{1}{1 - \varphi x} - \frac{1}{1 - \psi x}\right),$$

となり、それぞれの分数を等比級数として展開すると

$$F_n = \frac{\varphi^n - \psi^n}{\sqrt{5}}.$$

これが**ビネ（*Binet*）の公式**である。$|\psi| < 1$ であるから第 2 項は非常に小さく、したがって F_n は $\varphi^n/\sqrt{5}$ に最も近い整数である。また、隣り合うフィボナッチ数の比は黄金比（golden ratio）に収束する（Section 2.2 の主題である）。同じ方法で、定数係数の線形漸化式（linear recurrence）はどれも解くことができる。演習には STEP I 2004 の例を含めてある。

母関数がこれほど役に立つ理由

真の威力は掛け算をするときに現れる。積 $\mathrm{f}(x)\mathrm{g}(x)$ における x^n の係数は $\sum_k u_k v_{n-k}$ であり、これは n を二つの部分に分けるすべての方法にわたる和である。これはまさに、二つの部品から組み立てられたものを数えるのに必要なものである。続く二つの節では、これを用いて両替の方法の数を数え（Section 9.5）、普通のさいころと同じ目の和の分布をもつ、奇妙な目のさいころを見つける（Section 9.6）。確率論では、同じ考え方から**確率母関数**（probability generating function）が得られ、独立な確率変数（independent random variables）の和を積に変える。

ド・モアブル、オイラー、ラプラス

アブラーム・ド・モアブル（Abraham de Moivre）は 1720 年代に、本質的には上の方法によって、母関数を用いて線形漸化式を解いた。レオンハルト・オイラー（Leonhard Euler）は 1748 年に、自然数の分割（partitions）を研究するために母関数を用い、ピエール＝シモン・ラプラス（Pierre-Simon Laplace）は母関数を著書 *Théorie analytique des probabilités*（『確率の解析的理論』、1812 年）の基礎に据えた。20 世紀には母関数は組合せ論の中心的な道具となり、現在では解析的な方法（母関数を複素変数（complex variable）の関数として調べること）により、厳密に解くにはあまりに複雑な数え上げの問題に対しても、精密な評価が得られるようになっている。

思考のスキル

表現を変える

数列についての問題は、その数列を関数や行列や図に変えると易しくなることがある。

母関数は漸化式を代数に、数え上げを掛け算に翻訳する。大学ではこうした翻訳に数多く出会うだろう。フーリエ級数（Fourier series）は関数を数列に変え、ラプラス変換（Laplace transform）は微分方程式（differential equation）を代数に変え、行列（matrix）は幾何を計算に変える。

次の一歩

1 **2 桁ずつ。** STEP II 2022、問 3（OCR が配布している 2022 年の過去問一式に収録、`www.ocr.org.uk/Images/696587-2022-past-papers.zip`）に挑戦せよ。$\frac{1}{89}$ の小数展開がフィボナッチ数で始まる理由を説明し、さらに、小数展開にこのパターンが 2 桁ずつ現れる分数を求める問題である。

2 **漸化式を解く。** STEP I 2004、問 7（`step.maths.org/questions/04-s1-q7`）に挑戦せよ。母関数と部分分数分解を用いて線形漸化式を解き、次にその方法を逆向きにたどる問題である。

3 **数を数える。** $\frac{1}{9801} = 0.00\,01\,02\,03\,04\ldots$ となり、2 桁ずつの区切りが 1 ずつ増えていくことを示せ。このパターンが最初に崩れるのはどこか。また、それはなぜか。

4 **平方の和。** $\frac{1}{1-x}\mathrm{f}(x)$ が部分和（partial sums）$u_0 + u_1 + \cdots + u_n$ の母関数であることを説明せよ。このことと小問 (i) の答えを用いて、$1^2 + 2^2 + \cdots + n^2$ の公式を求めよ。

さらに学ぶために

- **Herbert Wilf, *generatingfunctionology***（A K Peters、オンラインで無料公開）。母関数への古典的な入門書。この節の後に読むには第 1 章が最適である。
- **Ronald Graham, Donald Knuth & Oren Patashnik, *Concrete Mathematics***（Addison-Wesley、邦訳『コンピュータの数学』）、第 7 章。
- **Philippe Flajolet & Robert Sedgewick, *Analytic Combinatorics***（Cambridge University Press、オンラインで無料公開。『解析的組合せ論』）。大学 1 年の水準をはるかに超えるが、冒頭の数ページを読めば、この分野がどこへ向かうのかがわかる。

9.5 両替の仕方

問題

STEP I 1997、問 1

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/97-s1-q1`

導入

これは本書でいちばん易しい問題に見える。可能性を書き並べればよいだけだからである。しかし、書き並べる作業はすぐに手に負えなくなる。イギリスの硬貨で 20p を作る方法は 41 通り、50p を作る方法は 451 通り、£1 を作る方法は 4563 通りもある。この問題が本当に求めているのは**体系**、すなわち、何も漏らさず、何も二重に数えないように数え方を整理する方法である。

その体系の背後には美しい数学がある。各硬貨は等比級数（geometric series）に対応し、n ペンスを作る方法の数はそれらの積の係数（coefficient）になる。そして同じ考え方をすべての自然数に一度に適用すると、整数論で最も奥深い話題の一つであるオイラー（Euler）の**分割**（partitions）の理論が得られる。

取りかかる前に

考えてみよう 2p 硬貨と 1p 硬貨だけを使って n ペンスを作る方法は何通りあるか。答えが 2p 硬貨を何枚使うかだけで決まるのはなぜか。

2p 硬貨の枚数を決めれば、残りはすべて 1p 硬貨でなければならない。したがって、2p 硬貨の枚数としてあり得る各値 $0, 1, \ldots, \lfloor n/2 \rfloor$ に対して、ちょうど 1 通りずつの方法がある。よって方法は $\lfloor n/2 \rfloor + 1$ 通りである。これを $a(n)$ とおく。たとえば $a(10) = 6$、$a(5) = 3$ である。

順を追って解く

段階 1　10 ペンス

考えてみよう　大きい硬貨から順に数え方を整理せよ。10p 硬貨は何枚使えるか。それを決めたとき、5p 硬貨は何枚使えるか。

- 10p 硬貨 1 枚：1 通り。
- 10p なし、5p 2 枚：1 通り。
- 10p なし、5p 1 枚：残りの 5p 分を 2p と 1p で作る。これは $a(5) = 3$ 通り。
- 10p も 5p もなし：10p 分を 2p と 1p で作る。これは $a(10) = 6$ 通り。

合計は $1 + 1 + 3 + 6 = 11$ である。 ■

段階 2　一層ずつ積み上げる

考えてみよう　5p、2p、1p 硬貨で n ペンスを作る方法の数を $b(n)$ とする。$b(n)$ を関数 a を用いて表すにはどうすればよいか。

5p 硬貨の枚数 k を選ぶと、残りの $n - 5k$ ペンスは 2p と 1p 硬貨で作られる。したがって

$$b(n) = a(n) + a(n-5) + a(n-10) + \cdots .$$

これより次の表が得られる。

n	0	5	10	15	20
$a(n)$	1	3	6	8	11
$b(n) = a(n) + b(n-5)$	1	4	10	18	29

同様に、10p 硬貨も使う方法の数を $c(n)$ とすると $c(n) = b(n) + b(n-10) + \cdots$ であるから、$c(10) = 10 + 1 = 11$（段階 1 と一致する）、$c(20) = b(20) + b(10) + b(0) = 29 + 10 + 1 = 40$ となる。

段階 3　20 ペンス

最後に 20p 硬貨を考える。これを使う（1 通り）か、使わない（$c(20)$ 通り）かのどちらかである。よって

$$40 + 1 = 41 \text{ 通り}. \qquad \blacksquare$$

手を止めて、やってみよう 構造に注目せよ。新しい硬貨を加えるたびに層が一つ増え、各層は、一つ前の層を新しい硬貨の額面の間隔で足し合わせたものになっている。£1 や £100 に対して、コンピュータがこの計算をどのように実行するか想像できるだろうか。

振り返り

- **最大の部分で整理する。**最も大きい硬貨の枚数を先に固定することで、数え方が体系的になった。
- **表を作る。**新しい硬貨を加えるたびに、前の行から計算される新しい行が加わった。これは動的計画法（dynamic programming）であり、コンピュータがこの種のものを数える標準的な方法である。
- **既知の場合と照合する。**表は 10p の場合の 11 通りを再現した。

背後にある数学

等比級数としての硬貨

この問題を代数に変える考え方を述べよう。使う 5p 硬貨の枚数は $0, 1, 2, \ldots$ であり、それぞれ $0, 5, 10, \ldots$ ペンスに寄与する。これを次の級数として記録する。

$$1 + x^5 + x^{10} + x^{15} + \cdots = \frac{1}{1 - x^5}.$$

各硬貨について同じことを行い、掛け合わせる。

$$\frac{1}{(1-x)(1-x^2)(1-x^5)(1-x^{10})(1-x^{20})} = \sum_{n} w(n) x^n.$$

括弧を展開すると、各項 x^n は各括弧から一つずつ項を選ぶこと、すなわち各硬貨の枚数を選ぶことで、合計額が n となる場合から生じる。したがって x^n の係数 $w(n)$ は、n ペンスを作る方法の数にちょうど等しい。段階 2 の表は、この積を括弧一つずつ展開していたにすぎない。これは Section 9.4 の母関数（generating function）の考え方であり、その威力が発揮されるのが掛け算である。母関数の積は、選択の組合せを数えるのである。

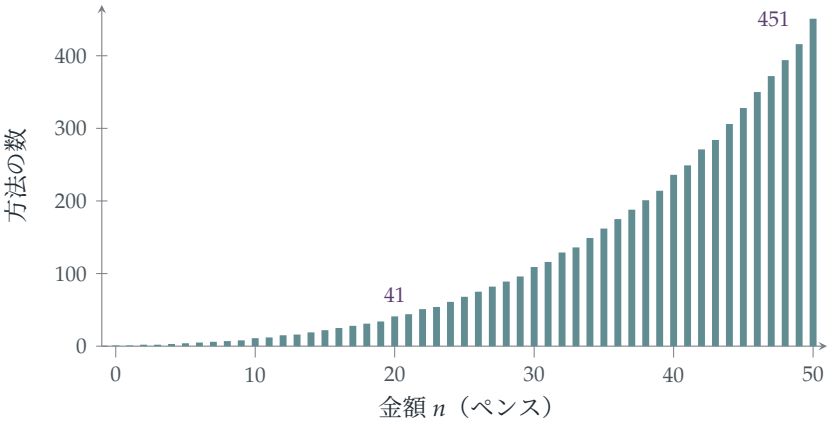


図 9.5.1　1p、2p、5p、10p、20p、50p 硬貨で n ペンスを作る方法の数。5 と 10 の倍数のところでの跳ね上がりは、新しい硬貨が初めて使えるようになる場所を示している。硬貨が 6 種類のとき、方法の数はおおよそ n^5 のように増加する。一般には、硬貨の種類の数より 1 小さい次数の多項式のように増加する。

分割

すべての正の整数が硬貨として使えるとしたらどうなるだろうか。このとき、順序を無視して n を正の整数の和として表す方法の数が**分割数**（partition number）$p(n)$ である。たとえば $4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1$ であるから $p(4) = 5$ である。オイラーは 1748 年に

$$\sum_{n\geq 0} p(n)x^n = \frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)\cdots},$$

であることを見抜き、これを用いて驚くべき恒等式を発見した。その一つは、n を**相異なる**部分の和として表す方法の数が、**奇数**の部分の和として表す方法の数に等しいというものである。（その証明は母関数を使えばわずか 1 行の代数計算である。演習で試してみよ。）

ハーディ、ラマヌジャンと $p(200)$

分割数は急速に増加する。$p(10) = 42$、$p(100) = 190\,569\,292$ である。1918 年、G. H. ハーディ（Hardy）とシュリニヴァーサ・ラマヌジャン（Srinivasa Ramanujan）は $p(n)$ に対する驚くべき公式を発見した。それは無限級数であり、その第 1 項は

$$p(n) \approx \frac{1}{4n\sqrt{3}}\, e^{\pi\sqrt{2n/3}}.$$

である。これを検証するため、Percy MacMahon はオイラーの恒等式を用いて $p(200) = 3\,972\,999\,029\,388$ を手計算で求めた。ハーディとラマヌジャンの級数の最初の数項は、誤差 1 未満で正しい答えを与えた。ラマヌジャンはまた、$p(5n+4)$ は常に 5 で、$p(7n+5)$ は 7 で、$p(11n+6)$ は 11 で割り切れることも発見した。このような規則性がほかに存在しない理由が解明されたのは、21 世紀になってからである。

思考のスキル

係数を通して数える

対象が独立な選択の組合せで作られるとき、各選択を一つの因子とすれば、全体の大きさが n である対象の個数は、その積における x^n の係数になる。

これにより、数え上げが代数に変わる。大学では、これが数え上げ組合せ論（enumerative combinatorics）の基礎となり、また確率母関数（probability generating functions）が独立な確率変数の和を扱う仕組みでもある。

次の一歩

1 **2 種類の 6。** STEP II 2012、問 1（`step.maths.org/questions/12-s2-q1`）に挑戦せよ。これは等比級数の積を用いて数える問題である。最後に、その係数が答えとなるような硬貨の数え上げ問題を述べよ。

2 **相異なる部分と奇数の部分。** $(1+x)(1+x^2)(1+x^3)\cdots$ が相異なる部分への分割の母関数であることを示せ。$1+x^k = \frac{1-x^{2k}}{1-x^k}$ を用いて、これが $\frac{1}{(1-x)(1-x^3)(1-x^5)\cdots}$ に等しいことを示し、オイラーの定理を導け。$n=6$ の場合に確かめよ。

3 **公式。** 1p、2p、5p 硬貨だけを用いて n ペンスを作る方法の数は、$\frac{(n+4)^2}{20}$ に最も近い整数であることを示せ。（まず小さい n で確かめよ。）

4 **順序を区別する。** 1p 硬貨と 2p 硬貨を 1 枚ずつ投入口に入れて n ペンスにする方法は、順序を区別すると何通りあるか。（この数列には以前に出会っているはずである。）

さらに学ぶために

- **George Andrews & Kimmo Eriksson, *Integer Partitions***（Cambridge University Press）。

学部生向けの、短く読みやすい入門書。

- **ポリア（George Pólya），「On picture-writing」**, *American Mathematical Monthly* 63 (1956)。1 ドルを両替する問題（方法は 292 通りある）を用いて母関数を説明した、ポリアによる古典的な解説。
- **Robert Kanigel, *The Man Who Knew Infinity***（Abacus）。ラマヌジャンの生涯と、ハーディとの共同研究を描いた伝記。

9.6 奇妙なサイコロ

問題

STEP I 1993、問 1

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/93-s1-q1`

導入

2 個の 6 面サイコロに正の整数を書き込んで、2 から 12 までのどの合計も普通のサイコロとちょうど同じ回数だけ出るようにする方法は、普通の書き方以外にあるだろうか。1978 年、マーティン・ガードナー（Martin Gardner）は『*Scientific American*』誌上で、そのような方法がちょうど 1 つだけあることを紹介した。1, 2, 2, 3, 3, 4 と書かれたサイコロと、1, 3, 4, 5, 6, 8 と書かれたサイコロの組である。これはジョージ・シッカーマン（George Sicherman）大佐が発見したもので、現在では**シッカーマンのサイコロ**（Sicherman dice）として販売されている。このサイコロでモノポリー（Monopoly）を遊んでも、普通のサイコロで遊ぶのとまったく区別がつかない。

この問題は準備運動であり、合計の表から 2 個のサイコロにどのように数が書かれているかを推定するものである。これを系統的に行う方法も、シッカーマンのサイコロが唯一の風変わりな組であることの証明（proof）も、どちらも各サイコロを多項式（polynomial）に置き換えることから得られる。

取りかかる前に

考えてみよう 1 個目のサイコロには i と書かれた面が p_i 面、2 個目のサイコロには j と書かれた面が q_j 面あるとする。合計 t を出す方法は何通りあるか。

その方法の数は $\sum_i p_i q_{t-i}$ である。1 個目のサイコロの目 i を選ぶと、2 個目は $t-i$ を出さなければならないからである。最初のサイコロの組では、合計 6 は $1+5$（1×1

通り）、$2+4$（2×1 通り）、$3+3$（2×2 通り）から得られ、それ以外はない。1 個目のサイコロには 4 も 5 もなく、2 個目には 0 がないからである。よって $1+2+4=7$ 通りである。 ■

順を追って解く

段階 1　両端から

2 個のサイコロを A, B とし、それぞれについて i と書かれた面の数を a_i, b_i とする。

> **考えてみよう**　合計 2 を出す方法も、合計 12 を出す方法もない。このことから 1 の面と 6 の面について何がいえるか。合計 3 を出す方法は 2 通りある。1 の面をもつのはどちらのサイコロか。

合計 2 が出ないことから $a_1b_1=0$ である。すなわち、1 の面をもつサイコロは高々 1 個である。合計 3 は $1+2$ か $2+1$ でしか得られず、それが 2 通りあるので、どちらかのサイコロは確かに 1 の面をもつ。それを A とすれば $b_1=0$ である。このとき

$$\text{合計3}:\quad a_1b_2=2,\qquad \text{よって}(a_1,b_2)=(2,1)\ \text{または}(1,2).$$

同様に、合計 12 が出ないことから $a_6b_6=0$ である。

段階 2　小さい合計から順に

> **考えてみよう**　$b_1=0$ に注意して、合計 4 についての式を書け。2 つの場合のそれぞれで、その式から何がわかるか。

合計 4 は $1+3$ または $2+2$ であり（$b_1=0$ なので $3+1$ はありえない）、$a_1b_3+a_2b_2=1$ である。

- **場合 (a)**：$a_1=2, b_2=1$ のとき、$2b_3+a_2=1$ より $b_3=0, a_2=1$。
- **場合 (b)**：$a_1=1, b_2=2$ のとき、$b_3+2a_2=1$ より $a_2=0, b_3=1$。

合計 5：$a_1b_4+a_2b_3+a_3b_2=1$。

- 場合 (a)：$2b_4+0+a_3=1$ より $b_4=0, a_3=1$。ここまでで A は $1,1,2,3$、B は 2 をもつ。B の残りの 5 面は 5 と 6 である。
- 場合 (b)：$b_4+0+2a_3=1$ より $a_3=0, b_4=1$。ここまでで A は 1、B は $2,2,3,4$ をもつ。A の残りの 5 面は $4,5,6$ のいずれかであり、B の残りの 2 面は $5,6$ のいずれかである。

段階 3 場合 (a) は成り立たない

考えてみよう 場合 (a) について、合計 7 の式を書き、$b_5 + b_6 = 5$ を用いよ。

合計 7：$a_1b_6 + a_2b_5 + a_3b_4 + a_4b_3 + a_5b_2 = 2b_6 + b_5 + 0 + 0 + a_5 = 3$。$b_6 = 5 - b_5$ を代入すると $10 - b_5 + a_5 = 3$ となり、$b_5 = 7 + a_5 \geq 7$ である。しかし B には 6 面しかない。よって場合 (a) はありえない。

段階 4 場合 (b) は成り立つ

考えてみよう 場合 (b) について、合計 6 と 11、および $a_6b_6 = 0$ を用いよ。

合計 6：$a_1b_5 + a_4b_2 = b_5 + 2a_4 = 4$（他の積は $a_2 = a_3 = 0$ または $b_1 = 0$ を含む）。$b_5 \leq 2$ であり、$b_5 = 4 - 2a_4$ は偶数なので、$b_5 = 0, a_4 = 2$ または $b_5 = 2, a_4 = 1$ である。

- $b_5 = 0$ ならば B は $2,2,3,4,6,6$ であるから $a_6 = 0$ となり、A は $1,4,4,5,5,5$ である。しかしこのとき合計 7 は $a_1b_6 + a_4b_3 + a_5b_2 = 2 + 2 + 6 = 10$ 通りとなり、3 通りではない。
- $b_5 = 2$ ならば B は $2,2,3,4,5,5$ で $b_6 = 0$ であり、A は $1,4$ と、5 と 6 からなる 4 面である。合計 11：$a_6b_5 = 2a_6 = 6$ より $a_6 = 3, a_5 = 1$。

したがって、ありうるのは次のものだけである。

$$A:\ 1,4,5,6,6,6, \qquad B:\ 2,2,3,4,5,5.$$

最後に、これらのサイコロが表全体を与えることを確かめなければならない。ここまでの推論では合計の一部しか使っていないからである。実際に展開する（あるいは後述の多項式を用いる）と、表のすべての値が確認できる。 ■

振り返り

- **両端から始める。**最小と最大の合計には積が 1 つか 2 つしか現れないので、最も強い情報が得られる。
- **場合分け（case analysis）をして、つぶしていく。**合計を 1 つ調べるごとに可能性が絞られ、最後に 1 つの場合だけが残った。
- **十分性（sufficiency）を確かめる。**推論によってサイコロがどうでなければならないかがわかり、最後の確認によってそれが実際に条件を満たすことがわかった。

背後にある数学

多項式としてのサイコロ

各サイコロを、i と書かれた面 1 つにつき項 x^i を 1 つもつ多項式として表す。普通のサイコロは $x+x^2+x^3+x^4+x^5+x^6$ であり、問題のサイコロは

$$A(x)=x+x^4+x^5+3x^6,\qquad B(x)=2x^2+x^3+x^4+2x^5.$$

である。掛け合わせると、面の各組は $x^ix^j=x^{i+j}$ を与えるので、$A(x)B(x)$ における x^t の係数は合計 t を出す方法の数になる。これは再び Section 9.4 の母関数（generating function）の考え方である。合計の表はまさに積 $A(x)B(x)$ にほかならず、先ほどの場合分けによる推論は、それを因数分解する一つの方法だったのである。

シッカーマンのサイコロ

普通のサイコロ 2 個の場合、積は $(x+x^2+\cdots+x^6)^2$ である。合計が同じになるサイコロの組はどれも、$P(x)Q(x)=(x+\cdots+x^6)^2$ を満たす多項式 $P(x),Q(x)$ をもたなければならない。そこで因数分解すると

$$x+x^2+\cdots+x^6=x(1+x)(1+x+x^2)(1-x+x^2),$$

となり、これらの因数は（整数係数の多項式として）これ以上分解できない。よって P と Q はそれぞれ因数 $x,1+x,1+x+x^2,1-x+x^2$ から作られ、各因数は全体でちょうど 2 回ずつ現れる。次の 3 つの条件によって選び方が絞られる。

- 各サイコロは 6 面をもつので $P(1)=Q(1)=6$ である。各因数は $x=1$ で値 $1,2,3,1$ をとるので、各サイコロは $1+x$ と $1+x+x^2$ を 1 つずつもつ。
- 0 と書かれた面はないので $P(0)=Q(0)=0$ である。よって各サイコロは因数 x を 1 つずつもつ。
- 残る自由度は、2 つの $1-x+x^2$ をどう分けるかだけである。1 つずつ分ければ普通のサイコロになる。両方を一方のサイコロに入れると

$$x(1+x)(1+x+x^2)=x+2x^2+2x^3+x^4,$$
$$x(1+x)(1+x+x^2)(1-x+x^2)^2=x+x^3+x^4+x^5+x^6+x^8.$$

  となる。

これがシッカーマンのサイコロ $1,2,2,3,3,4$ と $1,3,4,5,6,8$ であり（図 9.6.1）、この議論によって、これが普通のサイコロ以外の唯一の組であることが証明される。鍵となる事実は、多項式も整数と同様に既約元（irreducible）の積へ一意に分解される（unique factorisation）ということである。ここで整数論と組合せ論が出会うのである。

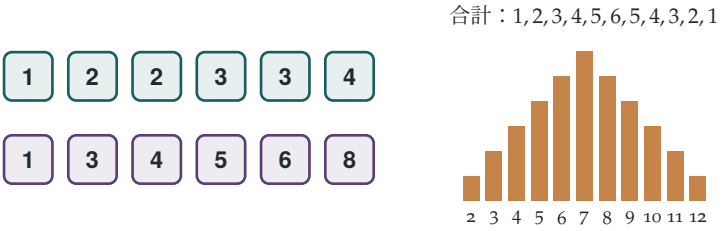


図 9.6.1　シッカーマンのサイコロ。2 個を同時に投げると、2 から 12 までのすべての合計が、普通のサイコロ 2 個とまったく同じ頻度で出る（右）。合計 2 は 1 通り、合計 3 は 2 通り、というように続き、合計 7 は 6 通りである。

確率母関数

確率論では、同じ考え方が**確率母関数**（probability generating function）として現れる。値 $0, 1, 2, \ldots$ をとる確率変数（random variable）X に対して $G(t) = E(t^X) = \sum P(X = k)t^k$ と定め、X と Y が独立（independent）ならば $E(t^{X+Y}) = E(t^X)E(t^Y)$ が成り立つ。独立な確率変数の和は、母関数の積に対応するのである。STEP III 2003 Q14（演習問題にある）はこの方法でシッカーマンのサイコロを求めており、Section 9.13 では関連する議論を用いて、2 個のサイコロにどのような偏りをもたせても、すべての合計を同じ確率にすることはできないことを示す。

思考のスキル

数え上げの問題を多項式に置き換える

対象が値の足し算によって組み合わさるときは、各対象を x の多項式で表せ。組み合わせることは掛け算になり、組み合わせについての問いは因数分解についての問いになる。

ここでは、サイコロについての問いが多項式の一意分解の問題になった。大学では、このような置き換えがいたるところに現れる。組合せ論にも、確率論にも、そして代数学にも現れる。代数学では、多項式は整数と似た算術をもつ環（ring）として、それ自体が研究対象となる。

次の一歩

1 **四面体のサイコロ。** STEP III 2003、問 14（`step.maths.org/questions/03-s3-q14`）

に挑戦せよ。これは 4 面のサイコロについてシッカーマンの問いを考えるものである。（**ヒント：**$x + x^2 + x^3 + x^4 = x(1 + x)(1 + x^2)$。）

2 **表の確認。**$(x + x^4 + x^5 + 3x^6)(2x^2 + x^3 + x^4 + 2x^5)$ を展開し、問題の表と照らし合わせよ。

3 **3 個のサイコロ。**正の整数が書かれた 6 面サイコロ 3 個で、すべてが標準のものではなく、合計の分布が標準のサイコロ 3 個と同じになるものは存在するか。（**ヒント：**今度は $(x + \cdots + x^6)^3$ の因数に $1 - x + x^2$ が 3 つ含まれる。）

4 **硬貨と八面体。**$1, \ldots, 8$ と書かれた 8 面サイコロと、1,2 と書かれた 2 面の「サイコロ」（硬貨）がある。合計が同じになるように、これらに別の数を書き直すことはできるか。

さらに学ぶために

- **Martin Gardner, *Penrose Tiles to Trapdoor Ciphers***（Mathematical Association of America）。シッカーマンのサイコロについてのコラムを収録している。
- **Joseph Gallian & David Rusin, 「Cyclotomic polynomials and nonstandard dice」**（円分多項式と非標準的なサイコロ）、*Discrete Mathematics* 27 (1979)。任意の面数のサイコロについての一般論である。
- **Herbert Wilf, *generatingfunctionology***（オンラインで無料公開）、第 1 章。

9.7 等しい累乗和

問題

STEP I 1992、問 5

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/92-s1-q5`

導入

1 から 16 までの数を、8 個ずつの 2 組に分けてみよう：

$$\{1,4,6,7,10,11,13,16\} \quad と \quad \{2,3,5,8,9,12,14,15\}.$$

どちらの組も和は 68 である。平方の和はどちらも 748 である。立方の和はどちらも 9248 である。偶然の一致としか思えないが、実はこれは果てしなく続くパターンの第 3 段階にすぎない。1 から 32 までを正しく分ければ、4 乗の和まで一致するのである。

この分け方は 1851 年に Eugène Prouhet が見つけたもので、その背後にある規則である**トゥエ–モース数列**（Thue–Morse sequence）は、驚くほど多様な場面に現れる。数論、計算理論、チェス、そして交代で物を取るときの最も公平な順番などである。この問題では、ある多項式とその導関数を通してこの数列を掘り起こす。

取りかかる前に

考えてみよう 多項式（polynomial）$\mathrm{p}(x) = \sum c_k x^k$ が $\mathrm{p}(1) = 0$ を満たすとき、係数（coefficient）について何がいえるか。$\mathrm{p}'(1) = 0$ ならばどうか。

$\mathrm{p}(1) = \sum c_k$ であるから、$\mathrm{p}(1) = 0$ は係数の和が 0 であることを意味する。また $\mathrm{p}'(x) = \sum k c_k x^{k-1}$ であるから、$\mathrm{p}'(1) = \sum k c_k$ である。係数がすべて ± 1 ならば、これらの条件は、$+1$ の位置と -1 の位置が同じ個数あり、しかもその和が等しいことを意味する。

順を追って解く

段階 1　三重根

考えてみよう　$1-x^2$ と $1-x^4$ を因数分解せよ。因数（factor）$1-x$ はいくつ現れるか。

$1-x^2=(1-x)(1+x)$ かつ $1-x^4=(1-x)(1+x)(1+x^2)$ であるから、

$$\mathrm{p}_0(x)=(1-x)^3(1+x)^2(1+x^2),$$

となり、$(1-x)^3$ は因数である。 ■

段階 2　1 における導関数の値

考えてみよう　$(1-x)^3$ が p_0 を割り切るとき、$(1-x)$ の何乗が p_0' を割り切るか。さらに $\mathrm{p}_1=x\mathrm{p}_0'$ と p_1' についてはどうか。

$\mathrm{p}_0(x)=(1-x)^3\mathrm{q}(x)$ とおく。積の微分法（product rule）により $\mathrm{p}_0'(x)=-3(1-x)^2\mathrm{q}(x)+(1-x)^3\mathrm{q}'(x)$ であり、これは $(1-x)^2$ を因数にもつ。よって $\mathrm{p}_0'(1)=0$ である。すると $\mathrm{p}_1(x)=x\mathrm{p}_0'(x)$ も $(1-x)^2$ を因数にもち、同じ議論により p_1' は $(1-x)$ を因数にもつ。したがって $\mathrm{p}_1'(1)=0$ である。 ■

段階 3　係数を読み取る

展開すると $(1-x)(1-x^2)=1-x-x^2+x^3$ であり、さらに

$$\mathrm{p}_0(x)=1-x-x^2+x^3-x^4+x^5+x^6-x^7.$$

となる。

考えてみよう　$\mathrm{p}_0'(1)$ と $\mathrm{p}_1'(1)$ を係数 c_k で表すとどうなるか。

$\mathrm{p}_1(x)=x\mathrm{p}_0'(x)=\sum kc_kx^k$ であるから、$\mathrm{p}_1'(1)=\sum k^2c_k$ である。係数は $k=0,3,5,6$ で $+1$、$k=1,2,4,7$ で -1 である。よって $\mathrm{p}_0'(1)=0$ と $\mathrm{p}_1'(1)=0$ は

$$0+3+5+6=1+2+4+7\quad(=14),$$
$$0^2+3^2+5^2+6^2=1^2+2^2+4^2+7^2\quad(=70),$$

を意味し、0 を除けば、これが求める等式である。 ■

段階 4　因数をもう一つ

> **手を止めて、やってみよう** 立方の和まで釣り合わせるには、$(1-x)$ の因数が 4 つ必要である。p_0 の代わりにどの多項式を使えばよいか。

$\mathrm{P}(x)=(1-x)(1-x^2)(1-x^4)(1-x^8)$ をとる。これは $(1-x)^4$ を因数にもつ。その係数は $\mathrm{p}_0(x)-x^8\mathrm{p}_0(x)$ の係数であり、0 から 7 までの符号のパターンに、8 から 15 までの符号を反転させた同じパターンが続く：

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
c_k	+	−	−	+	−	+	+	−	−	+	+	−	+	−	−	+

段階 2 の議論をもう一度適用すれば、$r=0,1,2,3$ に対して $\sum c_k k^r=0$ であることがわかる。+ の位置 $\{0,3,5,6,9,10,12,15\}$ と − の位置 $\{1,2,4,7,8,11,13,14\}$ をとる。$r=1,2,3$ では 0 からの項は 0 なので、除いてよい。よって並べ方

$$a_1,\dots,a_8=1,2,4,7,8,11,13,14,\qquad a_9,\dots,a_{15}=3,5,6,9,10,12,15$$

が条件を満たす。どちらの半分も和は 60、平方の和は 620、立方の和は 7200 である。■

振り返り

- **導関数は重根を検出する。** 因数 $(1-x)^m$ があれば、最初の $m-1$ 個の導関数は $x=1$ で 0 になる。
- **微分する前に x を掛けること**で、$\sum kc_k$ が $\sum k^2c_k$ に変わり、さらに高い冪へと進める。
- **倍化。** 因数 $(1-x^{2^m})$ を一つ加えるごとに長さが 2 倍になり、釣り合う冪が一つ増えた。

背後にある数学

トゥエ–モース数列

$(1-x)(1-x^2)(1-x^4)(1-x^8)\cdots$ の係数の符号は**トゥエ–モース数列**をなす。+ を 0、− を 1 と書くと次のようになる：

$$0\,1\,1\,0\,1\,0\,0\,1\,1\,0\,0\,1\,0\,1\,1\,0\ \dots$$

互いに同値な 3 通りの記述がある。

- **倍化：** 0 から始め、手元の列の補数（complement、0 と 1 を入れ替えたもの）を後ろにつなげることを繰り返す：$0\to 01\to 0110\to 01101001\to\cdots$。

- **2 進数の桁：**第 k 項は、k を 2 進法（binary）で書いたときの 1 の個数が偶数なら 0、奇数なら 1 である。（x^k の符号が $(-1)^{2\text{進表記中の}1\text{の個数}k}$ となるのはこのためである。積から x^k を作るには、k の 2 進表記を構成する因数 x^{2^m} を選ぶことになり、その一つ一つが負の符号をもたらす。）
- **多項式：**問題にあるとおり、$\prod_m (1 - x^{2^m})$ の係数。

$0, 1, \ldots, 2^N - 1$ をトゥエ–モース数列で分けると、$r < N$ を満たすすべての r について r 乗の和が等しい 2 つの集合が得られる（図 9.7.1）。これは *Prouhet–Tarry–Escott* 問題（Prouhet–Tarry–Escott problem）、すなわち $r = 1, \ldots, k$ に対して r 乗の和が等しくなる、異なる 2 つの整数の集合を見つける問題である。Prouhet の解は 2^{k+1} 個の数を使う。本当に必要な数の個数がどこまで少なくできるかは、有名な未解決問題（open problem）である。



$1 + 4 + 6 + 7 + 10 + 11 + 13 + 16 = 68$

$2 + 3 + 5 + 8 + 9 + 12 + 14 + 15 = 68$

平方和：$748 = 748$　　立方和：$9248 = 9248$　　4 乗和：$122\,692 \neq 121\,156$

図 9.7.1　トゥエ–モース数列で分けた 1 から 16 までの数。2 つの集合は和、平方の和、立方の和がそれぞれ等しいが、4 乗の和は等しくない。そのためには 1 から 32 までが必要である。色を左から右へ読むと、青緑–紫–紫–青緑、紫–青緑–青緑–紫、…というパターンになる。

最も公平な交代の仕方

2 人の子どもが、山積みのお菓子から良いものから順に交代で選んでいく。$ABABAB\ldots$ と交互に選ぶと、各ペアで A が常に良い方を取ることになり、系統的に有利になる。$ABBA$ の順の方が公平であり、$ABBABAAB$ はさらに公平である。これがトゥエ–モース数列であり、冪の和が釣り合うことがまさにその理由である。お菓子の価値が位置の滑らかな関数で与えられるとき、その関数を多項式として展開すると、トゥエ–モース順がその主要な項を打ち消すことがわかる。同じ考え方はサッカーの PK 戦（penalty shoot-out）にも提案されており（サッカーの競技規則を定める団体が 2017 年から試行した「$ABBA$」方式）、テニスのタイブレーク（tie-break）におけるサーブの順番にも使われている。

トゥーエ、モース、ユーワ

この数列は何度も発見されてきた。Prouhet は 1851 年にこれを用いた。トゥーエ（Axel Thue）は 1912 年、繰り返しパターンを含まない数列を研究する中でこれを再発見し

た。この数列は同じブロックを 3 回続けて含むことがない（「立方自由」（cube-free）である）。モース（Marston Morse）は 1921 年、曲面上の測地線（geodesic）の研究で再びこれを見いだした。そしてチェスの世界チャンピオンであるマックス・ユーワ（Max Euwe）は 1929 年、これを用いて、当時施行されていた同一局面の繰り返しによる引き分けの規則では無限に長い対局を防げないことを示した。今日では、n の 2 進数の桁を読む単純な機械によって計算される数列である**自動数列**（automatic sequences）の理論における中心的な例となっている。

思考のスキル

組合せ的な性質を多項式に符号化する

幂の和が釣り合うかどうかは、$+$ と $-$ の符号がどこに来るかで決まる。それらの符号を係数とする多項式を考えれば、その性質は根についての命題に変わる。

この問題では探索をする必要がまったくない。$x = 1$ における重根がすべての仕事をしてくれる。組合せ的な対象を試行錯誤で見つけるのではなく代数を使って作り出すことは、大学の組合せ論で繰り返し現れる考え方である。

次の一歩

1. **ずらし。** STEP II 2025、問 8（OCR が配布している 2025 年の過去問一式に収録、`www.ocr.org.uk/Images/750486-2025-past-papers.zip`）に挑戦してみよう。和と平方の和が釣り合う分け方から、一方のリストをずらして組み合わせることで、立方の和まで釣り合うより大きな分け方を作る方法がわかる。

2. **平方数の平方和。**（これも STEP II, 2025 より。）集合 $A = \{1, 3, 4, 5, 9, 11\}$ と $B = \{2, 6, 7, 8, 10\}$ は、和が等しく、平方の和も等しい。すべての正の整数 n について、$\{n^2, (n+1)^2, \ldots, (n+11)^2\}$ を和の等しい 2 つの集合に分けよ。（**ヒント：** 2 つ目の集合に 0 を加えよ。）

3. **平行移動不変性（translation invariance）。** 2 つの数の集合が $r = 0, 1, \ldots, k$ について r 乗の和が等しいならば、すべての要素に同じ数 c を加えて得られる集合もそうであることを示せ。このことから、問題の集合 $\{1, \ldots, 15\}$ を任意の連続する 16 個の整数に置き換えてもよいのはなぜか。

4 **公平なお菓子。**お菓子の価値が $1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{8}$ であるとする。順番 $ABABABAB$ と $ABBABAAB$ のそれぞれについて、A が得る合計を比較せよ。

さらに学ぶために

- **Jean-Paul Allouche & Jeffrey Shallit,「The ubiquitous Prouhet–Thue–Morse sequence」**, *Sequences and Their Applications* 所収（Springer, 1999）。この数列のさまざまな登場場面を概観したサーベイ。オンラインで無料で読める。
- **Matt Parker, *Things to Make and Do in the Fourth Dimension***（Penguin）。冪の和が等しくなる例をはじめ、数にまつわるさまざまな不思議を収める。
- **Joshua Cooper & Aaron Dutle,「Greedy Galois games」**, *American Mathematical Monthly* 120 (2013)。公平な交代とトゥエ–モース数列について。

9.8 誰も自分のシャツを受け取らない

問題

STEP II 2016、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/16-s2-q12`

導入

11 人のサッカーチームが大急ぎで着替え、ユニフォームを無作為につかみ取ったとする。誰ひとり自分のユニフォームを着ていない確率はいくらか。では、それが 50 人の選手団だったら、あるいは 100 万人の群衆だったらどうか。間違える人が増えるのだから確率は上がるのだろうか。それとも、偶然正しいものを取る人も増えるのだから下がるのだろうか。驚くべきことに、確率はほとんど変わらない。5 人以上であれば、その確率は $1/e \approx 0.368$ との差が 0.5 パーセント以内に収まるのである。

これは組合せ確率論（combinatorial probability）における最古の問題であり、1708 年にピエール・ド・モンモール（Pierre de Montmort）が *problème des rencontres*（一致の問題）として提起したものである。本問はこれを**包除原理**（inclusion–exclusion principle）、すなわち重なり合うものを数えるための道具を用いて解く。そしてその答えは、数学において e が現れる最も意外な場面のひとつなのである。

取りかかる前に

手を止めて、やってみよう $n = 3$ の場合を試してみよ。カード 1, 2, 3 の並べ方 6 通りをすべて書き出し、どのカードも自分の位置にないものがいくつあるか数えよ。根気があれば、$n = 4$ の場合も試してみよ（並べ方は 24 通りある）。

$n = 3$ のとき、どのカードも自分の位置にないのは 231 と 312 だけであるから、確率は

$\frac{2}{6} = \frac{1}{3}$ である。$n = 4$ のときは 24 通りのうち 9 通りがそのような並べ方であり、確率は $\frac{3}{8} = 0.375$ となる。どのカードも元の位置にない並べ方を**完全順列**（derangement）という。

順を追って解く

段階 1　3 つの事象に対する包除原理

> **考えてみよう**　2 つの事象に対する公式が使えるように、$A \cup B \cup C$ を 2 つの事象の和として表すにはどうすればよいか。

$A \cup B$ をひとつの事象とみなし、それと C に公式を適用すると

$$\mathrm{P}(A \cup B \cup C) = \mathrm{P}(A \cup B) + \mathrm{P}(C) - \mathrm{P}((A \cup B) \cap C).$$

ここで $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ であり、公式をもう一度適用すると $\mathrm{P}((A \cap C) \cup (B \cap C)) = \mathrm{P}(A \cap C) + \mathrm{P}(B \cap C) - \mathrm{P}(A \cap B \cap C)$ となる。$\mathrm{P}(A \cup B)$ も展開して項を整理すれば、結果が得られる。 ■

4 つの事象についても同じパターンが続く。4 つの単独の確率を足し、6 つの 2 つずつの共通部分を引き、4 つの 3 つずつの共通部分を足し、最後に $\mathrm{P}(A \cap B \cap C \cap D)$ を引けばよい。

段階 2　各確率

> **考えてみよう**　カード i が位置 i にあるとき、残りのカードの並べ方は何通りあるか。カード i と j がともに固定されているときはどうか。

並べ方は全部で $n!$ 通りあり、どれも同様に確からしい。カード i が位置 i に固定されているとき、他の $n-1$ 枚のカードはどのような順でもよいから、$(n-1)!$ 通りである。したがって

$$\mathrm{P}(E_i) = \frac{(n-1)!}{n!} = \frac{1}{n}, \qquad \mathrm{P}(E_i \cap E_j) = \frac{(n-2)!}{n!} = \frac{1}{n(n-1)},$$
$$\mathrm{P}(E_i \cap E_j \cap E_k) = \frac{(n-3)!}{n!} = \frac{1}{n(n-1)(n-2)}.$$

一般に、指定された k 枚のカードがすべて自分の位置にある確率は $\frac{(n-k)!}{n!}$ である。

段階 3　足し合わせる

> **考えてみよう** $\mathrm{P}(E_1 \cup \cdots \cup E_n)$ に対する包除原理の式において、k 個の事象の共通部分を含む項はいくつあり、その合計はいくらか。

k 個の事象の選び方は $\binom{n}{k}$ 通りあり、それぞれの共通部分の確率は $\frac{(n-k)!}{n!}$ である。よって k 重の項の合計は

$$\binom{n}{k}\frac{(n-k)!}{n!} = \frac{n!}{k!\,(n-k)!}\cdot\frac{(n-k)!}{n!} = \frac{1}{k!}.$$

$k!$ 以外はすべて約分される。符号を交互につけると

$$\mathrm{P}(\text{少なくとも 1 枚のカードが自分の位置にある}) = 1 - \frac{1}{2!} + \frac{1}{3!} - \cdots + (-1)^{n+1}\frac{1}{n!}. \qquad \blacksquare$$

したがって、完全順列となる確率は

$$d_n = 1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n\frac{1}{n!} = \sum_{k=0}^{n}\frac{(-1)^k}{k!}.$$

段階 4 ちょうど 1 枚

> **考えてみよう** ちょうど 1 枚のカードが自分の位置にあるとき、それはどのカードであり、他のカードはどうなっていなければならないか。

自分の位置にあるカードを選ぶ（n 通り）。カード i が自分の位置にある確率は $\frac{1}{n}$ であり、そのもとで残りの $n-1$ 枚のカードはそれらの間で完全順列をなさなければならず、その確率は d_{n-1} である。したがって

$$\mathrm{P}(\text{ちょうど 1 枚}) = n\cdot\frac{1}{n}\cdot d_{n-1} = \sum_{k=0}^{n-1}\frac{(-1)^k}{k!}. \qquad \blacksquare$$

振り返り

- **数えすぎてから修正する。** $\mathrm{P}(E_i)$ を足し合わせると、2 枚のカードが固定された並べ方は 2 回数えられる。2 つずつの組を引けばこれは修正されるが、3 つずつの組については引きすぎになる。以下同様である。
- **対称性により項が等しくなる。** k 重の共通部分はどれも同じ確率をもつので、公式の各層はひとつの数と二項係数（binomial coefficient）の積になる。
- **より小さな場合に帰着させる。**「ちょうど 1 枚」は $n-1$ 枚のカードの完全順列の問題になった。

背後にある数学

e はどこから来るのか

級数 $\sum(-1)^k/k!$ は、指数級数（exponential series）$e^x = \sum x^k/k!$ に $x = -1$ を代入したものである。したがって $n \to \infty$ のとき

$$d_n \to e^{-1} \approx 0.3679,$$

となり、ちょうど 1 枚が一致する確率も同じ極限に近づく。この収束は驚くほど速い（図 9.8.1）。$1/n!$ の項で打ち切ったときの誤差は $1/(n+1)!$ より小さいので、$n = 7$ の時点ですでに答えは小数第 4 位まで $1/e$ と一致する。実際、n 個の対象の完全順列の個数 $n!\,d_n$ は、$n!/e$ に最も近い整数にちょうど等しい。

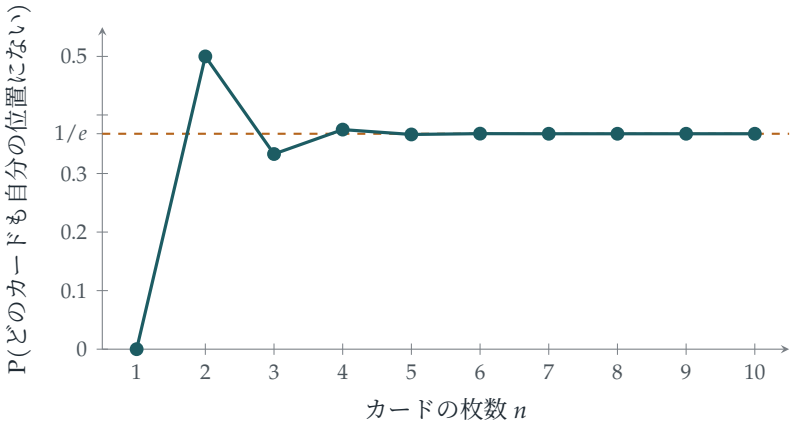


図 9.8.1　n 枚のカードを無作為に並べ替えたとき、どのカードも自分の位置にない確率。値は $1/e$ の上下を交互に行き来し、$n = 6$ 以降はこの縮尺では $1/e$ と区別がつかない。

一致の個数はポアソン分布に従う

さらに多くのことが成り立つ。自分の位置にあるカードの枚数を N とする。このとき各 k について $\mathrm{P}(N = k) \to \frac{e^{-1}}{k!}$ となる。すなわち、一致の個数は極限において平均 1 の**ポアソン分布**（Poisson distribution）に従う。平均が 1 である理由は計算なしでもわかる。N は $E_1, \ldots, E_n$ の指示変数（indicator variable）の和であり、それぞれの期待値（expectation）は $\frac{1}{n}$ である。そして事象が独立（independent）でなくても期待値は加法的である。STEP III 2004 Q12（演習問題を参照）では、分散（variance）も 1 であることを示す。ポアソン分布は、起こりにくい事象がほぼ独立に多数あるときに必ず現れる。完全順列はその古典的な例であり、第 12 章の Section 12.11 の主題でもある。

モンモールの *treize* ゲーム

フランスの貴族ピエール・レモン・ド・モンモール（Pierre Rémond de Montmort）は、著書 *Essay d'analyse sur les jeux de hazard*（『偶然のゲームに関する解析の試論』、1708 年）で賭けごとを研究した。*treize*（13）というゲームでは、プレイヤーが「1、2、3、…」と数を唱えながら 13 枚のカードを配り、配ったカードが唱えた数と一度でも一致すれば勝ちとなる。モンモールは勝つ確率を求め、ニコラウス・ベルヌーイ（Nicolaus Bernoulli）との書簡のやりとりを通じて、1713 年までに一般的な公式が確立された。オイラー（Euler）は 1753 年にこれを再発見した。包除原理はその後、ド・モアブル（Abraham de Moivre）によって、また一般的な形では 19 世紀にシルベスター（James Joseph Sylvester）によって定式化された。

思考のスキル

包除原理

重なり合う集合の和集合の要素を数えるには、各集合の大きさを足し、2 つずつの重なりを引き、3 つずつの重なりを足し、以下同様に続ければよい。

本問のように、対称性によって同じ大きさの重なりがすべて等しくなるとき、最も威力を発揮する。大学では、組合せ論（combinatorics）、確率論、そして整数論（number theory）で現れる。整数論では、与えられた素数のどれでも割り切れない整数を数えるのに使われ、オイラーのトーシェント関数（Euler's totient function）やメビウス関数（Möbius function）につながる。

次の一歩

1 **ユニフォーム。** STEP III 2004、問 12（`step.maths.org/questions/04-s3-q12`）に挑戦せよ。この問題では、自分のユニフォームを着ている選手の人数を指示変数を用いて数え、平均と分散を求め、その結果をポアソン分布と比較する。

2 **漸化式。** n 個の対象の完全順列の個数を D_n とする。カード 1 がどこへ行くか、そしてその位置にあったカードが位置 1 へ行くかどうかを考えることにより、漸化式（recurrence）$D_n = (n-1)(D_{n-1} + D_{n-2})$ を示せ。$D_3 = 2$、$D_4 = 9$ と照らし合わせて確かめよ。

3 **ちょうど k 枚。** ちょうど k 枚のカードが自分の位置にある確率は $\frac{1}{k!}d_{n-k}$ であり、それが $\frac{e^{-1}}{k!}$ に近づくことを示せ。

4 **互いに素な整数。** 包除原理を用いて、1 から 30 までの整数のうち 2、3、5 のいずれでも割り切れないものの個数を求めよ。その答えは $30\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$ とどのような関係にあるか。

さらに学ぶために

- **Geoffrey Grimmett & Dominic Welsh, *Probability: An Introduction***（Oxford University Press）。包除原理と一致の問題を扱う大学 1 年生向けの教科書。
- **William Feller, *An Introduction to Probability Theory and Its Applications*, Vol. 1**（Wiley）、第 IV 章。一致の問題のさまざまな変形を収めた古典。
- **Miklós Bóna, *A Walk Through Combinatorics***（World Scientific）。包除原理について。

9.9 誕生日問題

問題

STEP II 2007、問 13

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/07-s2-q13`

導入

部屋に何人いれば、その中の誰か 2 人の誕生日が一致する確率（probability）が半分を超えるだろうか。多くの人は 365 の半分の 180 前後と予想する。答えは 23 である。30 人のクラスなら誕生日が一致する組がある確率は 70%、50 人のパーティーなら 97% になる。

この意外さは、2 つの異なる問いを混同することから生じる。「**自分と**同じ誕生日の人はいるか」（こちらは確かに約 253 人が必要である）と、「**誰か 2 人の**誕生日が一致するか」である。23 人いれば組は $\binom{23}{2} = 253$ 通りあり、どの組も一致する可能性をもつ。この問題はその直観を厳密なものにする。そして同じ数学が、銀行口座を守る暗号（cryptography）の安全性を決めているのである。

取りかかる前に

考えてみよう どの 2 人の客も誕生日が一致しない確率の方が計算しやすいのはなぜか。客を一列に並べてみよ。2 人目が 1 人目の誕生日を避ける確率はいくらか。3 人目がその 2 人の誕生日をともに避ける確率はどうか。

「少なくとも 2 人が一致する」には、互いに重なり合う多くの場合が含まれる（2 人が一致する、3 人が一致する、異なる 2 組がそれぞれ一致する、...）。その余事象（complement）である「全員異なる」は、ただ 1 つのすっきりした事象である。2 人目が 1 人目の誕生日を避ける確率は $\frac{364}{365}$ であり、そのもとで 3 人目が 2 人の誕生日をともに避ける確率は $\frac{363}{365}$ である。以下同様である。

順を追って解く

段階 1　有用な近似

考えてみよう　$x=0$ における $y=e^{-x}$ の接線（tangent line）は何か。

$e^{-x}=1-x+\frac{x^2}{2}-\cdots$ であるから、x が小さいとき $e^{-x}\approx 1-x$ である。$x=r/n$ とおくと、

$$\frac{n-r}{n}=1-\frac{r}{n}\approx e^{-r/n}. \qquad \blacksquare$$

誤差はおよそ $\frac{r^2}{2n^2}$ であり、r が n よりずっと小さければ小さい。

段階 2　誕生日が一致する確率

k 人の誕生日がすべて異なる確率は

$$\frac{365}{365}\cdot\frac{364}{365}\cdot\frac{363}{365}\cdots\frac{365-(k-1)}{365}=\prod_{r=0}^{k-1}\frac{365-r}{365}.$$

である。各因数にこの近似を用い、指数関数の積は指数の和になることを使うと、

$$\prod_{r=0}^{k-1}e^{-r/365}=\exp\!\left(-\frac{0+1+\cdots+(k-1)}{365}\right)=\exp\!\left(-\frac{k(k-1)}{730}\right).$$

よって、誕生日が一致する組が少なくとも 1 つある確率は近似的に $1-e^{-k(k-1)/730}$ である。 $\blacksquare$

考えてみよう　指数に注目せよ。$\frac{k(k-1)}{730}=\binom{k}{2}\Big/365$ である。これは言葉で言うと何を意味するか。

これは客の組の数に、ある特定の組の誕生日が一致する確率 $\frac{1}{365}$ を掛けたもの、すなわち一致する組の数の期待値（expected number）である。この近似は、一致がない確率が $e^{-(\text{一致の個数の期待値})}$ であることを述べており、Section 9.8 と同様に、ここにもポアソン分布（Poisson distribution）の気配が現れている。

段階 3　23 人

$1-e^{-k(k-1)/730}\ge\frac{1}{2}$、すなわち $e^{-k(k-1)/730}\le\frac{1}{2}$ となる必要があるから、

$$\frac{k(k-1)}{730}\ge\ln 2\approx\frac{253}{365},\qquad\text{すなわち}\qquad k(k-1)\ge 506.$$

$22\times 21=462$、$23\times 22=506$ であるから、最小の値は $k=23$ である。 $\blacksquare$

（客が 23 人のときの正確な確率は 0.507、22 人のときは 0.476 であるから、この近似は正しい答えを与えている。）

段階 4 主催者と誕生日が一致する場合

> **考えてみよう** 各客について、主催者と誕生日が一致しない確率はいくらか。この点に関して、客どうしは互いに独立であるか。

各客は独立に確率 $\frac{364}{365} \approx e^{-1/365}$ で主催者の誕生日を外す。よって k 人の客の誰も主催者と誕生日が一致しない確率は $\left(\frac{364}{365}\right)^k \approx e^{-k/365}$ であり、

$$e^{-k/365} \le \tfrac{1}{2}, \qquad \text{すなわち} \qquad k \ge 365 \ln 2 \approx 253.$$

が必要である。したがって客は 253 人必要である。 ■

この対比こそが要点である。特定の 1 人と一致させるには 253 人の客が必要だが、どこかの組が一致するには 23 人で足りる。23 人いれば 253 組ができるからである。

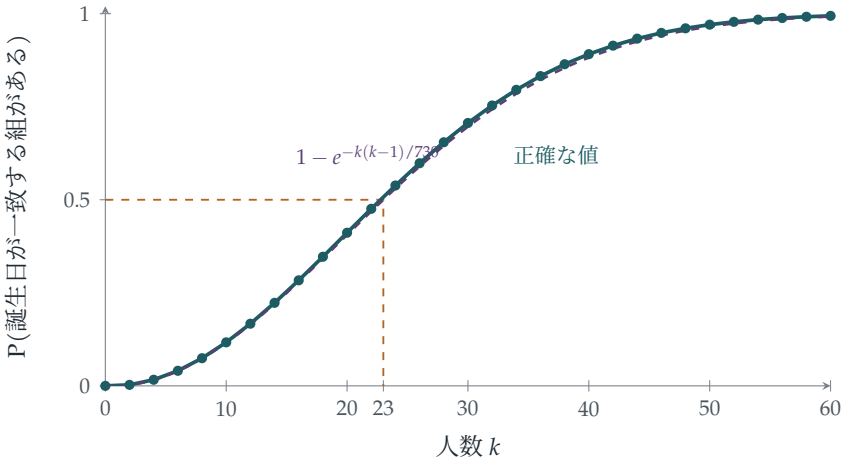


図 9.9.1 k 人のうち少なくとも 2 人の誕生日が一致する確率。正確な値（ティール）と近似 $1 - e^{-k(k-1)/730}$（プラム、破線）。両者は非常に近く、どちらも $k = 22$ と $k = 23$ の間で $\frac{1}{2}$ を超える。

振り返り

- **余事象を使う。**「全員異なる」はただ 1 つの積であったが、「少なくとも 1 組一致する」は煩雑であった。
- **線形化（linearise）してから指数関数にする。**各因数 $1 - x$ を e^{-x} で置き換えることで、積が和に変わった。

- **組を数える。** 指数は、組の数に 1 組が一致する確率を掛けたものであった。$k(k-1)$ に現れる 2 乗こそが、このパラドックス（paradox）の説明のすべてである。

背後にある数学

平方根則

365 の代わりに、等確率な n 個の日があるとすると、同じ議論から

$$\mathrm{P}(\text{一致がある、人数}k) \approx 1 - e^{-k^2/(2n)},$$

が得られる。よって一致が起こりやすくなるのは、k が n ではなく $\sqrt{n}$ 程度になったときである。より正確には、確率が $\frac{1}{2}$ に達するのは $k \approx 1.18\sqrt{n}$ のときであり、最初の重複が起こるまでに出会う必要のある人数の期待値は約 $\sqrt{\pi n/2}$ である（$n = 365$ なら約 24.6）。この**平方根則**（square-root law）こそが、偶然の一致がこれほどありふれている理由である。大量の出来事の集まりの中では、特定の一致はどれも起こりにくいにもかかわらず、何らかの組が何らかの形で一致する可能性は高いのである。

誕生日攻撃

コンピュータは、ファイルが改ざんされていないことを**ハッシュ**（hash）を計算して確認する。ハッシュとは、たとえば $n = 2^{128}$ 通りの値をとる指紋のようなものである。同じハッシュをもつ 2 つの文書（無害な契約書と不正な契約書）を作りたい偽造者は、2^{128} 個の文書を試す必要はない。誕生日の議論により、それぞれの変種を約 $\sqrt{2^{128}} = 2^{64}$ 個ずつ生成すれば、おそらく一致が見つかる。この**誕生日攻撃**（birthday attack）があるために、現代のハッシュ関数は 256 ビット以上を用いる。平方根則によってビット数の半分が失われるからである。同様の計算により、2 台のコンピュータが偶然同じものを選ぶことが決してないようにするには、ランダムな識別子をどれだけ長くすべきかも決められる。

最初に問うたのは誰か

誕生日問題（birthday problem）は通常、1939 年にこれを論じたリヒャルト・フォン・ミーゼス（Richard von Mises）に帰せられるが、それ以前から知られていた。Harold Davenport もそれ以前にこれを知っていたが、あまりに簡単に思えたので発表しなかったと言われている。Warren Weaver の語るところによれば、彼は第二次世界大戦中、陸軍将校たちとの夕食会でこれを実演するのを好んだ。その場にいた 22 人のうち 2 人の誕生日が一致するほうに賭けて負けたが、そのときウェイトレスが、自分の誕生日が将校の 1 人と同じであることを明かしたという。

思考のスキル

余事象を計算し、注意深く近似する

「少なくとも *1* つ」が複雑なときは、「*1* つもない」確率を求めよ。積が扱いにくいときは、各因数を指数関数で近似し、指数を足し合わせよ。

どちらの手法も大学では標準的なものである。2 つ目の $1 - x \approx e^{-x}$ は、ポアソン近似の理論や、正確に計算するには複雑すぎる量を見積もるための漸近的手法（asymptotic methods）の出発点である。

次の一歩

1. **最初の重複。** STEP II 2014、問 13（`step.maths.org/questions/14-s2-q13`）に挑戦せよ。乱数生成器から最初に重複して現れる値を調べる問題で、形を変えた誕生日問題である。その確率から 2 つの意外な恒等式が導かれる。

2. **3 人が一致。** 誰か 3 人の誕生日が一致する確率が半分を超えるには、おおよそ何人必要か。（ヒント：誕生日が一致する 3 人組の個数の期待値は $\binom{k}{3}/365^2$ である。これを約 $\ln 2$ とおけ。）真の答えは 88 である。

3. **ニアミス。** 2 人の誕生日が同じ日または隣り合う日である確率が半分になるには、何人必要か。

4. **偏りのある誕生日。** 現実の誕生日は一様ではない。各日の確率が $p_1, \dots, p_{365}$ であるとき、2 人の誕生日が一致する確率は $\sum p_i^2$ であり、これはすべての p_i が等しいときに最小となることを示せ。（よって一様でないことは、一致をより起こりやすくするだけである。）

さらに学ぶために

- **William Feller, *An Introduction to Probability Theory and Its Applications*, Vol. 1**（Wiley）、第 II 章。誕生日問題とその近似。
- **Persi Diaconis & Frederick Mosteller, “Methods for studying coincidences”**, *Journal of the American Statistical Association* 84 (1989)。偶然の一致がありふれている理由。非常に読みやすい。
- **David Hand, *The Improbability Principle***（Bantam）。平方根則をはじめ、起こりそう

にないことが絶えず起こる理由を解説する。

9.10 いつでもおつりを渡せる

問題

STEP I 2011、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/11-s1-q12`

導入

$\frac{m}{m+1}$、$\frac{m-1}{m+1}$、$\frac{m-2}{m+1}$ という規則性は見過ごせない。£2 硬貨を持つ人が n 人いれば、答えはきっと $\frac{m-n+1}{m+1}$ だろう。実際そのとおりであり、最も鮮やかな証明は組合せ論の中でも屈指の美しいアイデア、すなわち**鏡像原理**（reflection principle）による。これは、図の一部を直線に関して折り返すことで、難しい数え上げ（釣り銭が途中で尽きない列の個数）を易しい数え上げに変えてしまう方法である。

この問題はさまざまな姿で現れる。勝者が一度も相手に後れをとらない開票（1887 年のベルトラン（Bertrand）の投票問題）、決して破産しない賭博者、正しく対応する括弧などである。$m = n$ のとき、この数え上げは**カタラン数**（Catalan numbers）を与える。カタラン数は、組合せ論において二項係数（binomial coefficients）に次いで最もよく現れる数列といってよいだろう。

取りかかる前に

考えてみよう £1 の客が来るたびに硬貨が 1 枚増え、£2 の客が来るたびに（釣り銭として）1 枚減る。行き詰まるのはどのようなときか。

手元にある £1 硬貨の枚数を追っていく。この枚数は £1 の客ごとに 1 増え、£2 の客ごとに 1 減る。行き詰まるのは、ちょうど硬貨を 1 枚も持っていないときに £2 の客が来た場合であり、このとき枚数は -1 になってしまう。したがって、成功するための必要十分条件は、列のどの時点においても、それまでの £1 の客の人数がそれまでの £2 の客の人数以上であることである。

順を追って解く

段階 1　£2 硬貨が 1 枚の場合

$n = 1$ のとき、失敗するのは £2 の客が先頭にいる場合に限る。£2 の客は $m+1$ 個の位置のどこにも等確率でいるから、

$$\mathrm{P}(\text{成功}) = 1 - \frac{1}{m+1} = \frac{m}{m+1}. \qquad \blacksquare$$

段階 2　£2 硬貨が 2 枚の場合

考えてみよう　先頭の人は £1 硬貨を持っていなければならない。2 番目の人については何が起こりうるか。また、それぞれの場合にどのような状況が残るか。

先頭の人が £1 硬貨を持っている確率は $\frac{m}{m+2}$ であり、そうでなければその場で失敗する。先頭が £1 なら手元に硬貨が 1 枚あり、残りの列には £1 の人が $m-1$ 人、£2 の人が 2 人いる。

- 2 番目の人が £1 硬貨を持っている場合（確率 $\frac{m-1}{m+1}$）、手元の硬貨は 2 枚になり、2 枚の £2 硬貨がいつ来ても釣り銭を渡せる。成功は確実である。
- 2 番目の人が £2 硬貨を持っている場合（確率 $\frac{2}{m+1}$）、手元の硬貨は 0 枚に戻り、£1 の人が $m-1$ 人、£2 の人が 1 人残る。小問 (i) で m を $m-1$ に置き換えれば、成功する確率は $\frac{m-1}{m}$ である。

よって

$$\mathrm{P}(\text{成功}) = \frac{m}{m+2}\left(\frac{m-1}{m+1} + \frac{2}{m+1}\cdot\frac{m-1}{m}\right) = \frac{m}{m+2}\cdot\frac{m-1}{m+1}\cdot\frac{m+2}{m} = \frac{m-1}{m+1}. \qquad \blacksquare$$

手を止めて、やってみよう　同じ方法を $n = 3$ で試してみよ。うまくいくが、場合分けが膨れ上がる。成功する列を一度にまとめて数える方法はないだろうか。

段階 3　列を経路として見る

考えてみよう　対応した人数に対して手元の硬貨の枚数をグラフに描いてみよ。列はどのような図になるか。成功する列はどのような図になるか。

列は、m 個の上り段（£1）と n 個の下り段（£2）からなり、高さ 0 から始まって高さ $m-n$ で終わる経路である。このような経路は $\binom{m+n}{n}$ 個あり、どれも等確率である。列が成功するのは、その経路が一度も 0 より下に行かないときに限る。したがって、数えるべきは**悪い**経路、すなわち高さ -1 に触れる経路である。

段階 4 折り返し

> **考えてみよう** 悪い経路を 1 つとる。それが初めて -1 に触れる時点を見つけ、その時点**より前**の部分を直線 $y=-1$ に関して折り返せ。新しい経路はどこから始まり、どこで終わるか。

折り返した経路は -2（直線 $y=-1$ に関する 0 の鏡像）から始まり、元の経路と同じ $m-n$ で終わる（図 9.10.1）。逆に、-2 から $m-n$ へ向かうどの経路も、どこかで必ず $y=-1$ を横切る（$m \geq n$ より、下から始まって上で終わるからである）。初めて $y=-1$ に達するまでの部分を折り返せば、0 から始まる悪い経路に戻る。したがって、0 から始まる悪い経路は、-2 から $m-n$ へ向かう**すべての**経路とちょうど 1 対 1 に対応する。

-2 から $m-n$ へ $m+n$ 段で進む経路は $m-n+2$ だけ上昇するから、上り段が $m+1$ 個、下り段が $n-1$ 個である。このような経路は $\binom{m+n}{n-1}$ 個ある。ゆえに

$$\mathrm{P}(\text{失敗}) = \frac{\binom{m+n}{n-1}}{\binom{m+n}{n}} = \frac{n!\,m!}{(n-1)!\,(m+1)!} = \frac{n}{m+1},$$

であり、

$$\mathrm{P}(\text{成功}) = 1 - \frac{n}{m+1} = \frac{m-n+1}{m+1}.$$

$n=3$ のとき、これは $\frac{m-2}{m+1}$ である。 ■

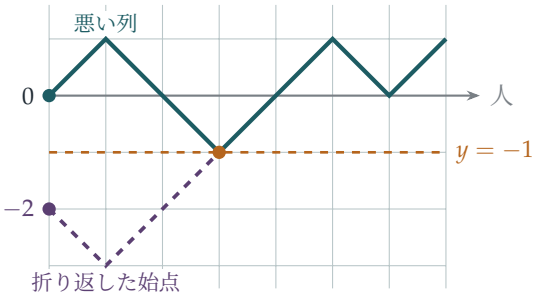


図 9.10.1 £1 硬貨が $m=4$ 枚、£2 硬貨が $n=3$ 枚の列を経路として描いたもの（ティール）。この経路は 3 人目（アンバー）で初めて -1 に達し、そこで釣り銭が渡せなくなる。その点までの経路を直線 $y=-1$ に関して折り返すと、-2 から同じ終点へ向かう経路（プラム、破線）が得られる。悪い列と -2 から始まる経路とのこの対応が鏡像原理である。

振り返り

- **適切な状態を見つける。**意味をもつのは手元の硬貨の枚数だけであり、これによって列が経路（歩み）に変わった。
- **最初の数歩で条件づける。**小問 (i) と (ii) は、最初の数人がどうするかを考えて、より小さな場合に帰着させることで解いた。
- **全単射で余事象を数える。**悪い経路を直接数えるのは難しかったが、折り返しによって、数えやすい集合と全単射（bijection）で対応づけることができた。

背後にある数学

カタラン数

$m = n$（£1 硬貨がぎりぎり足りる場合）のとき、成功する列の個数は

$$\binom{2n}{n} - \binom{2n}{n-1} = \frac{1}{n+1}\binom{2n}{n},$$

であり、これは第 n **カタラン数** C_n：$1, 1, 2, 5, 14, 42, 132, \ldots$ である。リチャード・スタンレー（Richard Stanley）の著書 *Catalan Numbers* には、カタラン数が数える対象が 200 以上も挙げられている。その中には、n 組の括弧を正しく並べる方法の数（「(())()」はよいが「())(()」はだめである。これは「(」を £1、「)」を £2 とみれば硬貨の議論そのものである）、$n+2$ 角形を互いに交わらない対角線で三角形に分割する方法の数、$n+1$ 個の因数の積に括弧をつける方法の数などがある。

ランダムウォーク

列はランダムウォーク（random walk）であり、鏡像原理はランダムウォークを調べるための基本的な道具の 1 つである。たとえば鏡像原理から、0 から出発する公平なランダムウォークはいつか必ず 0 に戻ること、また最初の $2n$ 歩の間ずっと正であり続ける確率が $\frac{1}{2}\binom{2n}{n}2^{-2n} \approx \frac{1}{2\sqrt{\pi n}}$ であることがわかる。連続版では、同じ折り返しの議論を**ブラウン運動**（Brownian motion）に適用すると、その最大値の分布が得られる。これは、株価がある障壁を一度でも越えるかどうかで支払いが決まる、ある種の金融オプションの価格づけの基礎になっている。

ベルトランの投票問題

1887 年、ジョゼフ・ベルトラン（Joseph Bertrand）は次の問いを立てた。候補者 A が a 票、B が $b < a$ 票を得る選挙において、開票の間ずっと A が真に B をリードし

ている確率はいくらか。答え $\frac{a-b}{a+b}$ は同じ年にデジレ・アンドレ（Désiré André）によって証明され、その議論は通常、鏡像原理として記憶されている（ただし歴史家たちは、アンドレの実際の証明は少し異なる全単射を用いていたと指摘している）。本問のくじ引きの問題は、同点を許す変形版である。すなわち成功とは、£1 の人数が £2 の人数を一度も**下回らない**ことである。演習問題の 1 つで、ベルトランの答えを本問の答えから導く。

思考のスキル

全単射による数え上げ

ある集合の要素を数えるには、数えられる集合との *1* 対 *1* 対応を見つけよ。

折り返しによって、悪い列を、別の始点から出発する制約のない経路と対応づけた。全単射による証明は組合せ論で最も満足感のある証明である。2 つの数が等しいことを単に示すだけでなく、**なぜ**等しいのかを説明してくれるからである。大学では組合せ論のいたるところで全単射による証明に出会い、ランダムウォークやブラウン運動の研究で再び鏡像原理に出会うだろう。

次の一歩

1. **3 枚の場合を場合分けで。** 小問 (ii) と同様に、列の最初の数人で条件づけて小問 (iii) を証明せよ。鏡像原理がどれほどの手間を省いてくれるかがわかるだろう。

2. **ベルトランの投票問題。** ある選挙で A は a 票、B は $b < a$ 票を得る。開票の間ずっと A が真にリードしている確率が $\frac{a-b}{a+b}$ であることを示せ。（**ヒント**：最初の 1 票は A でなければならない。その後、A が B に後れをとる差は決して…を超えてはならない。）

3. **括弧。** 3 組の括弧の正しい並べ方 5 通りと、五角形を三角形に分割する方法 5 通りをすべて書き出せ。両者の間の全単射を見つけられるか。

4. **£5 紙幣。** 価格 £1 のチケットを買う列に、£1 硬貨を持つ人が m 人、£5 紙幣を持つ人が n 人いる。鏡像原理ではもはや簡単な答えが得られない理由を説明せよ。（この一般化ははるかに難しい。）

さらに学ぶために

- **ウィリアム・フェラー（William Feller）, *An Introduction to Probability Theory and Its Applications*, Vol. 1**（Wiley）、第 III 章。ランダムウォークと鏡像原理についての古典的な解説。
- **Richard Stanley, *Catalan Numbers***（Cambridge University Press）。200 を超える解釈を演習問題とともに収録。
- **Marc Renault,「Lost (and found) in translation: André's actual method and its application to the generalized ballot problem」**, *American Mathematical Monthly* 115 (2008)。鏡像原理の歴史。

9.11 全種類を集める

問題

STEP II 1994、問 13

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/94-s2-q13`

導入

あるサッカーのステッカーアルバムには集めるべきステッカーが 600 種類あり、ステッカーは 1 枚ずつ無作為に売られている。アルバムを埋めるには、何枚買うことを見込めばよいだろうか。最初の数百枚はすぐに集まる。ほとんどすべてのステッカーが新しいからである。しかしアルバムが埋まってくるにつれて新しいステッカーは出にくくなり、最後の 1 枚だけで平均 600 回の購入が必要になる。合計はおよそ 4200 枚、アルバムの大きさの 7 倍にもなる。

これが**クーポン・コレクター問題**（coupon collector's problem）である。その答えは二つの考え方を組み合わせたものである。一つは成功するまでの待ち時間であり、もう一つは調和級数（harmonic series）$1 + \frac{1}{2} + \frac{1}{3} + \cdots$ で、これは $\ln n$ のように増大する。調和級数が発散（diverge）することは Section 2.3 で見た。ここでは、その増え方の遅さこそが、コレクションを完成させるために支払う代価となる。

取りかかる前に

? **考えてみよう** 各袋がそれぞれ独立に確率 p で新しいカードをくれるとき、最初の新しいカードが出るまで（その袋を含めて）開ける袋の数の期待値（expectation）はいくらか。

袋の数 X は**幾何分布**（geometric distribution）に従う：$\mathrm{P}(X = k) = (1-p)^{k-1}p$。その期待値は $\frac{1}{p}$ である。（これをすばやく確かめる一つの方法：$\mathrm{E}(X) = 1 + (1-p)\mathrm{E}(X)$。1 袋開けると、確率 $1-p$ で振り出しに戻るからである。）新しいカードが 3 回に 1 回

出るなら、3 袋待つことが見込まれる。

順を追って解く

段階 1　新しいカードを待つ

すでに r 種類の異なるカードを持っているとき、1 袋から新しいカードが出る確率は、それまでの袋とは独立に $\frac{n-r}{n}$ である。したがって、次の新しいカードが出るまでの袋の数の期待値は

$$\frac{1}{(n-r)/n} = \frac{n}{n-r}. \qquad \blacksquare$$

段階 2　和と積分を比べる

> **考えてみよう**　区間 $r \le x \le r+1$ において、$\frac{1}{x}$ はどの二つの値の間にあるか。それは曲線の下の面積について何を教えてくれるか。

$\frac{1}{x}$ は減少関数なので、$[r, r+1]$ 上で $\frac{1}{r+1} \le \frac{1}{x} \le \frac{1}{r}$ である。長さ 1 の区間で積分すると

$$\frac{1}{r+1} \le \int_{r}^{r+1} \frac{\mathrm{d}x}{x} \le \frac{1}{r}. \qquad \blacksquare$$

図で見ると（図 9.11.1）、曲線の下の面積は、高さ $\frac{1}{r+1}$ の長方形と高さ $\frac{1}{r}$ の長方形の間に挟まれている。これらを $r = 1$ から $r = n-1$ まで足し合わせると、積分はつながって $\int_1^n \frac{\mathrm{d}x}{x} = \ln n$ となり、したがって

$$\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \le \ln n \le 1 + \frac{1}{2} + \cdots + \frac{1}{n-1}. \qquad \blacksquare$$

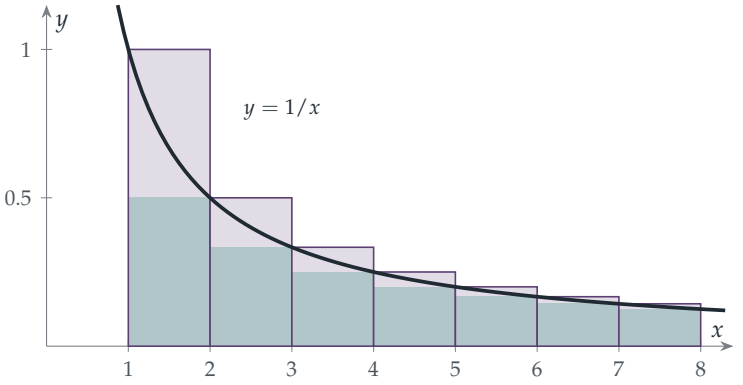


図 9.11.1　各区間 $[r, r+1]$ において、$y = 1/x$ の下の面積は、ティール色の長方形（高さ $\frac{1}{r+1}$）と、それより大きいプラム色の長方形（高さ $\frac{1}{r}$）の間にある。足し合わせると、$\ln n$ は $\frac{1}{2} + \cdots + \frac{1}{n}$ と $1 + \frac{1}{2} + \cdots + \frac{1}{n-1}$ の間にある。曲線とプラム色の長方形の間の隙間を合計すると有限の値になる。それがオイラーの定数（Euler's constant）$\gamma \approx 0.577$ である。

段階 3　セットを完成させる

考えてみよう　袋の総数は、最初のカード、2 枚目の新しいカード、……のそれぞれを待つ時間の和である。その期待値はいくらか。

r 種類の異なるカードから $r+1$ 種類になるまでに必要な袋の数を X_r とする。総数は $X_0 + X_1 + \cdots + X_{n-1}$ であり、期待値は足し合わせられるので、

$$\mathrm{E}(\text{総数}) = \sum_{r=0}^{n-1} \frac{n}{n-r} = n\left(\frac{1}{n} + \frac{1}{n-1} + \cdots + 1\right) = nH_n,$$

ここで $H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$ は第 n **調和数**（harmonic number）である。段階 2 より $\ln n + \frac{1}{n} \le H_n \le \ln n + 1$ なので、n が大きいとき H_n はおよそ $\ln n$ であり、私が食べることになると見込まれるのはおよそ

$$n \ln n \text{ 袋.} \qquad \blacksquare$$

振り返り

- **長い待ち時間を段階に分ける。**全体の時間は n 個の待ち時間に分かれ、そのそれぞれは単純な幾何分布型であった。
- **期待値は加法的である。**総数の分布は一度も必要とせず、各部分の期待値だけで済んだ。

- **和を積分と比べる。**図によって、値を求められない和が、誤差高々 1 の対数に置き換わった。

背後にある数学

この評価はどれほど良いか

この比較はさらに精密にできる。図 9.11.1 において曲線と上側の長方形の間にある影の付いた隙間は、面積の合計が有限なので、$H_n - \ln n$ はある極限に収束（converge）する。

$$\gamma = \lim_{n\to\infty}(H_n - \ln n) = 0.5772156649\ldots,$$

これが**オイラーの定数**である。（γ が有理数かどうかは誰も知らない。）したがって袋の数の期待値は $n\ln n + \gamma n + \frac{1}{2} + \cdots$ である。600 種類のステッカーアルバムでは $600 \times (\ln 600 + 0.577) \approx 4185$ となり、これが導入で挙げた数値である。

時間はどこに費やされるのだろうか。各段階はきわめて不均等である。セットの前半を集めるのにかかるのはわずか約 $n\ln 2 \approx 0.69n$ 袋であるのに対し、最後の 1 枚だけで平均 n 袋かかる。労力の大部分は最後の数枚に費やされる。コレクターたちがダブったカードを交換するのはこのためである。

集中

期待値は出発点にすぎない。総数はどれくらいばらつくのだろうか。総数の分散（variance）は $\sum nr/(n-r)^2$ であり、これはおよそ $\frac{\pi^2}{6}n^2$ である（Section 2.4 の和 $\sum 1/k^2 = \pi^2/6$ が現れる）。したがって標準偏差（standard deviation）はおよそ $1.28n$ であり、n が大きいときには平均 $n\ln n$ よりもずっと小さい。つまり総数はその平均の周りに**集中**（concentrated）している。ポール・エルデシュ（Paul Erdős）とアルフレッド・レーニ（Alfréd Rényi）は 1961 年に、より精密に、総数から $n\ln n$ を引いて n で割ったものが極限分布をもつことを示した。それが**ガンベル分布**（Gumbel distribution）であり、多数の確率的な量の最大値も記述する分布である（Section 12.25）。

至るところにクーポン

この問題はアブラーム・ド・モアブル（Abraham de Moivre、1712 年）とラプラス（Laplace）にさかのぼる。現在ではさまざまな姿で現れる。システムのすべての部品を確かめるには、無作為なテストが何回必要か。ネットワーク上のランダムウォークがすべての頂点を訪れるまでどれくらいかかるか。コンピュータのハッシュ表を何回探索しなければならないか。いずれの場合も答えには $n\ln n$ が現れる。生物学で

は、同じ計算によって、ゲノム全体を網羅するのに必要なシーケンシングの「リード」の数が見積もられる。

思考のスキル

期待値の線形性

和の期待値は期待値の和である。各部分が独立であるかどうかは関係ない。複雑な確率的な量を単純な部分に分けよ。

これは確率論で最も役に立つ事実の一つである。期待値の線形性（linearity of expectation）は、ここではクーポン・コレクター問題を n 個の幾何分布型の待ち時間に帰着させた。Section 9.8 では、何の計算もなしに一致の個数の期待値を与えた。大学では、同じ考え方がアルゴリズムの解析や組合せ論（combinatorics）における確率的手法（probabilistic method）を支えている。

次の一歩

1. **セットの半分。** $\frac{n}{2}$ 種類の異なるカードを集めるのに必要な袋の数の期待値（n は偶数）が $n(H_n - H_{n/2})$ であること、そしてこれがおよそ $n \ln 2$ であることを示せ。

2. **異なるカードの数。** k 袋を開けた後に持っている異なるカードの種類数の期待値が $n\left(1 - (1 - \frac{1}{n})^k\right)$ であることを示せ。（**ヒント**：各カードについて、それを持っている確率を求め、足し合わせよ。）セットの 95% を集めるにはおよそ何袋必要か。

3. **二人のコレクター。** 二人の子どもが同じセットを集めており、一方にとってのダブりが他方にとっては新しいカードになりうるように袋を共有する。両方のセットを完成させるのに必要な袋の数の期待値がおよそ $n(\ln n + \ln \ln n)$ であることを示せ。（これは難しい。まず、それが $2n \ln n$ よりずっと小さいことを納得せよ。）

4. **より精密な評価。** 長方形の代わりに台形公式（trapezium rule）の図を用いて、$H_n - \ln n$ が減少し、$H_n - \ln n - \frac{1}{2n}$ が増加することを示せ。小さな n の値から $0.5 < \gamma < 0.7$ を導け。

さらに学ぶために

- **Geoffrey Grimmett & David Stirzaker, *One Thousand Exercises in Probability***（Oxford

University Press）。クーポン・コレクター問題のさまざまな変種が収められている。

- **Julian Havil, *Gamma: Exploring Euler's Constant***（Princeton University Press）。γ と調和級数のすべてを、親しみやすい水準で解説している。
- **Michael Mitzenmacher & Eli Upfal, *Probability and Computing***（Cambridge University Press）。クーポン・コレクター問題と、そのコンピュータ科学における応用。

9.12 ランダムな部分集合

問題

STEP III 2019、問 12

先に進む前に、まず問題を読んでおこう。問題は、OCR が配布している 2019 年の STEP 過去問一式（zip ファイル）のうち、STEP III の問題用紙にある：

`www.ocr.org.uk/Images/696590-2019-past-papers.zip`

導入

$\{1, 2, \ldots, 100\}$ の部分集合（subset）を二つ、まったくランダムに選ぶ。それらが共通の要素を一つももたない確率はどのくらいだろうか。直観は「かなり高い。たいていの集合の組は異なるのだから」と言うかもしれない。実際には、その確率は $\left(\frac{3}{4}\right)^{100}$、およそ 3×10^{-13} である。ランダムな集合は大きく（全体のおよそ半分を含み）、そのためほとんど必ず重なり合うのである。

この問題は短いが、その核にある一つの考え方は強力である。集合を全体として考えるのではなく、要素を一つずつ考えるのである。ランダムな部分集合とは、各要素に一回ずつ、合計 n 回の独立（independent）な硬貨投げにすぎず、ランダムな部分集合に関するあらゆる問いは、それらの硬貨投げに関する問いに帰着する。

取りかかる前に

考えてみよう $\{1, \ldots, n\}$ の部分集合を、「はい／いいえ」で答える n 個の問いへの答えの列で表すにはどうすればよいか。

各要素 i について、「i はその集合に含まれるか」という問いに答える。部分集合が決まれば答えが決まり、答えが決まれば部分集合が決まる。各要素について選択肢は 2 通りなので、部分集合は全部で 2^n 個ある。部分集合を一様ランダムに選ぶことは、各問いに公平な硬貨を独立に投げて答えることと同じである。

順を追って解く

段階 1　一つの要素

硬貨投げによる記述から、$\mathrm{P}(1 \in A_1) = \frac{1}{2}$ である。実際、2^n 個の部分集合のうちちょうど半分が 1 を含む。1 を含まない各部分集合に、それに 1 を加えて得られる部分集合を対応させればよい。

段階 2　互いに素な集合

> **考えてみよう**　$A_1 \cap A_2 = \varnothing$ となるためには、各要素 i について何が成り立たなければならないか。一つの要素について、その確率はいくらか。なぜ要素ごとの確率を掛け合わせてよいのか。

A_1 と A_2 が互いに素（disjoint）であるのは、両方に属する要素が一つもないときであり、またそのときに限る。一つの要素 i については、等確率の四つの可能性がある。どちらの集合にも属さない、A_1 のみに属する、A_2 のみに属する、両方に属する、の四つである（図 9.12.1 左）。禁じられるのは最後のものだけなので、i が両方には属さない確率は $\frac{3}{4}$ である。異なる要素は異なる独立な硬貨投げによって決まるので、

$$\mathrm{P}(A_1 \cap A_2 = \varnothing) = \left(\frac{3}{4}\right)^n. \qquad \blacksquare$$

三つの集合の場合、要素 i が三つすべてに属する確率は $\frac{1}{8}$ なので、$\mathrm{P}(A_1 \cap A_2 \cap A_3 = \varnothing) = \left(\frac{7}{8}\right)^n$ である。一般に、

$$\mathrm{P}(A_1 \cap \cdots \cap A_m = \varnothing) = \left(1 - \frac{1}{2^m}\right)^n. \qquad \blacksquare$$

段階 3　包含関係

> **考えてみよう**　$A_1 \subseteq A_2$ となるためには、一つの要素についての四つの可能性のうちどれが禁じられるか。

$A_1 \subseteq A_2$ が成り立たないのは、A_1 には属するが A_2 には属さない要素が存在するときであり、またそのときに限る。ここでも四つのうち一つのパターンが禁じられるので、

$$\mathrm{P}(A_1 \subseteq A_2) = \left(\frac{3}{4}\right)^n,$$

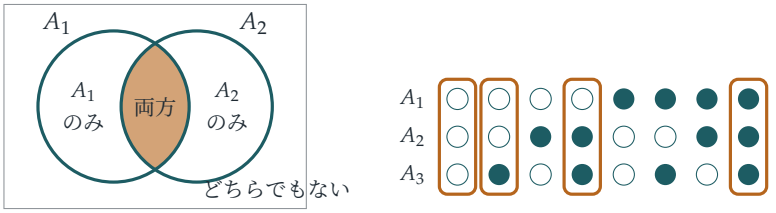
となり、互いに素である確率と同じになる。これは偶然ではない。$A_1 \subseteq A_2$ となるのは A_1 と A_2 の補集合（complement）が互いに素であるときであり、またそのときに限る。そして、ランダムな集合の補集合もまたランダムな集合なのである。

考えてみよう $A_1 \subseteq A_2 \subseteq A_3$ となるためには、一つの要素について、所属の仕方（各集合に属するか属さないか）の 8 通りのパターンのうちどれが許されるか。

鎖（chain）A_1, A_2, A_3 を順にたどると、要素はいったん属したら、その後も属し続けなければならない。したがって許されるパターンは「属さない、属さない、属さない」「属さない、属さない、属する」「属さない、属する、属する」「属する、属する、属する」の 8 通り中 4 通りである（図 9.12.1 右）。よって $\mathrm{P}(A_1 \subseteq A_2 \subseteq A_3) = \left(\frac{4}{8}\right)^n = \left(\frac{1}{2}\right)^n$ である。

m 個の集合からなる鎖については、許されるパターンは、その要素が最初に属する集合（$A_1, \ldots, A_m$ のいずれか、あるいはどれにも属さない）によって決まるので、2^m 通りのパターンのうち $m+1$ 通りが許される。

$$\mathrm{P}(A_1 \subseteq A_2 \subseteq \cdots \subseteq A_m) = \left(\frac{m+1}{2^m}\right)^n. \qquad \blacksquare$$



各要素：等確率の 4 通りの位置　$A_1 \subseteq A_2 \subseteq A_3$ で許されるもの：8 通り中 4 通り

図 9.12.1　左：S の要素は、A_1 と A_2 に対して四つの位置のいずれかにあり、それぞれの確率は $\frac{1}{4}$ である。互いに素であることは「両方」（琥珀色）を禁じ、$A_1 \subseteq A_2$ は「A_1 のみ」を禁じる。右：A_1、A_2、A_3 への所属の仕方の 8 通りのパターン（塗りつぶした円は「属する」を表す）。鎖 $A_1 \subseteq A_2 \subseteq A_3$ が許すのは、枠で囲んだ四つのパターンだけであり、そこでは要素はいったん属したら属し続ける。

振り返り

- **要素ごとに分解する。**集合全体についての各条件（互いに素、包含、鎖）は、それぞれの要素についての個別の条件であった。
- **要素間の独立性。**各要素は独立な硬貨投げによって決まるので、確率は掛け合わされる。
- **パターンを数える。**どの答えも（許されるパターンの数 ÷ すべてのパターンの数）^{n} であった。

背後にある数学

確率を使わずに数える

選び方の総数を掛けると、各確率は個数に変わる。$A_1 \subseteq A_2$ を満たす順序対 (A_1, A_2) の個数は $4^n \times \left(\frac{3}{4}\right)^n = 3^n$ である。これらの組は直接数えることもできる。A_2 の大きさ k を選び、次に A_2 そのものを $\binom{n}{k}$ 通りの方法で選び、さらに A_1 をその 2^k 個の部分集合のいずれかとして選ぶ。したがって

$$\sum_{k=0}^{n} \binom{n}{k} 2^k = 3^n,$$

となり、これは $(1+2)^n$ に対する二項定理（binomial theorem）である。同じものを二通りの方法で、一度は要素ごとに、一度は大きさごとに数えることで、恒等式が証明される。これが**二重数え上げ**（*double counting*）の方法であり、Section 7.9 で正多面体とともに出会ったものである。同様に、鎖 $A_1 \subseteq \cdots \subseteq A_m$ の個数は $(m+1)^n$ である。

部分集合の束

$\{1, \dots, n\}$ の部分集合全体は、包含関係によって順序づけると、**ブール束**（*Boolean lattice*）と呼ばれる構造をなす。これは n 次元の立方体として図示できる。各部分集合は頂点であり、その「はい／いいえ」の答えの列によってラベルづけされ、辺に沿って移動することは要素を一つ加えるか取り除くことに対応する。鎖は上向きに進む経路である。部分集合の族に条件を課したとき、その族がどこまで大きくなりうるかを記述する深い結果がある。**シュペルナー**（*Sperner*）**の定理**（1928 年）は、どの集合も他の集合を含まないような族のうち最大のものは $\binom{n}{\lfloor n/2 \rfloor}$ 個の集合からなることを主張する。**エルデシュ–コー–ラドー**（*Erdős–Ko–Rado*）**の定理**（1961 年）は、どの二つも重なり合うように k 元集合を最大でいくつ選べるかを述べる。どちらも組合せ論（combinatorics）の最初の講義で標準的に扱われるものであり、部分集合を硬貨投げとして見る視点は、それらの最も鮮やかな証明のいくつかを与える。

ブールの代数

ジョージ・ブール（George Boole）の *The Laws of Thought*（『思考の法則』、1854 年）は、論理的な命題を集合として扱い、「かつ」「または」「でない」を共通部分、和集合、補集合として扱った。集合を「はい／いいえ」の答えの列として符号化することは、まさにコンピュータが集合を表現する方法である。$\{1, \dots, 64\}$ の部分集合は一つの 64 ビットの数であり、共通部分は「ビットごとの AND」命令である。この問題の方法、すなわち要素（ビット）を一つずつ考えることは、こうした演算を解析する方法そのものである。

思考のスキル

要素を一つずつ考える

対象が各要素についての独立な選択から構成されているとき、各要素に個別に課される条件の確率は積で表される。

この方法により、2^n 個の部分集合についての問いが、4 通りや 8 通りのパターンについての問いに変わった。大学では、組合せ論（集合や多重集合（multiset）の母関数（generating function））、確率論（独立な座標）、計算機科学（ビットごとの推論）の中で再び現れる。

次の一歩

1. **被覆。** $\mathrm{P}(A_1 \cup A_2 = S)$ および $\mathrm{P}(A_1 \cup A_2 \cup \cdots \cup A_m = S)$ を求めよ。

2. **同じ大きさ。** $\mathrm{P}(|A_1| = |A_2|) = \binom{2n}{n}/4^n$ を示せ。（**ヒント：** $|A_1| = |A_2|$ となるのは $|A_1| + |S \setminus A_2| = n$ のときであり、またそのときに限る。）さらに、n が大きいとき、これがおよそ $1/\sqrt{\pi n}$ であることを示せ。

3. **三つへの分割。** S の互いに素な部分集合の順序対 (A, B) の個数が 3^n であることを示し、互いに素な部分集合の順序を考えない組 $\{A, B\}$ の個数を求めよ。

4. **小さい n に対するシュペルナーの定理。** $n = 3$ および $n = 4$ のそれぞれについて、どの集合も他の集合を含まないような $\{1, \ldots, n\}$ の部分集合の族のうち最大のものを求めよ。

さらに学ぶために

- **Miklós Bóna, *A Walk Through Combinatorics***（World Scientific）。部分集合と半順序集合に関する章。
- **Béla Bollobás, *Combinatorics: Set Systems, Hypergraphs, Families of Vectors and Combinatorial Probability***（Cambridge University Press）。シュペルナーの定理から始まる、部分集合の族についての短く優美な本。
- **Peter Cameron, *Combinatorics: Topics, Techniques, Algorithms***（Cambridge University Press）。二通りに数えることに重点を置いた入門書。

9.13 いかさまサイコロ

問題

STEP I 1999、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/99-s1-q12`

導入

公正なさいころを二つ振ると、合計が 7 になる確率は合計が 2 になる確率の六倍である。ボードゲームの設計者は、そうでなければよいのにと思うことがある。さいころに細工をして（load、特定の目が出やすくなるように重りを入れて）、2 から 12 までのどの合計も同じ確率 $\frac{1}{11}$ で出るようにできないだろうか。十二個の確率は自由に選べるのだから、余地は十分にありそうに見える。

答えは「できない」であり、その証明は珠玉である。十一通りの合計のうち三つと、不等式 $x + \frac{1}{x} \geq 2$ しか使わないのである。これは何かが**不可能**であることを証明する方法の手本である。不可能性の証明は、何かが可能であることを示すよりも難しく、そしてより面白いことが多い。

取りかかる前に

考えてみよう $x > 0$ に対して $x + \frac{1}{x} \geq 2$ をどのように証明するか。等号が成り立つのはどのようなときか。

$x > 0$ を掛けると、不等式は $x^2 + 1 \geq 2x$、すなわち $(x-1)^2 \geq 0$ となり、これは正しい。等号は $x = 1$ のときに限り成り立つ。（別解として、$x + \frac{1}{x} - 2 = \left(\sqrt{x} - \frac{1}{\sqrt{x}}\right)^2$ としてもよい。）これは最も単純な形の相加平均・相乗平均の不等式（AM–GM inequality）である。すなわち、x と $\frac{1}{x}$ の相加平均は、それらの相乗平均 1 以上である。

順を追って解く

段階 1　両端の合計

考えてみよう　合計 2 を出す方法は何通りあるか。合計 12 はどうか。それらの確率を q_i と r_j を用いて表せ。

合計 2 には両方のさいころで 1 が、12 には両方で 6 が必要であるから、$\mathrm{P}(2) = q_1 r_1$、$\mathrm{P}(12) = q_6 r_6$ である。

背理法（proof by contradiction）のために、十一通りの合計がすべて等確率、すなわちそれぞれ確率 $\frac{1}{11}$ であると仮定する。このとき

$$q_1 r_1 = \frac{1}{11}, \qquad q_6 r_6 = \frac{1}{11}.$$

特に、q_1、r_1、q_6、r_6 の四つはすべて正である。

段階 2　真ん中の合計

考えてみよう　合計 7 の作り方は六通りある。そのうち 1 と 6 の目だけを含むのはどの二つか。上の等式を用いて、それらの確率を表せ。

合計 7 には結果 $(1,6)$ と $(6,1)$ が含まれるから

$$\mathrm{P}(7) \geq q_1 r_6 + q_6 r_1.$$

ここでステージ 1 の等式を用いて比を導入する。$q_1 = \frac{1}{11 r_1}$、$q_6 = \frac{1}{11 r_6}$ であるから

$$q_1 r_6 + q_6 r_1 = \frac{1}{11}\left(\frac{r_6}{r_1} + \frac{r_1}{r_6}\right) \geq \frac{1}{11} \times 2 = \frac{2}{11},$$

となる。ここで $x = r_6 / r_1 > 0$ として $x + \frac{1}{x} \geq 2$ を用いた。よって $\mathrm{P}(7) \geq \frac{2}{11}$ となり、$\mathrm{P}(7) = \frac{1}{11}$ に矛盾する。したがって、合計がすべて等確率になることはありえない。$\blacksquare$

手を止めて、やってみよう　何が証明をうまく機能させたかを見てみよう。2 と 12 を 7 と同じくらい出やすくすると、1 と 6 の目がかなり出やすくなければならない。すると「混ざった」結果 $(1,6)$ と $(6,1)$ だけで、7 が出やすくなりすぎてしまうのである。図 9.13.1 に関係するマスを示す。



図 9.13.1　二つのさいころの 36 通りの結果。各マスには合計を記してある。証明では四隅のマスだけを用いる。琥珀色の二つの確率の積は濃い青緑色の二つの確率の積に等しく、$q_1r_1q_6r_6 = q_1r_6 \cdot q_6r_1$ であり、相加平均・相乗平均の不等式により、青緑色の組の和は琥珀色の組の相乗平均の二倍以上である。

段階 3　一つのさいころを二回振る

> **考えてみよう**　一つのさいころを二回振るとき、二つの目が一致する確率を q_j を用いて表せ。公正なさいころではいくらか。

二回の目が一致する確率は $q_1^2 + q_2^2 + \cdots + q_6^2$ である。公正なさいころではこれは $6 \times \frac{1}{36} = \frac{1}{6}$ であり、すでに $\frac{1}{36}$ よりずっと大きい。

> **考えてみよう**　細工によって $\sum q_j^2$ を $\frac{1}{6}$ より小さくできるか。$\sum q_j = 1$ であることはわかっている。

$q_j = \frac{1}{6} + e_j$ とおく。ここで偏差 e_j の和は 0 である。すると

$$\sum q_j^2 = \sum\left(\frac{1}{36} + \frac{e_j}{3} + e_j^2\right) = \frac{1}{6} + \frac{1}{3}\sum e_j + \sum e_j^2 = \frac{1}{6} + \sum e_j^2 \geq \frac{1}{6}.$$

よって同じ目が続く確率はつねに $\frac{1}{6}$ 以上であり、等号は公正なさいころの場合に限り成り立つ。まして $\frac{1}{36}$ 未満になることはありえない。 ■

振り返り

- **背理法。**すべての合計が等確率であると仮定し、不可能なことを導いた。
- **必要なものだけを使う。**十一個の等式のうち、三つで十分であった。正しい等式を選ぶことが鍵となる一歩であった。
- **不等式は不可能性を証明する。**小問 (i) では相加平均・相乗平均の不等式が、小問

(ii) では「平方和は負でない」ことが、可能性の族全体を一挙に排除した。

背後にある数学

多項式による証明

ここでは Section 9.6 の母関数（generating function）を用いた、まったく別の証明を紹介する。$Q(x) = q_1 x + \cdots + q_6 x^6$、$R(x) = r_1 x + \cdots + r_6 x^6$ とおく。すべての合計の確率が $\frac{1}{11}$ であるとすると

$$Q(x)R(x) = \frac{x^2 + x^3 + \cdots + x^{12}}{11} = \frac{x^2}{11}\bigl(1 + x + \cdots + x^{10}\bigr).$$

ここで $Q(x)/x$ は実数係数の 5 次多項式であり、奇数次の実数係数多項式はすべて実数解をもつ（グラフが $-\infty$ から $+\infty$ へ、あるいはその逆へ向かうからである）。よって左辺は 0 でない実数解をもつ。ところが $1 + x + \cdots + x^{10} = \frac{x^{11}-1}{x-1}$ であり、その解は 1 以外の 11 乗の単位根（roots of unity）で、そのどれも実数ではない。これは矛盾である。同じ議論により、$n - 1$ が奇数のとき、すなわち n が偶数のとき、二つの n 面さいころにどのような細工をしても合計を等確率にはできないことがわかる。（n が奇数のときは多項式による議論にはさらに工夫が必要であるが、上の相加平均・相乗平均の不等式による証明はすべての $n \geq 2$ で通用する。）

衝突確率

小問 (ii) の量 $\sum q_j^2$、すなわち独立な二回の抽出が一致する確率は、分布の**衝突確率**（collision probability）とよばれる。小問 (ii) は、これが一様分布のとき最小になることを示している。衝突確率は分布がどれほど集中しているかを測る量である。生態学では、q_j をある生息地における種 j の割合として、$\sum q_j^2$ はシンプソンの多様度指数（Simpson's index）である。経済学では市場集中度を表すハーフィンダール指数（Herfindahl index）であり、暗号理論ではパスワードの分布がどれほど推測されやすいかを測る。さらにこれは Section 9.9 の最後で述べたこと、すなわち誕生日の確率が不均等であれば誕生日が一致する確率は大きくなるしかない、ということを説明している。

不可能性の証明

数学で最も有名な結果のいくつかは、何かができないことを主張するものである。2 乗して 2 になる分数は存在しない。定規とコンパスによる作図で任意の角を三等分することはできない。冪根を用いた公式ですべての五次方程式を解くことはできない。あらゆる数学的命題の真偽を判定するアルゴリズムは存在しない。これらはどれ

もその分野を変えた。なぜなら、どの方法もうまくいかないことを証明するには、方法の全体を理解しなければならないからである。細工したさいころの問題はその縮図である。あらゆる細工を排除するために、どの細工も従わねばならない不変な性質（相加平均・相乗平均の不等式）が必要であった。

思考のスキル

背理法と不等式で不可能性を証明する

どのようなパラメータの選び方もうまくいかないことを示すには、うまくいく選び方があると仮定し、互いに衝突する少数の条件を選び出し、不等式を用いてそれらが同時には成り立たないことを示す。

大学では、背理法と不等式の組合せは、対象が存在しないことを証明する標準的な方法である。解析学でも、組合せ論でも、最適化でもそうであり、最適化では相加平均・相乗平均の不等式やコーシー＝シュワルツ（Cauchy–Schwarz）の不等式のような不等式が、達成できることの限界を定める。

次の一歩

1. **コーシー＝シュワルツの不等式。** コーシー＝シュワルツの不等式 $\left(\sum a_j b_j\right)^2 \le \sum a_j^2 \sum b_j^2$ を $a_j = q_j$、$b_j = 1$ として用い、小問 (ii) の一行の証明を与えよ。

2. **異なる二つのさいころ。** 異なる二つの細工したさいころをそれぞれ一回ずつ振るとき、同じ目が出る確率は $\frac{1}{6}$ より小さくなりうるか。0 になりうるか。

3. **別の目をもつさいころでの一様な合計。** 目の数の付け方が異なれば、二つのさいころで合計を等確率にできることを示せ。一方のさいころの目を $0, 1, 2, 3, 4, 5$、もう一方を $0, 6, 12, 18, 24, 30$ としてみよ。どのような合計が現れるか。これが問題と矛盾しないのはなぜか。

4. **三つのさいころ。** 目が 1 から 6 である三つの細工した六面さいころで、3 から 18 までのすべての合計を等確率にできるか。（**ヒント**：合計 3、8、13、18 と、六つの数に対する相加平均・相乗平均の不等式を用いよ。今回、多項式による証明がうまくいかないのはなぜか。）

さらに学ぶために

- **J. Michael Steele, *The Cauchy–Schwarz Master Class***（Cambridge University Press）。相加平均・相乗平均の不等式から始まる、不等式への美しい入門書。
- **Geoffrey Grimmett & Dominic Welsh, *Probability: An Introduction***（Oxford University Press）。母関数と、上のような証明におけるその使い方。
- **Ian Stewart, *Galois Theory***（CRC Press）、冒頭の数章。五次方程式に関する、あらゆる不可能性の証明の中で最も有名なもの。

学んだこと

本章の冒頭で、数えることは最も古い数学であり、それを巧みに行うことは今なお最も難しいことの一つである、と述べた。そして 3 つの問いを立てた。列挙せずにどう数えるか、何かが必ず起こるのはどのようなときか、数え上げと確率はどのように助け合うのか。本章の 13 問が示したことを以下にまとめる。

1. 列挙せずに数えるには？

本章では一揃いの道具を積み上げてきた。

- **漸化式（recurrence）。**平面に直線を 1 本加える（Section 9.1）、あるいは柵に支柱を 1 本加える（Section 9.3）と、個数は単純な形で変化し、解くことのできる漸化式が得られた。少しだけ余分な情報、すなわち最後の支柱の色を記録しておくことで、漸化式が閉じた形になった。
- **母関数（generating function）。**数列をべき級数（power series）としてまとめると、漸化式は代数の問題に変わり（Section 9.4）、$1/89 = 0.01123\ldots$ となる理由が説明でき、組合せの数え上げは多項式の掛け算になった。Section 9.5 の硬貨、Section 9.6 のさいころ、そして Section 9.7 の釣り合ったべき乗和がその例であり、最後の例では $x = 1$ における重根がすべての役割を果たした。
- **全単射（bijection）。**Section 9.10 の鏡像原理（reflection principle）は、条件を満たさない列を制約のない経路と対応させることで数え上げた。また、ランダムな集合の補集合（complement）をとることで、部分集合が互いに素な対に変わった（Section 9.12）。
- **包除原理（inclusion–exclusion）。**多く数えすぎてから補正することで、攪乱順列（derangement）の個数が求まった（Section 9.8）。
- **二重数え上げ（double counting）。**オイラー（Euler）の公式による領域の数え上げ（Section 9.1）や、大きさごとに分けた部分集合の対の数え上げ（Section 9.12）は、異なる道筋から同じ答えを与え、その途中で恒等式を証明した。

2. 何かが必ず起こるのはどのようなときか？

いくつかの節で、大きさだけで構造が強制されることを見た。6 人の中には、互いに友人である 3 人か、互いに見知らぬ 3 人が必ずいる（Section 9.2）。これは鳩の巣原理（pigeonhole principle）による。ただし 5 人では足りない。23 人いれば、誕生日が一致する人がいる確率は半分を超える（Section 9.9）。ペアの数が人数の 2 乗のように増えるからである。大きな集合のランダムな部分集合どうしは、ほぼ確実に共通部分をもつ（Section 9.12）。そして、どう工夫しても**起こりえない**こともある。2 個のさいころにどのような偏りをつけても、すべての和を等確率にすることはできない（Section 9.13）。また、Sicherman のもの以外に、通常の和の分布を再現するさいころの目の付け方は存在しない（Section 9.6）。

3. 数え上げと確率はどのように助け合うのか？

本章の後半では、確率は数え上げによって求められた。攪乱順列は包除原理で、誕生日問題（birthday problem）は積で、投票問題（ballot problem）は鏡像によって求めた。しかし、逆向きの流れもあった。期待値の線形性（linearity of expectation）は、クーポン収集問題（coupon collector）の nH_n（Section 9.11）や、シャッフルにおける一致の個数の期待値を、数え上げをまったくせずに与えた。ランダムな部分集合を n 回の硬貨投げとみなすと（Section 9.12）、3^n や $(m+1)^n$ のような個数が 1 行の計算で求まった。そして Section 9.2 のエルデシュ（Erdős）の確率的方法（probabilistic method）は、ランダムな彩色が正の確率でうまくいくことを示すことによって、よい彩色が存在することを証明した。2 つの定数がどこからともなく現れた。攪乱順列となる確率の極限に現れる e と、コレクションを完成させるコストに現れるオイラーの γ である。

4. 数え上げの道具箱

手法	使った場所
1つ加えると何が変わるか	直線（9.1）、柵の支柱（9.3）
鳩の巣原理	ラムゼー（Ramsey、9.2）
連立漸化式（coupled recurrences）	柵の支柱（9.3）
母関数	9.4, 9.5, 9.6, 9.7, 9.13
両極端からの場合分け	奇妙なさいころ（9.6）、偏りのあるさいころ（9.13）
包除原理	攪乱順列（9.8）
補集合と指数関数による近似	誕生日（9.9）
鏡像原理	投票問題（9.10）
期待値の線形性	クーポン（9.11）、一致（9.8）
1要素ずつ考える	ランダムな部分集合（9.12）
相加相乗平均の不等式（AM–GM）による背理法	偏りのあるさいころ（9.13）

この先へ

- 攪乱順列のポアソン（Poisson）極限は Section 12.11 で再び登場し、確率変数の母関数は Section 12.15 で家系図の研究の原動力となる。
- 連立漸化式は Section 12.16 でマルコフ連鎖（Markov chain）になる。
- クーポン収集問題に現れるガンベル分布（Gumbel distribution）は、Section 12.25 で多数の確率的な量のうち最大のものを記述する。

大学入学前にさらに先へ進みたい人へ

- **Miklós Bóna, *A Walk Through Combinatorics***：本章のほぼすべての考え方を扱う、親しみやすい入門書。
- **Herbert Wilf, *generatingfunctionology***：母関数についての古典。オンラインで無料で読める。
- **Ronald Graham, Donald Knuth & Oren Patashnik, *Concrete Mathematics***：和、漸化式、母関数を、ウィットに富んだ語り口と豊富な演習問題で扱う。
- **Geoffrey Grimmett & Dominic Welsh, *Probability: An Introduction***：大学1年次の確率論のうち、数え上げの側面を扱う。

ホワイトヘッド（Whitehead）は組合せ論（combinatorics）を「位相幾何学のスラム街」と呼んだ。本章では、今ではなぜ誰もそうは言わないのかを示そうとしてきた。

巧みな数え上げの背後には、必ずそれをはるかに超えて広がる考え方があった。母関数、全単射、漸化式、不等式である。こうした考え方が数え上げを代数学、解析学、確率論と結びつける。新たな小技を一つ探すのではなく、こうした考え方を探すことを身につけることこそが、数え上げを数学へと変えるのである。

「次の一歩」の解答

ここに示すのは完全な解答ではなく、簡潔な答えとヒントである。結果と鍵となる一歩を示すので、自分の解答を確かめるのに使ってほしい。答えを見る前に、それぞれの問題にしっかり取り組むこと。

9.1 平面を分割する直線

1. 円が 1 つなら領域（region）は 2 個である。n 番目の円は他の円と $2(n-1)$ 個の点で交わり、これらの点によって $2(n-1)$ 本の弧に分けられる。各弧は 1 つの領域を 2 つに分ける。よって $R_n = R_{n-1} + 2(n-1)$ であり、$n^2 - n + 2$ を得る。

2. 各直線は、その上にある交点の個数に 1 を加えた数だけ領域を増やす。よって総数は $1 + n +$ (交点の個数) である。k 本の平行線によって交点が $\binom{k}{2}$ 個失われるので、答えは $1 + n + \binom{n}{2} - \binom{k}{2}$ である。

3. n 番目の平面は、他の平面によって一般の位置（general position）にある $n-1$ 本の直線で切られ、$\frac{1}{2}(n^2 - n + 2)$ 個の部分に分けられる。各部分は空間の領域を 1 つずつ 2 つに分ける。これらを $\frac{1}{6}\big((n-1)^3 + 5(n-1) + 6\big)$ に加えると $\frac{1}{6}(n^3 + 5n + 6)$ を得る。

4. $n = 6$ のとき、領域は 32 個ではなく 31 個である。円の内部で、このグラフの頂点（vertex）の個数は $V = n + \binom{n}{4}$（各交点は 4 点から生じる）、辺（edge）の本数は $E = n + \binom{n}{2} + 2\binom{n}{4}$（円の弧と弦があり、各交点が断片を 2 つずつ増やす）である。オイラー（Euler）の公式 $V - E + F = 2$ は外側も数えるので、領域の個数は $F - 1 = 1 + \binom{n}{2} + \binom{n}{4}$ である。

9.2 ミニチュア版ラムゼーの定理

1. 2 色の角（bichromatic angle）は高々 $6 \times 6 = 36$ 個である。単色（one-colour）でない三角形はそのような角をちょうど 2 つ含むので、そのような三角形は高々 18 個である。$\binom{6}{3} = 20$ なので、少なくとも 2 個の三角形は単色である。

2. 1 点からは 16 本の辺が出るので、少なくとも 6 本は同じ色である。その色を赤とし、これらの辺が点 $P_1, \ldots, P_6$ へ向かうとする。P_i どうしを結ぶ辺に赤いものがあれば、赤い三角形ができる。なければ、P_i は 2 色に塗られた K_6 をなし、そこには単色の三角形がある。

3. 点 v からは 9 本の辺が出るので、金の辺が少なくとも 4 本あるか、銀の辺が少なくとも 6 本ある。金の辺で結ばれた隣接点が 4 個ある場合：それらの間に金の辺があれば v と合わせて金の三角形ができ、なければそれらは銀の K_4 をなす。銀の辺で結ばれた隣接点が 6 個ある場合：それらの中に単色の三角形がある。それが金ならそれで終わりであり、銀なら v と合わせて銀の K_4 をなす。

4. 各項に (i, d) というラベルをつける。これは、その項で終わる最長の増加部分列（increasing subsequence）と最長の減少部分列の長さである。2 つの項について、後の項のほうが i か d が大きいので、ラベルはすべて異なる。長さ 3 の部分列が存在しなければ、5 個の項に対してラベルは 4 通りしかない。どちらも存在しない例：$2, 1, 4, 3$。

9.3 柵の杭を塗り分ける

1. 以前と同様に $r_{n+1} = s_n$ であり（杭（post）n が赤でなければ杭 $n+1$ を赤にできる）、最初の杭以外の各杭には $k-1$ 通りの選び方があるので $r_n + s_n = (k-1)^{n-1}$ である。よって $r_{n+1} + r_n = (k-1)^{n-1}$ であり、$r_n = \frac{(k-1)^{n-1} + (k-1)(-1)^{n-1}}{k}$ となる。円の場合：杭 1 の色の選び方が k 通りあり、その後は同じ色で終わる $n+1$ 本の杭の列を考えればよいので、$kr_{n+1} = (k-1)^n + (-1)^n(k-1)$ を得る。

2. $2, 3, 5, 8, \ldots$：a_n 通りとすると、白で終わる列は長さ $n-1$ の任意の列を延長したものであり、赤で終わる列は白で終わる長さ $n-2$ の列を延長したものなので、$a_n = a_{n-1} + a_{n-2}$ である。答えは F_{n+2} である。

3. 中心の色の選び方が 4 通りあり、その後に n 頂点の閉路（cycle）を 3 色で塗り分けるので、$4\left(2^n + 2(-1)^n\right)$ である。

4. $n = 4$ のとき：塗り方は 18 通りである。4 分の 1 回転で固定されるものはなく、半回転では向かい合う杭が同じ色である 6 通りが固定されるので、首飾り（necklace）は $\frac{1}{4}(18 + 0 + 6 + 0) = 6$ 個である。$n = 5$ のとき：塗り方は 30 通りで、どの回転もどの塗り方も固定しないので 6 個である。

9.4 関数としての数列

1. 残りの部分の和は高々 $F_7 \sum_{r \geq 7} 2^{r-7} 10^{-r} = \frac{13 \times 10^{-7}}{0.8} < 2 \times 10^{-6}$ である。$\sum F_r 10^{-r} = \frac{10}{89}$ であり、最初の 6 項の和は 0.112358 なので、$\frac{10}{89}$ は 0.112358 と 0.112360 の間にある。よって $\frac{1}{89} = 0.011235\ldots$ である。2 桁ずつの区切りを使うと $\sum F_r 100^{-r-1} = \frac{1}{9899}$ となる。

2. 漸化式（recurrence relation）の和をとると $\mathrm{f}(x)(1 - 7x + 10x^2) = 2 - 7x$ となり、$\frac{2-7x}{(1-2x)(1-5x)}$ は問題に述べられた通りに分解される。b_n について：$10p + 5q = 40$

と $40p+10q=100$ から $p=1, q=6$ を得る。$t^2=t+6$ の根は 3 と -2 であり、$b_n = 4\cdot 3^n + (-2)^n$ である。

3. $\sum nx^n = \frac{x}{(1-x)^2}$ であり、$x=\frac{1}{100}$ のときこれは $\frac{100}{9801}$ となるので、$\frac{1}{9801} = \sum n\cdot 100^{-n-1}$ である。このパターンは区切り 98 のところで崩れる：100 の区切りが 99 に 1 を繰り上げ、それがさらに 98 に繰り上がるので、展開は …96 97 99 00 01… となる。

4. $\frac{1}{1-x} = 1+x+x^2+\cdots$ を掛けると、x^n の係数は $u_0+\cdots+u_n$ となる。平方数の母関数（generating function）は $\frac{x(1+x)}{(1-x)^3}$ なので、部分和（partial sum）の母関数は $\frac{x+x^2}{(1-x)^4}$ であり、x^n の係数は $\binom{n+2}{3}+\binom{n+1}{3} = \frac{n(n+1)(2n+1)}{6}$ である。

9.5 両替の仕方

1. x^{24} の係数は $6a+6b+3c=24$ の解の個数である：$s=a+b$ が 0 から 4 のそれぞれの値について $s+1$ 通りの選び方があるので、15 となる。一般に、x^n の係数は $n=3m$ でなければ 0 であり、$n=3m$ のときは $k=\lfloor m/2\rfloor$ として $\frac{1}{2}(k+1)(k+2)$ である。余分な因数があると、係数は部分和になる：x^{24}, x^{25}, x^{66} に対してそれぞれ 55, 55, 650 である。これらは、1p 硬貨、3p 硬貨、および 2 種類の異なる 6p 硬貨を使って支払う方法の数を数えている。

2. 各部分（part）k は 1 回使うか、まったく使わないかである。この積は次々に打ち消し合う：$\prod \frac{1-x^{2k}}{1-x^k}$ では偶数の指数をもつ因数がすべて分母から約分され、$\prod \frac{1}{1-x^{\text{奇数}}}$ が残る。これは奇数の部分への分割（partition）の母関数である。$n=6$ の場合：$6, 5+1, 4+2, 3+2+1$ と、$5+1, 3+3, 3+1+1+1, 1+1+1+1+1+1$ であり、それぞれ 4 つずつある。

3. $n=0,1,2,\ldots$ に対する値は $1,1,2,2,3,4,5,6,7,8,10,\ldots$ であり、$\frac{(n+4)^2}{20}$ とこれらの差は常に $\frac{1}{2}$ 以内である（$n=60$ まで確認済み。証明には $\frac{1}{(1-x)(1-x^2)(1-x^5)}$ の部分分数分解（partial fractions）を用いる）。

4. 最後の硬貨は 1p か 2p なので $c_n = c_{n-1}+c_{n-2}$ である：これはフィボナッチ（Fibonacci）数であり、$c_n = F_{n+1}$ となる。

9.6 奇妙なサイコロ

1. 各さいころは、因数 $1+x, 1+x, 1+x^2, 1+x^2$ のうちいくつかの積で $x=1$ における値が 4 となるものに x を掛けたものなので、因数を 2 つとる。標準的な組を除くと、唯一の選択肢は $x(1+x)^2$ と $x(1+x^2)^2$ であり、目は 1,2,2,3 と 1,3,3,5 である。

2. 積は $2x^3+x^4+x^5+4x^6+3x^7+8x^8+6x^9+5x^{10}+6x^{11}$ であり、表と一致する。

3. 可能である：シッカーマン（Sicherman）の組 $1,2,2,3,3,4$ と $1,3,4,5,6,8$ に、標準的なさいころを 1 つ合わせればよい。

4. $(x+x^2)(x+\cdots+x^8) = x^2(1+x)^2(1+x^2)(1+x^4)$ である。硬貨には値が 2 となる因数が必要である：標準的な選び方 $x(1+x)$ のほかに、$x(1+x^2)$（目は $1,3$ で、八面体は $1,2,2,3,5,6,6,7$）または $x(1+x^4)$（目は $1,5$ で、八面体は $1,2,2,3,3,4,4,5$）とすることができる。

9.7 等しい累乗和

1. $\sum(c+b_k)^3 - \sum(c+a_k)^3 = 3c^2\left(\sum b_k - \sum a_k\right) + 3c\left(\sum b_k^2 - \sum a_k^2\right) + \sum b_k^3 - \sum a_k^3$ であり、最初の 2 つの括弧は 0 になる。$\{1,4,6,7\}, \{2,3,5,8\}$ から始めて $c=8$ とすると、$\{1,4,6,7,10,11,13,16\}$ と $\{2,3,5,8,9,12,14,15\}$ を得る。

2. A と $B\cup\{0\}$ はどちらも要素の個数が 6、和が 33、平方和が 253 である。したがって $\sum_{a\in A}(n+a)^2 = \sum_{b\in B\cup\{0\}}(n+b)^2$ となり、これが $\{n^2,\ldots,(n+11)^2\}$ を 2 つに分ける。

3. $(x+c)^r$ を二項定理（binomial theorem）で展開すると、r 次以下のべきだけが現れ、それらの和は一致する。問題の集合は、2 番目の集合に 0 を加えると $\{0,\ldots,15\}$ となり、平行移動すれば任意の連続する 16 個の整数が得られる。

4. $ABABABAB$ では、A は約 1.676、B は約 1.042 を得る。$ABBABAAB$ では、A は約 1.560、B は約 1.158 を得る：まだ等しくはないが、かなり近い。

9.8 誰も自分のシャツを受け取らない

1. $\mathrm{E}(C_1) = \frac{1}{m}$, $\mathrm{Var}(C_1) = \frac{1}{m} - \frac{1}{m^2}$ であり、$\mathrm{Cov}(C_1,C_2) = \frac{1}{m(m-1)} - \frac{1}{m^2} = \frac{1}{m^2(m-1)}$ である。すると $\mathrm{E}(N)=1$ であり、$\mathrm{Var}(N) = m\left(\frac{1}{m}-\frac{1}{m^2}\right) + m(m-1)\frac{1}{m^2(m-1)} = 1$ となる。$m=4$ のとき $\mathrm{P}(N=0) = \frac{9}{24} = 0.375$ であり、これは $\mathrm{e}^{-1} \approx 0.368$ に近い。

2. カード 1 はある位置 i に行く（$n-1$ 通り）。カード i が位置 1 に行くなら、残りは $n-2$ 枚の完全順列（derangement）である。そうでなければ、位置 1 をカード i の禁止された場所とみなすと、$n-1$ 枚の完全順列が得られる。確認：$D_3 = 2(1+0) = 2$, $D_4 = 3(2+1) = 9$。

3. 固定される k 枚のカードを選び、残りを完全順列にする：$\binom{n}{k}\frac{D_{n-k}}{n!} = \frac{1}{k!}\cdot\frac{D_{n-k}}{(n-k)!} = \frac{d_{n-k}}{k!}$ であり、これは $\frac{\mathrm{e}^{-1}}{k!}$ に近づく。

4. $30-(15+10+6)+(5+3+2)-1 = 8$ であり、これは $30\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5}$ に等しい：包除原理（inclusion–exclusion）の和が因数分解されるのである（これはオイラーの $\varphi(30)$ である）。

9.9 誕生日問題

1. $\mathrm{P}(X = r) = \left(1 - \frac{1}{n}\right) \cdots \left(1 - \frac{r-2}{n}\right) \frac{r-1}{n}$ であり、これらの和は 1 である。期待値（expectation）については、$\mathrm{P}(Y = r)$ は $\mathrm{P}(Y \geq 1), \ldots, \mathrm{P}(Y \geq r)$ のそれぞれで 1 回ずつ数えられる。$Q_k = \mathrm{P}(X > k) = \prod_{j=1}^{k-1} \left(1 - \frac{j}{n}\right)$ とおく。すると $\mathrm{E}(X) = \sum (k+1) \frac{k}{n} Q_k$ であり、また $\mathrm{E}(X) = 1 + \sum Q_k$ でもある。$\sum \frac{k}{n} Q_k = 1$ を用いて引き算すると、$\sum Q_k \left(1 - \frac{k^2}{n}\right) = 0$ を得る。

2. $\binom{k}{3} \approx 365^2 \ln 2$ から $k \approx 82$ を得る。この近似は 3 つ組どうしの従属性を無視しており、正しい答えは 88 である。

3. 14 人である。（各ペアが「近い」確率は $\frac{3}{365}$ であり、$\binom{k}{2} \frac{3}{365} \approx \ln 2$ から $k \approx 14$ を得る。正確に数えると、確率は 14 人で約 0.537、13 人で約 0.483 である。）

4. 2 人が日 i を共有する確率は p_i^2 であり、これらを足し合わせる。コーシー・シュワルツ（Cauchy–Schwarz）の不等式より $1 = \left(\sum p_i\right)^2 \leq 365 \sum p_i^2$ であり、等号はすべての p_i が等しいときに限り成り立つ。

9.10 いつでもおつりを渡せる

1. 最初の人は £1 硬貨を持っていなければならない。続く数人について条件づけると多くの場合に分かれ（各 £2 の客の後で手元にどの硬貨があるか）、それぞれが小問 (i) と小問 (ii) の答えで終わる。それらをまとめると $\frac{m-2}{m+1}$ を得る。鏡像原理（reflection principle）を使えば 1 行で済む。

2. 最初の票は A への票でなければならない。A で始まる開票のうち悪いもの（同数になるもの）は、最初に同数になるまでの部分を反転することで、B で始まる開票と対応する。よって良い開票の数は $\binom{a+b-1}{a-1} - \binom{a+b-1}{a}$ であり、これを $\binom{a+b}{a}$ で割ると $\frac{a-b}{a+b}$ を得る。

3. $((()))$, $(()())$, $(())()$, $()(())$, $()()()$。全単射（bijection）：最初の括弧の組は、列をその内側の部分とその後ろの部分に分ける。これに対応して、固定された辺の上にある三角形は、多角形を 2 つの小さな多角形に分ける。両方について再帰的に繰り返せばよい。

4. £5 の客はおつりとして £1 硬貨を 4 枚必要とするので、経路は 1 上がるか 4 下がる。経路は障壁に触れずに飛び越えることができるので、鏡像によって悪い経路を単純な集合と対応させることはもはやできない。

9.11 全種類を集める

1. 待ち時間の期待値は $\frac{n}{n} + \frac{n}{n-1} + \cdots + \frac{n}{n/2+1} = n(H_n - H_{n/2}) \approx n(\ln n - \ln \frac{n}{2}) = n \ln 2$ である。

2. 各カードが欠けている確率は $(1-\frac{1}{n})^k$ であり、これを n 枚のカードについて足し合わせる。95% にするには $(1-\frac{1}{n})^k \approx \mathrm{e}^{-k/n} = 0.05$ とすればよいので、$k \approx n\ln 20 \approx 3n$ である。

3. t 袋を開けた後、あるカードが見られた回数が 2 回未満である確率は約 $\mathrm{e}^{-t/n}(1+\frac{t}{n})$ である。2 人の子どもがともに集め終わるのは、おおよそそのようなカードの個数の期待値 $n\mathrm{e}^{-t/n}(1+\frac{t}{n})$ が約 1 まで下がるときであり、これから $\frac{t}{n} \approx \ln n + \ln\ln n$ を得る。これは $2\ln n$ よりはるかに小さい。

4. $\frac{1}{n+1} < \ln\frac{n+1}{n}$（$[n, n+1]$ 上の $\frac{1}{x}$ のグラフの下の面積）なので、$H_n - \ln n$ は減少する。凸性（convexity）より台形は面積を過大評価するので $\ln\frac{n+1}{n} < \frac{1}{2}\left(\frac{1}{n}+\frac{1}{n+1}\right)$ であり、したがって $H_n - \ln n - \frac{1}{2n}$ は増加する。$n=1$ とすると $\gamma > \frac{1}{2}$、$n=4$ とすると $\gamma < H_4 - \ln 4 \approx 0.697$ である。

9.12 ランダムな部分集合

1. 各要素は少なくとも 1 つの集合に含まれなければならない：$\left(\frac{3}{4}\right)^n$ であり、一般には $\left(1-2^{-m}\right)^n$ である。

2. $|S \setminus A_2|$ は $|A_2|$ と同じ分布をもち、A_1 と独立であるので、求める確率は $|A_1| + |S \setminus A_2| = n$ となる確率に等しい。組 $(A_1, S \setminus A_2)$ は $2n$ 個の要素からなる集合のランダムな部分集合に対応し、その大きさが n である確率は $\binom{2n}{n}/4^n$ である。スターリング（Stirling）の公式（またはウォリス（Wallis）の公式、Section 4.4）により、これは $\approx \frac{1}{\sqrt{\pi n}}$ となる。

3. 各要素は A に入るか、B に入るか、どちらにも入らないかのいずれかである：3^n。$A = B$ となる順序対は $(\varnothing, \varnothing)$ だけなので、順序を考えない組は $\frac{3^n-1}{2}+1 = \frac{3^n+1}{2}$ 個ある。

4. $n=3$ では 3 個の集合（すべての 1 元集合、またはすべての 2 元集合）。$n=4$ では 6 個の集合（すべての 2 元集合）。一般には $\binom{n}{\lfloor n/2 \rfloor}$ である（シュペルナー（Sperner）の定理）。

9.13 いかさまサイコロ

1. $1 = \left(\sum q_j\right)^2 \le 6\sum q_j^2$ なので、P(同じ目) $= \sum q_j^2 \ge \frac{1}{6} > \frac{1}{36}$ である。

2. どちらも可能である：確率は $\sum q_j r_j$ であり、たとえば一方のさいころが常に 1 を、他方が常に 2 を出すなら 0 になる。

3. 合計は $0, 1, \ldots, 35$ がそれぞれちょうど 1 回ずつ現れるので、一様である。問題では両方のさいころに 1 から 6 までの数が書かれていることを要求しているが、ここではそうなっていない。

4. 不可能である。$\mathrm{P}(3) = q_1r_1s_1$, $\mathrm{P}(18) = q_6r_6s_6$ とおくと、どちらも $\frac{1}{16}$ である。$\mathrm{P}(8)+\mathrm{P}(13)$ は 6 つの項 $q_1r_1s_6, \ldots, q_1r_6s_6$（1 が 2 つと 6 が 1 つ、または 6 が 2 つと 1 が 1 つ）を含み、それらの積は $(\mathrm{P}(3)\mathrm{P}(18))^3$ である。相加平均・相乗平均の不等式（AM–GM）より $\mathrm{P}(8)+\mathrm{P}(13) \geq 6 \cdot \frac{1}{16} > \frac{2}{16}$ となる。与えられた多項式による証明がそのままではうまくいかないのは、$1+x+\cdots+x^{15}$ が実数の根 -1 を**もつ**からである。（これは修正できる：実係数の 5 次式が 3 つあれば実数の根が 3 つ必要だが、-1 は単根にすぎない。）

Beyond STEP

STEP は、ほとんどの中高生がこれまでに受けるなかで最も難しい数学の試験である。そして最も優れた試験の一つでもある。その問題は短く、見慣れず、奥が深い。なかでも最良の問題は、姿を変えた大学数学の小さな断片なのである。

本書は、1987 年の第 1 回試験に先立つ見本問題（specimen papers）から 2025 年の試験問題までのなかから、特に興味深い STEP の問題を選び、その一つひとつを扉として用いる。どの問題も、優れた学生が途中で抱く疑問に触れながら丁寧に解き、そのうえで扉の向こうへと踏み出す。その考え方はどこから来たのか、大学では何へと発展するのか、次に何を読めばよいのか。

本書は、STEP に向けて準備を進める才能ある数学者の卵のうち、過去問演習以上のものを求める人のために書かれている。数学専攻の学部生のように考え始め、その先に何が待っているのかを知ってほしい。

- 純粋数学（pure mathematics）、力学（mechanics）、確率（probability）、統計（statistics）にわたる 13 の章
- STEP の過去問 136 題、それぞれに道筋を示した解答つき
- すべての問題の背後にある大学数学
- 解答つきの発展演習と、さらに学ぶための文献案内

全 13 章のうちの第 9 章。 本書全体、すべての章、すべての解答は、次のサイトで自由に閲覧・ダウンロード・共有できる：

beyondstep.keithmcnulty.org

本文はパブリックドメイン（public domain）に提供されている（CC0 1.0）。STEP の問題 © Cambridge University Press & Assessment.