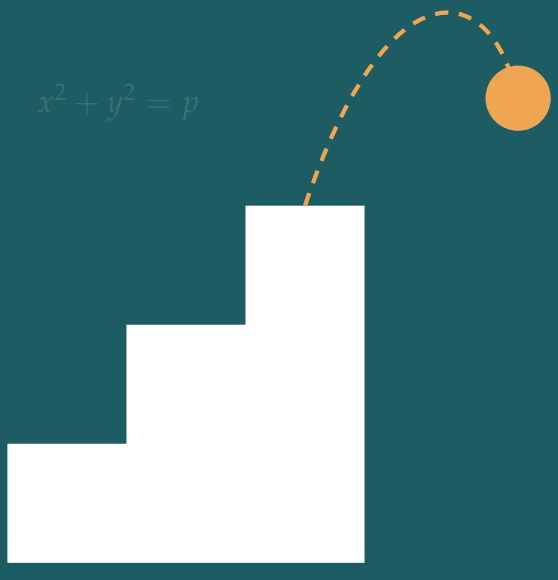
STEP 対策 · 大学の数学

Beyond STEP

第 1 章

整数論（number theory）と証明（proof）



KEITH McNULTY

Beyond STEP

大学数学への入り口としての
STEP 過去問

第 1 章

整数論（number theory）と証明（proof）

Keith McNulty

Beyond STEP：大学数学への入り口としての STEP 過去問

第 1 章：整数論（number theory）と証明（proof）

これは *Beyond STEP* 全 13 章のうちの第 1 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

1

数論と証明

整数は数学で最も古い対象であり、今なお数学の最も深い秘密のいくつかを抱えている。

この章の内容

1.1	素数を生み出す工場	STEP II 2002
1.2	素数はどれほどまばらか？	STEP III 2016
1.3	最小の反例	STEP III 2015
1.4	e は無理数であり、e^2 もまた無理数である	STEP III 2024
1.5	無限降下法	STEP III 2022
1.6	二つの平方数の和	STEP II 2023
1.7	因数分解が破綻するとき	STEP I 2016
1.8	有理数を数える	STEP III 2020
1.9	三次曲線の接線	STEP I 2009
A	演習問題の答え	p. 73

なぜ整数なのか

> 数学は科学の女王であり、数論は数学の女王である。
>
> — カール・フリードリヒ・ガウス（Carl Friedrich Gauss）

整数（whole numbers）は、誰もが最初に出会う数学的対象である。字が読めるようになる前から、私たちは数を数えることを覚えた。それにもかかわらず、整数についてのごく単純な問いが、恐ろしく難しいことがある。2 より大きいすべての偶数は、2 つの素数（prime）の和で表せるだろうか。答えは誰にもわからない。クリスティアン・ゴールドバッハ（Christian Goldbach）が 1742 年にこの問いを立て、コンピュータは 4×10^{18} を超えるところまで確かめたが、いまだに証明されていない。11 と 13、101 と 103 のように、差が 2 である素数の組は無限に存在するだろうか。これも誰にもわからない。もっとも 2013 年には、ほとんど無名の数学者であった張益唐（Yitang Zhang）が、差が高々 70 百万である素数の組が無限に存在することを証明して世界を驚かせた。この値はその後 246 まで引き下げられている。ピエール・ド・フェルマー（Pierre de Fermat）は 1637 年、$n \geq 3$ のとき $x^n + y^n = z^n$ は正の整数解をもたない、と本の余白に書き付けた。アンドリュー・ワイルズ（Andrew Wiles）が 1994 年にフェルマーの正しさを証明するまでには、350 年以上の歳月と、これまでに生み出された中でも最も高度な数学のいくつかが必要であった。

子どもにも理解できる問いと、何世紀もかかりうる答え。この組み合わせこそが、数論（number theory）を病みつきにさせるものである。そしてこれは、数論がつねに**証明**（proof）の訓練の場であり続けてきた理由でもある。整数は無限に存在するので、すべての場合を確かめることはできない。そのようなときは、すべての場合を一度に扱える論証を見つけなければならない。これから先の数学人生で使うことになる証明の技法の多くは、もともと整数についての問いを通して磨かれたものである。

純粋で、役に立たず、そしてインターネットを支えるもの

1940 年、ケンブリッジの数学者ハーディ（G. H. Hardy）は、数論はあらゆる数学の中で最も純粋なものであり、日常生活からあまりにかけ離れているので実用には使えず、したがって**有害な**用途にも使えない、といくらか誇らしげに書いた。これほど見当違いの予言もなかなかない。オンラインで買い物をするとき、安全なメッセージを送るとき、スマートフォンのロックを解除するとき、私たちは数論に頼っている。RSA 暗号（1977 年）は、2 つの大きな素数を掛け合わせるのは簡単だが、その積からもとの素

数を復元するのは絶望的に難しいと考えられている、という事実に基づいている。現代の暗号方式は、この章の最後に登場する曲線そのものの算術を利用している。18 世紀と 19 世紀の「役に立たない」数学は、21 世紀の安全を支えるものとなったのである。

大学で出会うもの

大学で数学を学ぶなら、数論は最初に訪れる場所のひとつであり、最後に行き着く場所のひとつでもある。

- **最初の学期には**、ほぼ間違いなく「数と集合（*Numbers and Sets*）」や「数学の基礎（*Foundations*）」といった名前の講義を受けることになる。そこでは証明をきちんと書く方法を学ぶが、その素材の多くは数論である。帰納法（induction）、ユークリッドの互除法（Euclidean algorithm）、合同算術（modular arithmetic）、フェルマーの小定理（Fermat's Little Theorem）、中国剰余定理（Chinese Remainder Theorem）、そして無限集合の中には他より大きいものがあるという驚くべき事実などである。
- **群論**（group theory）では（通常は 1 年目に学ぶ）、数論の多くの事実が、対称性についてのただひとつの定理、すなわちラグランジュの定理（Lagrange's Theorem）の影であることを知るだろう。
- **2 年目には**、**数論**の講義で、平方剰余の相互法則（quadratic reciprocity、ガウスの「黄金定理」）、連分数（continued fractions）、ペル方程式（Pell's equation）を扱うのが普通である。
- **その先には**さらに進むことができる。ガウス整数（Gaussian integers）のような新しい数の体系によって素因数分解の一意性（unique factorisation）を救い出す**代数的整数論**（algebraic number theory）、微積分と複素解析（complex analysis）を用いて素数を数える**解析的整数論**（analytic number theory）、そしてフェルマーの最終定理（Fermat's Last Theorem）の証明や、賞金 100 万ドルの 7 つのミレニアム懸賞問題（Millennium Prize Problems）のひとつの背後にある**楕円曲線**（elliptic curves）の理論である。

この章を貫く問い

この章の 9 つの STEP の問題は、3 つの大きな問いのまわりを巡っている。問題に取り組む間、これらを頭の片隅に置いておいてほしい。章の最後で再びこれらに立ち返る。

1. **素数はいくつあり、どのように分布しているのか。**素数が無限に存在することは誰もが知っている。しかし、素数はどれほどまばらになっていくのか。そして、どのような論証がそれを教えてくれるのか。

2. **ある数が分数ではないことは、どうすれば証明できるのか。**ある数が有理数（rational）であることを示すには、例をひとつ挙げればよい。しかし無理数（irrational）であることを示すには、無限に多くの可能性を排除しなければならない。そんなことがいったいどうすればできるのか。

3. **どの方程式が整数解をもつのか。そして、数の体系を変えると何が起こるのか。**方程式が解をまったくもたないことを示せる場合もある。また、整数を理解する最善の方法が、整数の外に出て、複素数の世界や曲線の上に踏み出すことである場合もある。

証明についての章

これら 3 つの問いの底には、第 4 のテーマが流れている。それは**どのように証明するか**である。各節は、異なる証明の方法が実際に働くところを示すという理由もあって選ばれており、全体として大学 1 年生にとって十分な道具箱になっている。

§	テーマ	考え方
1.1	フェルマー数（Fermat numbers）	無限に多くの素数を必要とする無限の数の族
1.2	素数の積	強帰納法（strong induction）、二項係数（binomial coefficients）に隠された情報
1.3	再び $\sqrt{2}$	「最小のものをとれ」：整列原理（well-ordering principle）
1.4	e と e^2	整数を 0 と 1 の間に厳密に閉じ込める
1.5	解をもたない方程式	無限降下法（infinite descent）、法 n（modulo n）で考える
1.6	2 つの平方数の和	舞台を変える：複素数
1.7	奇妙な数の体系	当然と思っていることを疑う
1.8	分数を並べ上げる	全単射（bijection）を構成する、逆向きの降下法
1.9	立方数と曲線	幾何で算術を解く

この章の読み方

各節は、出題されたままの STEP の問題へのリンクから始まる。読み進める前に、まず少なくとも 30 分は自分で取り組んでみてほしい。読んだだけの問題よりも、苦労して格闘した問題からのほうが、はるかに多くを学べる。読み進めるときには、**自問してみよう**の枠は答えが示される前に立ち止まって考えるよう促すものであり、**手を止めて考えよう**の枠は鍵となる考え方に手が届く瞬間を示している。そして各節の**背後**

にある数学の部分では、試験の先にある、大学で出会う数学を見渡す。

各節はおおむね後になるほど高度になるが、互いにほぼ独立している。ある節に興味を引かれなければ、先に進み、後で戻ってくればよい。

1.1 素数を生み出す工場

問題

STEP II 2002、問 3

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/02-s2-q3`

導入

素数（prime）が無限に存在することは、ほぼ間違いなくすでに知っているだろう。ユークリッド（Euclid）が紀元前 300 年頃に証明したもので、誰もが最初に出会う証明の一つである。では、なぜ STEP の問題がそれをもう一度証明させるのだろうか。

それは、この証明がまったく異なる仕組みで働くからである。ユークリッドの議論は「素数の有限なリストを一つ与えよ。それが不完全であることを示してみせよう」というものである。一方この証明は「ここに、あらかじめ書き下された一つの具体的な数列がある。そのどの項も、他のどの項にも含まれない素数を含んでいる」と主張する。これは新しい素数を次々と生み出す機械であり、それが機能する理由は、問題が導いてくれる美しく単純な恒等式にある。

その途中で、フェルマー本人さえも欺いた数に出会うことになる。

取りかかる前に

まず問題を一通り読み、その構成に注目しよう。四つの段階からなっている。

1. いくつかの例を計算する。
2. パターンを見つけ（というより、教えてもらい）、それらの例で確かめる。
3. そのパターンを一般に証明する。
4. そのパターンを二度使う。まず公約数（common factor）についての結論を導き、次に素数についての結論を導く。

この「例 → 予想（conjecture）→ 証明 → 帰結」という構造は、実際に多くの数学が行われる方法そのものであり、STEP の問題もしばしばこの流れに従う。これに気づいたら、前半の小問は単なる準備運動ではないことが多い。後で必要になる直観を養う場所なのである。

> **考えてみよう**　最後の行は**無限に多くの素数**について問うている。中ほどでは**公約数**について問うている。「どの二つのフェルマー数も共通の約数をもたない」ことと「素数は無限に存在する」こととは、いったいどうつながりうるのだろうか。

この問いを心に留めておこう。後で戻ってくる。

順を追って解く

段階 1　数の感触をつかむ

記法に注意しよう。2^{2^n} は $2^{(2^n)}$ を意味し、$(2^2)^n$ ではない。指数そのものが 2 の累乗なので、これらの数は**非常に**速く大きくなる。

$$F_0 = 2^1 + 1 = 3, \qquad F_2 = 2^4 + 1 = 17,$$
$$F_1 = 2^2 + 1 = 5, \qquad F_3 = 2^8 + 1 = 257.$$

> **考えてみよう**　これら四つの数について、何に気づくだろうか。

すべて素数である。（257 を確かめよう。これは 2, 3, 5, 7, 11 のいずれでも、また 13 でも割り切れず、$17^2 = 289 > 257$ なので、ここで調べるのをやめてよい。）次の $F_4 = 2^{16} + 1 = 65537$ も素数である。ピエール・ド・フェルマー（Pierre de Fermat）は 1640 年にまさにこのことに気づき、この形の数は**すべて**素数であると予想した。このことを覚えておこう。彼が正しかったかどうかは後で見る。

段階 2　恒等式を確かめる

次に、小さな k について $(*)$ を確かめよう。

- $k = 1$：左辺は単に $F_0 = 3$ であり、$F_1 - 2 = 3$ である。✓
- $k = 2$：$F_0 F_1 = 3 \times 5 = 15$ であり、$F_2 - 2 = 15$ である。✓
- $k = 3$：$F_0 F_1 F_2 = 15 \times 17 = 255$ であり、$F_3 - 2 = 255$ である。✓

考えてみよう $k=2$ から $k=3$ への移り変わりを見てみよう。15 に 17 を掛けて 255 を得た。フェルマー数（Fermat number）の言葉で言えば、$(F_2-2)\times F_2$ を計算して F_3-2 を得たことになる。これは偶然だろうか。

この観察こそが、証明全体の縮図である。なぜそれが成り立つはずなのかを見ていこう。

段階 3 恒等式を証明する

手を止めて、やってみよう 先を読む前に、

$$(F_k-2)\,F_k = F_{k+1}-2.$$

を直接示してみよう。**ヒント：**すべてを 2 の累乗で表してみよ。F_k-2 はどのような形をしているか。

$F_k-2=2^{2^k}-1$ かつ $F_k=2^{2^k}+1$ であるから、

$$(F_k-2)\,F_k=\left(2^{2^k}-1\right)\left(2^{2^k}+1\right).$$

考えてみよう これは $(a-1)(a+1)$ の形の積である。これは何に等しいか。

これは平方の差（difference of two squares）a^2-1 である。$a=2^{2^k}$ とすると、

$$a^2=\left(2^{2^k}\right)^2=2^{2\cdot 2^k}=2^{2^{k+1}},$$

したがって

$$(F_k-2)\,F_k=2^{2^{k+1}}-1=F_{k+1}-2. \tag{†}$$

これが原動力である。2 乗することが何をしているかに注目しよう。2 乗は指数を 2 倍にし、2^k を 2 倍すると 2^{k+1} になる。フェルマー数の定義は、平方の差による因数分解にぴったり合うように作られているのである。

ここまで来れば、帰納法（induction）はほとんど自動的である。

考えてみよう 帰納法のステップでは、正確には何を示す必要があるか。

ある $k\geq 1$ について $(*)$、すなわち

$$F_0F_1\cdots F_{k-1}=F_k-2,$$

が成り立つと仮定し、$k+1$ についても成り立つこと、すなわち

$$F_0F_1\cdots F_{k-1}F_k=F_{k+1}-2.$$

を示したい。仮定の両辺に F_k を掛け、(†) を用いると

$$F_0F_1\cdots F_{k-1}F_k = (F_k-2)\,F_k = F_{k+1}-2.$$

となる。$k=1$ はすでに確かめたので、数学的帰納法により $(*)$ はすべての $k\geq 1$ について成り立つ。 ■

> **考えてみよう**　帰納法をまったく使わずに済ませることはできただろうか。

できる。その方法を見ておく価値がある。$F_0-2=1$ から出発して、(†) を繰り返し適用すると

$$F_k-2 = (F_{k-1}-2)F_{k-1} = (F_{k-2}-2)F_{k-2}F_{k-1} = \cdots = (F_0-2)\,F_0F_1\cdots F_{k-1}.$$

となる。$F_0-2=1$ であるから、これで示された。この「展開」は実は同じ帰納法をすべて書き下したものにすぎないが、こちらのほうが見通しやすいと感じる人もいる。

段階 4　共通の約数はない

$m\neq n$ ならば F_m と F_n が 1 より大きい公約数をもたないことを示したい。

> **考えてみよう**　ある数 d が F_m と F_n の両方を割り切るとし、$m<n$ とする。F_m は $(*)$ のどこに現れるか。

$(*)$ で $k=n$ とすると

$$F_0F_1\cdots F_m\cdots F_{n-1} = F_n-2.$$

$m<n$ であるから、F_m は左辺の因数の一つである。よって d が F_m を割り切るならば、d は左辺全体を割り切る。すなわち、d は F_n-2 を割り切る。

> **考えてみよう**　さて、d は F_n と F_n-2 の両方を割り切る。ほかに何を割り切らなければならないか。

それらの差である。d は $F_n-(F_n-2)=2$ を割り切る。よって $d=1$ または $d=2$ である。

> **考えてみよう**　d は 2 でありうるか。

ありえない。どのフェルマー数も 2 の累乗に 1 を加えたものなので奇数である。したがって $d=1$ であり、相異なる二つのフェルマー数が 1 より大きい共通の約数をもつことはない。 ■

数学者はこれを、フェルマー数は**どの二つも互いに素**（pairwise coprime）であるという。

段階 5 素数は無限に存在する

ここで、最初に立てた問いに戻ろう。

> **考えてみよう** 1 より大きいすべての整数は、少なくとも一つの素因数（prime factor）をもつ。各フェルマー数から素因数を一つずつ選ぶ。選んだ素数について何が言えるか。

p_n を F_n を割り切る任意の素数とする。もしこれらのうち二つが等しい、たとえば $m \neq n$ で $p_m = p_n$ であるとすると、その素数は F_m と F_n の 1 より大きい公約数となるが、これは先ほど不可能であると示した。したがって素数

$$p_0,\ p_1,\ p_2,\ p_3,\ \dots$$

はすべて**相異なる**。フェルマー数は無限に存在するので、相異なる素数も無限に存在する。 ■

各フェルマー数を**どの**素数が割り切るのかを知る必要はまったくなかったし、フェルマー数自身が素数かどうかさえ知る必要がなかったことに注目しよう。必要だったのは、それらが決して共通の約数をもたないということだけである。各フェルマー数は、他のどれも使えない素数を少なくとも一つ「使い切る」ことを強いられているのである。

n	$F_n = 2^{2^n} + 1$	素因数分解
0	3	素数
1	5	素数
2	17	素数
3	257	素数
4	65 537	素数
5	4 294 967 297	$641 \times 6\,700\,417$
6	18 446 744 073 709 551 617	$274\,177 \times 67\,280\,421\,310\,721$

図 1.1.1 最初のいくつかのフェルマー数。フェルマーはこれらがすべて素数であると推測したが、オイラー（Euler）が 1732 年に F_5 の約数 641 を見つけた。F_4 より先のフェルマー数で素数であると知られているものは一つもない。それでも恒等式 $(*)$ は、異なるフェルマー数の素因数が決して重ならないことを示している。各行が新しい素数をもたらすのである。

振り返り

何がこの議論をうまく機能させたのかを立ち止まって確かめておく価値がある。同じ考え方は本書で何度も現れるからである。

- **例は飾りではなかった。** $15 \times 17 = 255$ が「$(F_2 - 2) \times F_2 = F_3 - 2$」であると見抜くことこそが、鍵となる考え方だったのである。問題が小さな場合を与えてくれたら、数値が一致するかどうかだけでなく、各ステップが何をしているのかを問おう。
- **一つの恒等式がすべての仕事をした。** すべては $(a-1)(a+1) = a^2 - 1$ から流れ出た。難しそうに見える STEP の問題は、しばしば一つの単純な代数計算によって動いている。
- **最後の議論は大きさではなく構造についてのものである。** 新しい素数を一つも見つけることなく、素数が無限に存在することを証明した。その代わりに、無限個の数の族を作り上げるには無限に多くの素数が**必要である**ことを示したのである。

背後にある数学

フェルマーは正しかったか

正しくなかった。1732 年、レオンハルト・オイラー（Leonhard Euler）は

$$F_5 = 2^{32} + 1 = 4\,294\,967\,297 = 641 \times 6\,700\,417.$$

であることを示した。オイラーは偶然 641 を見つけたのではない。彼は F_n の素因数はきわめて特殊な形をしていなければならないこと（$n = 5$ のときは、64 の倍数に 1 を加えた数でなければならないこと）を証明し、それによって候補を大幅に絞り込んだのである。このことは演習 4 で自分で証明できる。

それ以来、これまでに調べることができた F_5 から F_{32} までのすべてのフェルマー数は、合成数（composite）であることが判明している。知られている限りでは、F_0 から F_4 までが**唯一の**フェルマー素数かもしれないが、それを証明できた者はいない。これは正真正銘の未解決問題である。

愉快なひねりは、私たちの証明はそのことをまったく気にしないという点である。素数であれ合成数であれ、フェルマー数はやはり無限に多くの素数を生み出すのである。

フェルマー素数と多角形の作図

フェルマー素数は、まったく思いがけない場所に現れる。古代ギリシャ人は定規とコンパスで正三角形と正五角形を作図する方法を知っていたが、$3 = F_0$ かつ $5 = F_1$ であることに注目しよう。二千年もの間、辺の数が素数であるそれ以外の正多角形を作図できた者はいなかった。そして 1796 年、19 歳のカール・フリードリヒ・ガウス（Carl Friedrich Gauss）が正 *17* **角形**の作図法を示した。そして $17 = F_2$ である。

ガウスはさらに進んだ。正 N 角形が定規とコンパスで作図できるのは、N が 2 の累乗と**相異なるフェルマー素数**の積であるときであり、かつそのときに限る。（Pierre Wantzel が 1837 年に証明を完成させた。）つまり、どの多角形が作図できるかは、フェルマー素数がいくつあるかに依存するのである。ガウスの 17 角形の背後にある鍵となる計算には Section 6.2（STEP II 1991, Question 4）で出会うことになる。そして物語の全貌は、大学の学部課程の白眉の一つである**ガロア理論**（Galois theory）に属している。

一つの定理、多くの証明

数学者はなぜ同じ定理を何度も証明しようとするのだろうか。それは、異なる証明が異なることを明らかにするからである。この証明は通常、クリスティアン・ゴールドバッハ（Christian Goldbach）が 1730 年にオイラーに宛てた手紙によるものとされるが、これは、1 より大きい整数からなり、どの二つも互いに素であるような**任意の**無限数列が、無限に多くの素数の存在を導くことを示している。フェルマー数はその便利な一例にすぎない。（演習 3 で別の例を扱う。）

この証明はまた、ユークリッドの証明よりも多くのことを教えてくれる。素数 $p_0, p_1, \ldots, p_{n-1}$ は n 個の**相異なる**素数であり、それぞれ F_{n-1} 以下である。したがって、$2^{2^{n-1}} + 1$ 以下の素数は少なくとも n 個ある。これは素数がどのように分布しているかについての**定量的**（quantitative）な主張である。非常に弱い主張ではある（実際にはずっと良いことが成り立つ）が、素数がどのようにまばらになっていくかを正確に記述する、19 世紀数学の偉大な成果の一つである**素数定理**（Prime Number Theorem）への第一歩なのである。Section 1.2 でその次の一歩を踏み出す。

思考のスキル

構造的な性質から議論を組み立てる

種類 A の対象が無限に存在することを示すには、種類 B の対象を無限に見つけ、そのそれぞれが自分専用の種類 A の対象を必要とするようにせよ。

ここでは A = 素数、B = フェルマー数であり、「自分専用のものを必要とする」とは「他のどれとも共有しない素因数をもつ」ことを意味する。同じパターンは、数え上げの議論や、線形代数（無限に多くの一次独立なベクトルがあれば次元は無限になる）、そして解析学にも現れる。

また、帰納法、とりわけ「k から $k+1$ へのステップは実際に何をしているのか」と問う習慣も練習した。この問いは、形式的なひな形よりも役に立つことが多い。

次の一歩

1 **ユークリッドの証明。** 素数が無限に存在することのユークリッドによる証明を書き出せ。それはどのような意味で「背理法（contradiction）による」証明であり、フェルマー数による証明はどのような意味で「構成的（constructive）」な証明であるか。

2 **一の位の数字。** $n \geq 2$ のとき、フェルマー数 F_n の一の位は 7 であることを示せ。

3 **シルベスター（Sylvester）の数列。** $a_1 = 2$、$a_{n+1} = a_n^2 - a_n + 1$ と定める。この数列は $2, 3, 7, 43, 1807, \ldots$ と始まる。

   (a) $a_{n+1} - 1 = a_1 a_2 \cdots a_n$ を示せ。

   (b) 各項はどの二つも互いに素であることを導き、それにより素数が無限に存在することの別証明を与えよ。

   (c) やや難 $\dfrac{1}{a_1} + \dfrac{1}{a_2} + \cdots + \dfrac{1}{a_n} = 1 - \dfrac{1}{a_{n+1} - 1}$ を示せ。

4 **オイラーの技法。** この問題ではフェルマーの小定理（*Fermat's Little Theorem*）を用いる。すなわち、p が素数で $p \nmid a$ ならば $a^{p-1} \equiv 1 \pmod{p}$ である。素数 p が F_n を割り切るとする。

   (a) $2^{2^n} \equiv -1 \pmod{p}$ を示し、それにより $2^{2^{n+1}} \equiv 1 \pmod{p}$ を示せ。

   (b) d を $2^d \equiv 1 \pmod{p}$ を満たす最小の正の整数とする。d は 2^{n+1} を割り切るが 2^n は割り切らないことを示し、$d = 2^{n+1}$ であると結論せよ。

(c) フェルマーの小定理を用いて、d が $p-1$ を割り切ることを示せ。それにより $p \equiv 1 \pmod{2^{n+1}}$ を導け。

(d) $n = 5$ のとき、これは F_5 の任意の素因数が $64k+1$ の形をしていることを意味する。641 がこの形であることを確かめよ。641 より小さいこの形の素数はいくつあるか。

5 素数の上界。一つの定理、多くの証明の議論を用いて、n 番目の素数は $2^{2^{n-1}}+1$ 以下であることを示せ。$n = 5$ のとき、この上界はどの程度良いか。

さらに学ぶために

- **Martin Aigner & Günter M. Ziegler, *Proofs from THE BOOK***（Springer）、第 1 章「Six proofs of the infinity of primes」（素数が無限に存在することの六つの証明）。この証明が、ユークリッドの証明や、位相空間論を用いるものを含む他の四つの証明とともに収められている。大学入学前に読める最良の本の一つである。
- **Harold Davenport, *The Higher Arithmetic***（Cambridge University Press）、第 1–2 章。素数と素因数分解への見事な筆致の入門書であり、大学入学前の夏に読むのに理想的である。
- **Michal Křížek, Florian Luca & Lawrence Somer, *17 Lectures on Fermat Numbers***（Springer, 2001）。オイラーによる因数分解からガウスの多角形まで、フェルマー数のすべてが書かれている。最初のほうの章を拾い読みするとよい。
- **Ian Stewart, *Why Beauty Is Truth***（Basic Books）、ガウスについての章。17 角形の物語が一般読者向けに語られている。

1.2 素数はどれほどまばらか？

問題

STEP III 2016、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/16-s3-q5`

導入

Section 1.1 では、素数（prime）が無限に存在することを見た。しかし「無限に存在する」というのは大ざっぱな主張である。素数は確かにまばらになっていく。100 未満の素数は 25 個あるが、900 と 1000 の間には 14 個しかない。では、素数は**どの程度**まばらになるのだろうか。

この問題で証明するのは、一見ごく控えめな事実である。n 以下のすべての素数を掛け合わせると、その積は 4^n より小さい。しかしこの何気ない不等式（inequality）こそが「どの程度まばらか」という問いに答えるための最初の本格的な一歩であり、1932 年に若きポール・エルデシュ（Paul Erdős）が与えた、数学で最も有名な短い証明の一つにおける鍵となる補題（lemma）なのである。

取りかかる前に

記号 $P_{r,s}$ は煩わしく見えるが、考え方は単純で、ある範囲にある素数を掛け合わせるだけである。例をしっかり理解しておこう。$P_{3,7}$ は 3 より大きく 7 以下の素数、すなわち 5 と 7 を用いるので、35 となる。

? **考えてみよう** 小問 (iv) では、**すべての** $n \geq 2$ について命題を証明することが求められている。小問 (iii) では、$2m$ までのすべての k について命題が成り立つと仮定している。これはどのような帰納法（induction）だろうか。

これは**強い**帰納法（strong induction）である。n の場合を証明するために、直前の場合だけでなく、それ以前の**すべての**場合を仮定してよい。このことを覚えておこう。

問題がこのように構成されているのはそのためである。

順を追って解く

段階 1　二項係数（binomial coefficient）はそれほど大きくない

> **考えてみよう**　$(1+x)^{2m+1}$ の二項展開（binomial expansion）で $x=1$ とおくと何が得られるか。

次が得られる。

$$2^{2m+1} = \binom{2m+1}{0} + \binom{2m+1}{1} + \cdots + \binom{2m+1}{2m+1}.$$

すべての項は正なので、どの項も 2^{2m+1} より小さい。しかしこれでは少し足りない。欲しいのは 2^{2m}、つまりその半分である。

> **考えてみよう**　パスカルの三角形（Pascal's triangle）は左右対称である。和の中で $\binom{2m+1}{m}$ と等しい項は他にどれか。

対称性より $\binom{2m+1}{m} = \binom{2m+1}{m+1}$ であり、これらは和の中の**異なる 2 つの項**である（$m \neq m+1$ だから）。したがって

$$2\binom{2m+1}{m} = \binom{2m+1}{m} + \binom{2m+1}{m+1} < 2^{2m+1},$$

となる。和には $\binom{2m+1}{0} = 1$ など他の正の項も含まれているので、不等号は等号を含まない。2 で割ると $\binom{2m+1}{m} < 2^{2m}$ を得る。 ■

段階 2　その二項係数を割り切る素数はどれか

二項係数を書き下すと、

$$\binom{2m+1}{m} = \frac{(2m+1)!}{m!\,(m+1)!} = \frac{(m+2)(m+3)\cdots(2m+1)}{m!}.$$

> **考えてみよう**　p を $m+1 < p \le 2m+1$ を満たす素数とする。p は分子を割り切るか。分母を割り切ることはあり得るか。

分子 $(m+2)(m+3)\cdots(2m+1)$ は因数の一つとして p 自身を含むので、p はこれを割り切る。分母 $m!$ はすべて p より小さい数の積である。p は素数なので、どれも p で割り切れない数の積を割り切ることはできない。よって p は分子を割り切るが分母は割り切らず、したがって二項係数全体（これが整数であることを思い出そう）を割り切る。

> **手を止めて、やってみよう** これで、この範囲にある各素数が $\binom{2m+1}{m}$ を割り切ることがわかった。では、なぜそれらの積 $P_{m+1,2m+1}$ もこれを割り切るといえるのか。（注意：4 と 6 がともにある数を割り切っても、24 がその数を割り切るとは限らない。）

違いは、ここでの素数が**相異なる素数**であることにある。相異なる素数 $p_1, p_2, \ldots$ がそれぞれ N を割り切るならば、それらの積も N を割り切る。実際、$N = p_1 N_1$ と書くと、p_2 は $p_1 N_1$ を割り切るが p_1 は割り切らないので、N_1 を割り切る。以下同様である。（ここでは、素数がある積を割り切るならばその因数のいずれかを割り切る、という事実を用いている。この事実には少し立ち止まって敬意を払う価値がある。Section 1.7 では、これに相当する性質が成り立たない世界を紹介する。）

よって $P_{m+1,2m+1}$ は $\binom{2m+1}{m}$ を割り切り、正の数の約数はその数を超えないので、

$$P_{m+1,\,2m+1} \le \binom{2m+1}{m} < 2^{2m}. \qquad \blacksquare$$

段階 3 積を分割する

> **考えてみよう** $2m+1$ 以下のすべての素数の積 $P_{1,2m+1}$ を、すでにわかっている積からどのように組み立てられるか。

$2m+1$ 以下の素数を、$m+1$ 以下のものと $m+1$ より大きいものに分ける。

$$P_{1,2m+1} = P_{1,m+1} \times P_{m+1,2m+1}.$$

2 つ目の因数は段階 2 より $2^{2m} = 4^m$ より小さい。1 つ目については、2 から $2m$ までのすべての k について $P_{1,k} < 4^k$ を仮定してよく、$k = m+1$ はこの範囲に入っている（$m \ge 1$ より $2 \le m+1 \le 2m$ だから）。したがって

$$P_{1,2m+1} < 4^{m+1} \times 4^m = 4^{2m+1}. \qquad \blacksquare$$

ここで強い帰納法がその真価を発揮する。$2m+1$ の場合を扱うのに必要だったのは、直前の場合ではなく、およそ**半分**の大きさである $m+1$ の場合だったのである。

段階 4 すべての n

> **考えてみよう** 小問 (iii) は奇数を扱っている。偶数 $n = 2m+2$ の場合はどうなるか。それは素数だろうか。

まず出発点を確認する。$P_{1,2} = 2 < 16$、$P_{1,3} = 6 < 64$ である。次に、$n \ge 4$ として、2 から $n-1$ までのすべての k について $P_{1,k} < 4^k$ が成り立つと仮定する。

- n が偶数ならば、n は（2 より大きいので）素数ではなく、n 以下の素数は $n-1$ 以下の素数と同じである。よって $P_{1,n} = P_{1,n-1} < 4^{n-1} < 4^n$ となる。
- n が奇数ならば、$m \geq 2$ として $n = 2m+1$ と書く。すると小問 (iii) により直ちに $P_{1,n} < 4^n$ を得る。

強い帰納法により、すべての $n \geq 2$ について $P_{1,n} < 4^n$ が成り立つ。 ■

振り返り

- **二項係数は数論的な情報を担っている。** $\binom{2m+1}{m}$ は（4^m 未満という）小さな一つの数でありながら、多くの素数で割り切れざるを得ない。多くの素数を小さな数に押し込むことで、それらの素数がそれほど多くはあり得ないことがわかるのである。
- **問題が自らを半分にするとき、強い帰納法は自然な道具である。** $2m+1$ の場合は $m+1$ の場合に依存していた。
- **小さな場合は別に確認する必要がある。** 帰納法が回り始めるのは $n \geq 4$ からなので、$n = 2$ と 3 は手で確かめなければならなかった。

背後にある数学

4^n から素数定理（Prime Number Theorem）へ

結果の対数（logarithm）をとると $\ln P_{1,n} < n \ln 4$、すなわち

$$\sum_{p \leq n} \ln p < (\ln 4)\, n \approx 1.39\, n.$$

となる。1850 年代にパフヌティ・チェビシェフ（Pafnuty Chebyshev）は、まさにこの種の評価を上からも下からも証明し、$\sum_{p \leq n} \ln p$ が n に比例して増大することを示した。ガウス（Gauss）はそれ以前、およそ 15 歳のときにすでに、数表から n 以下の素数の個数はおよそ $n/\ln n$ であると予想していた。これが**素数定理**となり、1896 年にジャック・アダマール（Jacques Hadamard）とシャルル・ド・ラ・ヴァレ・プーサン（Charles de la Vallée Poussin）が複素解析（complex analysis）を用いてついに証明した。対数の形で述べると

$$\sum_{p \leq n} \ln p \sim n,$$

であり、したがって n 以下の素数の積はおよそ e^n である。我々の上界 4^n はまったく的外れではない。図 1.2.1 に 3 つすべてを示す。

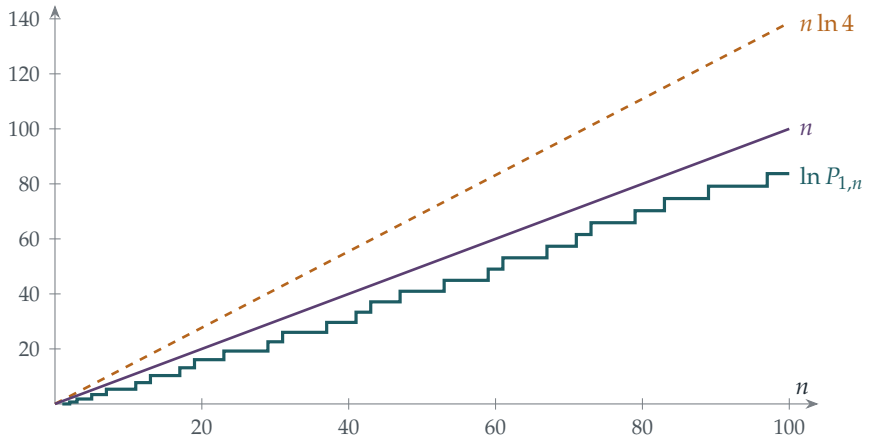


図 1.2.1　n 以下のすべての素数の積の対数（青緑）。各素数 p で $\ln p$ だけ跳ね上がる。本節では、これが $n \ln 4$（琥珀色、破線）より下にとどまることを証明する。素数定理によれば、これは n（紫）と同じように増大する。

ベルトランの仮説（Bertrand's postulate）

1845 年にジョゼフ・ベルトラン（Joseph Bertrand）は、すべての $n \geq 1$ について n と $2n$ の間に必ず素数が存在すると予想した。チェビシェフは 1852 年にこれを証明した。その 80 年後、19 歳のポール・エルデシュが美しい初等的証明を見いだした。その鍵となる要素は、この問題の補題と、**中央二項係数** $\binom{2n}{n}$ を割り切る素数がどれかを注意深く調べることである。Martin Aigner と Günter Ziegler は、数学で最も優美な証明を集めた *Proofs from THE BOOK* の第 2 章としてこの証明を選んだ。

この先へ

素数の正確な分布は、リーマンゼータ関数（Riemann zeta function）

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots,$$

の零点によって支配されている。この関数には Section 2.4 で、ずっと控えめな姿で出会うことになる。そこでは $\zeta(2) = \pi^2/6$ である。これらの零点がどこにあるかを正確に予言する**リーマン予想**（Riemann Hypothesis）が正しければ、素数定理の誤差を可能な限り厳しく押さえ込むことができる。これはおそらく数学で最も有名な未解決問題であり、ミレニアム懸賞問題（Millennium Prize Problems）の一つでもある。

思考のスキル

強い帰納法と、巧妙な対象から情報を引き出すこと

n の場合が $n-1$ よりずっと小さい場合に依存するときは、それ以前のすべての場合を一度に仮定せよ。

ここでのもう一つの考え方はより繊細で、数論（number theory）に極めて特徴的なものである。ある範囲の**すべての**素数について何かを示すには、それらの素数のどれもが割り切らなければならず、しかもそれほど大きくないことも示せるような一つの対象（ここでは二項係数）を見つけるのである。

次の一歩

1. **数の感覚をつかむ。** $n = 10, 20, 30$ について $P_{1,n}$ を計算し、4^n および e^n と比較せよ。（ここでは電卓を使ってよい。）

2. **中央二項係数。** $\binom{2m}{m}$ が $(1+1)^{2m}$ の展開における $2m+1$ 個の項の中で最大であることを示し、$\binom{2m}{m} \geq \dfrac{4^m}{2m+1}$ を導け。

3. **素数はそれほど多くない。** $\pi(n)$ を n 以下の素数の個数とする。$\sqrt{n}$ と n の間にある素数はすべて $\sqrt{n}$ より大きく、それらの積は $P_{1,n} < 4^n$ 以下である。これより

$$\pi(n) - \pi(\sqrt{n}) < \frac{2 \ln 4}{\ln n}\, n,$$

   を導き、さらに $\pi(n) < 2.8\, n / \ln n + \sqrt{n}$ を導け。これを素数定理の $\pi(n) \approx n / \ln n$ と比較せよ。

4. **ベルトランの仮説を確かめる。** $n = 1, 2, \ldots, 50$ のそれぞれについて n と $2n$ の間にある素数を見つけることで、ベルトランの仮説を確かめよ。各素数が直前の素数の 2 倍未満であるような短い素数のリストを使って、効率よく確かめられるだろうか。

さらに学ぶために

- **Aigner & Ziegler, *Proofs from THE BOOK***、第 2 章「Bertrand's postulate」（ベルトランの仮説）。
- **Marcus du Sautoy, *The Music of the Primes***（Fourth Estate）。素数定理とリーマン予

想の歴史を一般向けに描いた本。

- **G. J. O. Jameson, *The Prime Number Theorem***（Cambridge University Press）。厳密でありながら平易で、学部生向けに書かれている。最初の数章は A レベル（A level、英国の大学入学資格試験）程度の微積分しか必要としない。

1.3 最小の反例

問題

STEP III 2015、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/15-s3-q5`

導入

$\sqrt{2}$ が無理数（irrational）であることの証明は、おそらく見たことがあるだろう。$\sqrt{2} = a/b$ を既約分数と仮定し、両辺を 2 乗して、a が偶数であること、続いて b も偶数であることを導き、矛盾を得るというものである。これは立派な証明である。しかし、この証明は**偶数**に関する技巧に頼っており、それがそのまま一般化できるかどうかは明らかでない。$\sqrt[3]{2}$ ならどうだろうか。$\sqrt{7}$ ならどうだろうか。

この問題は別の証明を与えるものであり、その中心にある考え方はほとんど拍子抜けするほど単純である。それは**最小のものに注目せよ**ということである。同じ考え方は、姿を変えて、この章で何度も再登場する。

取りかかる前に

これは STEP の問題としては珍しいものである。証明の骨組みが与えられ、欠けている根拠を埋めることが求められている。これはまさに、大学生が数学の読み方を身につけるやり方そのものである。教科書の証明にはしばしば「明らかに」や「このことから〜が従う」と書かれており、それが本当にそうなっているかを確かめるのも読み手の仕事の一部である。

? **考えてみよう** ステップ 4 では「k を S に属する最小の正の整数と定める」とある。なぜそうしてよいのだろうか。S が正の**実数**の集合であったとしても、それは許されるだろうか。

正の整数からなる空でない集合には、必ず最小元が存在する。これを**整列性原理**

（well-ordering principle）といい、数学的帰納法（mathematical induction）の原理と同値である。正の実数の集合に対しては、これは**成り立たない**。実際、集合 $\{x : x > 0\}$ には最小元がない。したがって、ステップ 4 はステップ 3（集合が空でないこと）と、S が整数からなることに依存している。

順を追って解く

段階 1　ステップ 3：S は空でない

> **考えてみよう**　正の整数 a, b によって $\sqrt{2} = a/b$ と書けるとき、S の元を一つ具体的に書き出せるだろうか。

$\sqrt{2} = a/b$ ならば $b\sqrt{2} = a$ であり、これは整数である。よって b は S に属し、S は空でない。

段階 2　ステップ 5：より小さい元

さて、k は S の最小元であるから、$k\sqrt{2}$ は整数である。これを j とおく。

> **手を止めて、やってみよう**　$(\sqrt{2}-1)k$ が S に属することを示すには、三つのことを確かめなければならない。それは何だろうか。

$(\sqrt{2}-1)k$ が (a) 整数であり、(b) 正であり、(c) $\sqrt{2}$ を掛けると整数になる、ということを示す必要がある。

- (a) $(\sqrt{2}-1)k = k\sqrt{2} - k = j - k$ であり、これは整数どうしの差である。
- (b) $\sqrt{2} > 1$ より $\sqrt{2} - 1 > 0$ であるから、$(\sqrt{2}-1)k > 0$ である。
- (c) $(\sqrt{2}-1)k \cdot \sqrt{2} = 2k - k\sqrt{2} = 2k - j$ であり、これは整数である。

よって $(\sqrt{2}-1)k \in S$ である。

段階 3　ステップ 6：矛盾

> **考えてみよう**　$\sqrt{2} - 1$ はどのくらいの大きさだろうか。

$1 < \sqrt{2} < 2$ であるから $0 < \sqrt{2} - 1 < 1$ であり、したがって $(\sqrt{2}-1)k < k$ である。こうして、S の最小元である k よりも小さい S の元が見つかった。これは不可能であるから、ステップ 1 の仮定は誤りであった。すなわち $\sqrt{2}$ は無理数である。 ■

「既約分数」も、偶数・奇数に関する性質も一切使わなかったことに注意しよう。証明全体は三つの事実の上に成り立っている。$\sqrt{2}\cdot\sqrt{2}$ が整数であること、$\sqrt{2}$ が連続する二つの整数の真に間にあること、そして整数が整列性をもつことである。

段階 4 立方根：二つの数を結びつける

$c = 2^{1/3}$ とおくと、$c^2 = 2^{2/3}$ かつ $c^3 = 2$ である。

> **考えてみよう** c が有理数（rational）ならば、c^2 も有理数だろうか。また、c^2 が有理数ならば、掛け算と割り算だけを使って c に戻れるだろうか。

c が有理数ならば、$c^2 = c \times c$ も有理数である。逆に、c^2 が有理数ならば、$2/c^2 = c^3/c^2 = c$ も有理数である。よって、$2^{1/3}$ が有理数であることと $2^{2/3}$ が有理数であることは同値である。 ■

段階 5 議論を応用する

> **考えてみよう** 小問 (i) での鍵は $(\sqrt{2})^2 = 2$ が整数であることであった。そのため、S の元に $\sqrt{2}$ を 2 回掛けると整数に戻る。$c = 2^{1/3}$ の場合は 3 回掛ける必要がある。集合 S をどのように変えればよいだろうか。

c が有理数であると仮定する。このとき c^2 も有理数である。

$$S = \{n \text{ は正の整数} : nc \text{ と} nc^2 \text{ はともに整数}\}.$$

と定める。

- **S は空でない。** $c = a/b, c^2 = a'/b'$ とすると、bb' は S に属する。
- **k をその最小元とし、** $(c-1)k$ を考える。$1 < c < 2$（$1^3 < 2 < 2^3$ による）であるから、$0 < (c-1)k < k$ である。
- **これは整数である：** $(c-1)k = kc - k$。
- **c を掛けると：** $(c-1)k \cdot c = kc^2 - kc$ であり、これは整数である。
- **c^2 を掛けると：** $(c-1)k \cdot c^2 = kc^3 - kc^2 = 2k - kc^2$ であり、これは整数である。

よって $(c-1)k \in S$ であり、しかも k より小さい。これは矛盾である。したがって $2^{1/3}$ は無理数であり、段階 4 により $2^{2/3}$ も無理数である。 ■

振り返り

- **「最小のものをとる」は証明の技法である。** 反例が存在すると仮定し、その最小のも

のをとって、さらに小さい反例を作り出す。これを**極端原理**（extremal principle）、あるいは**最小反例**（minimal counterexample）による議論という。

- **集合 S が帳簿係を務めた。**分子と分母をあれこれ操作する代わりに、「よい」乗数をすべて一つの集合にまとめたのである。
- **一般化とは、何が本当に証明を成り立たせていたのかを問うことであった。**$\sqrt{2}$ の場合は $\sqrt{2}$ を 1 回掛ければよく、$\sqrt[3]{2}$ の場合は 2 回必要であった。このことに気づいたおかげで、S をどう定義し直せばよいかが正確にわかった。

背後にある数学

図に描ける証明

小問 (i) の背後には、Stanley Tennenbaum による美しい図がある。$\sqrt{2} = a/b$ ならば $a^2 = 2b^2$ である。つまり、一辺 a の正方形は、一辺 b の正方形 2 個と同じ面積をもつ。図 1.3.1 のように、二つの b の正方形を a の正方形の向かい合う隅に置く。すると、それらは小さな正方形の部分で重なり、また覆われない小さな正方形が二つ残る。面積が等しいことから、重なった部分は覆われない二つの正方形を合わせたものに等しくなければならず、同じ性質をもつ**より小さい**整数の組が得られる。より小さい組がいつまでも続くことはありえないので、そのような正方形は存在しない。より小さい組はちょうど $(2b - a,\ a - b)$ であり、これは私たちの $(\sqrt{2} - 1)k$ のステップが姿を変えたものにほかならない。

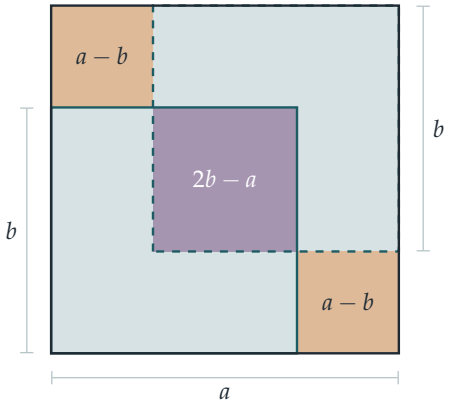


図 1.3.1 Tennenbaum の証明。一辺 b の二つの正方形（ティール色）が、一辺 a の正方形の向かい合う隅に置かれている。$a^2 = 2b^2$ ならば、2 回数えられた面積（プラム色の重なり）は数えられなかった面積（二つのアンバー色の隅）に等しくなければならないので、$(2b - a)^2 = 2(a - b)^2$ となる。これはより小さい解である。

整列性、帰納法、降下法

整列性原理と帰納法の原理は論理的に同値である。すなわち、それぞれが他方から証明できる。大学では、どちらも自然数の基礎として用いられるのを目にするだろう。Section 1.5 では、同じ原理を別の形、すなわちフェルマー（Fermat）の**無限降下法**（method of infinite descent）として用いる。それは、正の整数からなる狭義単調減少の無限数列は存在しない、という形である。

どこまで通用するか

この議論によって、N が平方数（perfect square）でないときには必ず $\sqrt{N}$ が無理数であること（演習を参照）、さらに一般に、整数の n 乗根は整数であるか無理数であるかのいずれかであることが証明できる。大学では、これは**代数的整数**（algebraic integers）に関する主張となる。すなわち、$x^3 - 2 = 0$ のような、整数係数のモニック多項式（monic polynomial）の方程式を満たす有理数は、整数でなければならない。この考え方には Section 6.3 で再び出会うことになる。

ピタゴラス学派（Pythagoreans）が $\sqrt{2}$ の無理性を明かしたヒッパソス（Hippasus）を溺死させたという伝説は、おそらく事実ではない。確かなのは、この発見によってギリシャの数学者たちが数の研究と長さの研究を切り離さざるをえなくなったということである。この分裂が癒やされるには、19 世紀、そしてデデキント（Dedekind）による実数の構成を待たなければならなかった。

思考のスキル

極端原理

あることが決して起こらないことを示したいときは、それが起こると仮定し、その最小の（あるいは最大の、あるいは最も単純な）例を選び、それを用いてさらに小さい例を作れ。

「最小」が何を意味するかの選び方こそが、創造的なステップである。ここでは、それは $n\sqrt{2}$ を整数にする最小の n であった。

次の一歩

1. **ほかの平方根。** この議論を応用して、$\sqrt{3}$ が無理数であることを示せ。$\sqrt{2}-1$ の役割を果たすのはどの数か。

2. **平方数でないものすべて。** N を平方数でない正の整数とし、m を $m < \sqrt{N} < m+1$ を満たす整数とする。$(\sqrt{N}-m)k$ を考えることにより、$\sqrt{N}$ が無理数であることを証明せよ。

3. **誤りを見つけよ。** この議論を $\sqrt{4}$ に対して実行してみよ。正確にはどのステップで破綻するか。

4. **Tennenbaum の図。** 図 1.3.1 を用いて、$a^2 = 2b^2$ ならば $(2b-a)^2 = 2(a-b)^2$ であることを示せ。また、この恒等式を代数的にも確かめよ。

さらに学ぶために

- **Daniel Velleman, *How to Prove It***（Cambridge University Press）。帰納法や整列性を含む、証明への徹底した入門書。
- **R. P. Burn, *A Pathway into Number Theory***（Cambridge University Press）。注意深く順序立てられた問題だけで構成された本。大学 1 年次の講義への準備として理想的である。
- **John Conway & Joseph Shipman,「Extreme proofs I: the irrationality of $\sqrt{2}$」**(*Mathematical Intelligencer*, 2013)。一つの事実に対する多くの証明を、機知に富んだ筆致で比較している。

1.4 e は無理数であり、e^2 もまた無理数である

この節では 2 つの問題を扱う。1 つ目は 1997 年の問題で、e が無理数（irrational）であることを証明する。2 つ目は 2024 年の問題で、同じ考え方をより巧妙にした形を用いて e^2 が無理数であることを証明する。こちらは本当に難しくなる。

ウォームアップ

STEP III 1997、問 7

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-s3-q7`

本題

STEP III 2024、問 7

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 2024 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/725753-2024-past-papers.zip`

導入

Section 1.3 では、$\sqrt{2}$ が単純な方程式 $x^2 = 2$ を満たすという事実を用いて、$\sqrt{2}$ が無理数であることを証明した。しかし e は、知られている限りそのような方程式を満たさない。手がかりは次の級数（series）だけである。

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots .$$

級数から、ある数が分数でないことがどうしてわかるのだろうか。

その答えは、数論（number theory）で最も役に立つ考え方の 1 つである。すなわち、**整数は 0 と 1 の間に（両端を除いて）存在しえない**。ある量が整数であり、しかも 0 より大きく 1 より小さいことを示せれば、矛盾（contradiction）が得られる。この節の内容はすべて、この主題の変奏である。

取りかかる前に

考えてみよう　$e = p/q$ と仮定する。e に q を掛けると整数になる。では、$q!$ を掛けると e の級数の各項はどうなるか。

$k \le q$ であれば、$\dfrac{1}{k!}$ に $q!$ を掛けると整数になる。したがって $q!\,e$ は、整数の部分（最初の $q+1$ 項）と「裾」（tail、それ以降のすべて）に分かれる。$e = p/q$ ならば $q!\,e$ 自身が整数なので、裾も整数でなければならない。方針は、裾が 0 と 1 の間に（両端を除いて）あることを示すことである。

順を追って解く

段階 1　ウォームアップ：e は無理数である

級数 b_n は初項と公比がともに $\frac{1}{n+1}$ の等比級数（geometric series）であるから、

$$b_n = \frac{1/(n+1)}{1 - 1/(n+1)} = \frac{1}{n}.$$

考えてみよう　a_n と b_n を項ごとに比べよ。どちらが大きいか。

初項は等しい。それ以降は $(n+1)(n+2) > (n+1)^2$ であり、一般に $k \ge 2$ に対して $(n+1)(n+2)\cdots(n+k) > (n+1)^k$ が成り立つので、a_n の 2 項目以降の各項は b_n の対応する項より小さい。よって $0 < a_n < b_n = 1/n$ である。

ここで a_n が実際には何であるかを見てみよう。e の級数に $n!$ を掛けると

$$n!\,e = \underbrace{\frac{n!}{0!} + \frac{n!}{1!} + \cdots + \frac{n!}{n!}}_{\text{整数}} + \underbrace{\frac{n!}{(n+1)!} + \frac{n!}{(n+2)!} + \cdots}_{= a_n}.$$

$0 < a_n < 1$ であるから、$n!\,e$ の整数部分は最初のまとまりであり、a_n は小数部分（fractional part）である。すなわち $a_n = n!\,e - [n!\,e]$ である。

手を止めて、やってみよう　では証明を完成させよう。$e = p/q$ と仮定する。n をどの値に選べばよいか。

$n = q$ とする。すると $q!\,e = (q-1)!\,p$ は整数なので、その小数部分 a_q は 0 である。しかし $a_q > 0$ である。これは矛盾であり、e は無理数である。 ■

この証明は、1815 年ごろのフーリエ（Fourier）によるものである。

段階 2 e^2 が難しい理由

考えてみよう 同じ考え方を e^2 に試してみよ。その級数は $\sum 2^k/k!$ である。$n!$ を掛けて裾を見ると、何がうまくいかないか。

今度は裾が $\dfrac{2^{n+1}}{n+1} + \dfrac{2^{n+2}}{(n+1)(n+2)} + \cdots$ となり、2 のべきがすべてを台無しにする。裾はもはや小さくないのである。$n!$ を掛けても、分子の 2^k には何の効果もない。

2024 年の問題の工夫は、e^2 をまったく扱わないようにすることである。$e^2 = p/q$ ならば

$$qe = \frac{p}{e}.$$

こうすると 2 つの数 e と $1/e$ が得られ、どちらも階乗（factorial）による級数をもち、厄介な 2 のべきを含まない。

$$e = \sum_{k=0}^{\infty} \frac{1}{k!}, \qquad \frac{1}{e} = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!}.$$

段階 3 2 つの裾

小問 (i) はウォームアップそのものであり、$0 < f(n) < 1/n$ である。

小問 (ii) の $g(n)$ は、項の大きさが減少していく**交代級数**（alternating series）である。

考えてみよう $t_1 > t_2 > t_3 > \cdots > 0$ である交代級数 $t_1 - t_2 + t_3 - \cdots$ について、和が 0 と t_1 の間にあるのはなぜか。

項を 2 つずつ組にすると、$(t_1 - t_2) + (t_3 - t_4) + \cdots$ は正の括弧の和なので正である。組み方を変えると、$t_1 - (t_2 - t_3) - (t_4 - t_5) - \cdots$ は t_1 から正の括弧を引いたものなので t_1 より小さい。ここでは $t_1 = \frac{1}{n+1}$ であり、各項は前の項を 1 より大きい数で割ったものなので項は減少する。よって $0 < g(n) < \frac{1}{n+1}$ である。

段階 4 再び整数

ウォームアップとまったく同様に、e に $(2n)!$ を掛けて裾を切り離すと

$$(2n)!\, e = (\text{整数}) + f(2n).$$

よって $(2n)!\, e - f(2n)$ は整数である。$1/e$ についても同じことを行うと

$$\frac{(2n)!}{e} = \sum_{k=0}^{2n} (-1)^k \frac{(2n)!}{k!} + \sum_{k=2n+1}^{\infty} (-1)^k \frac{(2n)!}{k!}.$$

考えてみよう　裾の最初の項 $k=2n+1$ の符号は何か。裾は $g(2n)$ とどのような関係にあるか。

裾の最初の項は $k=2n+1$ で奇数なので、負である。裾は

$$-\frac{1}{2n+1}+\frac{1}{(2n+1)(2n+2)}-\cdots=-g(2n).$$

よって $\dfrac{(2n)!}{e}+g(2n)$ は整数である。 ■

問題で n ではなく $2n$ を用いているのはこのためである。偶数の階乗を掛けると、$1/e$ の裾は予測どおりの符号をもち、ちょうど $-g$ になる。

段階 5　矛盾

$qe=p/e$ と仮定する。両辺に $(2n)!$ を掛け、段階 4 を用いると

$$q\bigl(\text{整数}+f(2n)\bigr)=p\bigl(\text{整数}-g(2n)\bigr).$$

整理すると、$qf(2n)+pg(2n)$ は整数の組合せに等しいので整数である。これが小問 (iv) である。

手を止めて、やってみよう　では段階 3 で得た評価を使おう。n が非常に大きいとき、$qf(2n)+pg(2n)$ はどうなるか。

$f(2n)$ と $g(2n)$ はどちらも正なので、$qf(2n)+pg(2n)>0$ である。また

$$qf(2n)+pg(2n)<\frac{q}{2n}+\frac{p}{2n+1}<\frac{p+q}{2n}.$$

$n>(p+q)/2$ と選ぶ。すると $qf(2n)+pg(2n)$ は 0 と 1 の間に（両端を除いて）ある整数となる。これはありえないので、e^2 は無理数である。 ■

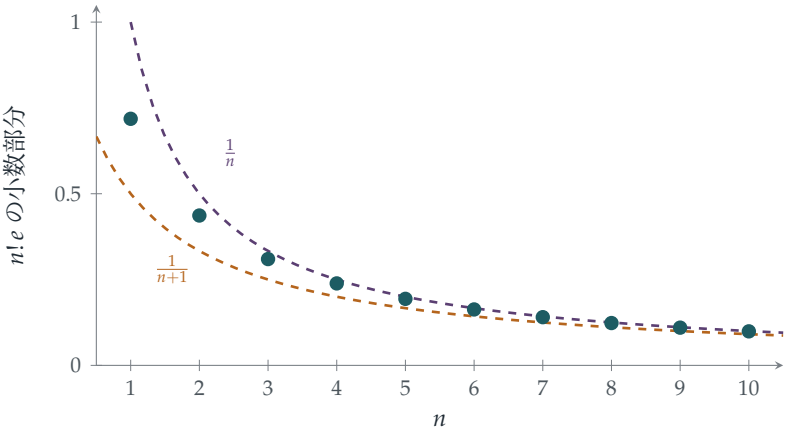


図 1.4.1　裾 $a_n = n!\,e - [n!\,e]$（青緑色）。これは $n!\,e$ の小数部分である。これは常に $\frac{1}{n+1}$ と $\frac{1}{n}$ の間に（両端を除いて）あり、決して 0 にはならないが、1 より小さい。もし e が分数 $\frac{p}{q}$ であれば、$n \geq q$ であるすべての n に対して $n!\,e$ は整数となり、青緑色の点は 0 になるはずである。

振り返り

- **原動力は「0 と 1 の間に（両端を除いて）整数は存在しない」ことである。**どちらの証明も、整数でなければならない量を作り、それを挟み込んでいる。
- **階乗は裾を小さくする。** $n!$ を掛けることで級数の初めの部分が整数になり、$1/n$ のように小さくなる裾が残った。
- **正面から攻めてうまくいかなければ、式を変形せよ。** $e^2 = p/q$ に正面から取り組む代わりに、$qe = p/e$ と書き直し、難しさを扱いやすい 2 つの数に分散させた。
- **細部が重要である。** n ではなく $2n$ を選んだことで、裾の符号が定まった。多くの証明は、このような小さな細部にかかっている。

背後にある数学

e はどれほど無理数なのか

リウヴィル（Liouville）は 1840 年に、e^2 が無理数であること、さらには整数係数の二次方程式（quadratic equation）を満たさないことを証明した。1873 年、エルミート（Hermite）ははるかに先へ進み、e が**超越数**（transcendental）であること、すなわち整数係数の**いかなる**多項式（polynomial）の根でもないことを証明した。その証明は、

まさに上の議論を高度にしたものである。つまり、整数を作り、それが 0 と 1 の間に（両端を除いて）あることを示すのである。その 9 年後、リンデマン（Lindemann）はエルミートの方法を応用して π が超越数であることを示し、定規とコンパスによる「円積問題」という古代からの問題が不可能であることをついに証明した。

まだわかっていないこと

これらの方法がこれほど強力であるにもかかわらず、きまりが悪いほど単純な問題が未解決のまま残っている。$e+\pi$ は無理数か。$e\pi$ はどうか。誰も知らない。ただし、少なくとも一方は超越数でなければならない（演習 4）。$\zeta(3) = 1 + \frac{1}{8} + \frac{1}{27} + \cdots$ は無理数か。答えは「はい」である。アペリー（Apéry）が 1978 年にこれを証明し、数学界を驚かせた。$\zeta(5)$ はどうか。誰も知らない。

近似

これらの証明の背後には、より深い考え方がある。それは、ある数が分数によって**あまりにもよく**近似できるならば、その数は無理数である、というものである。e の級数の部分和（partial sums）は、非常に速く e に非常に近づく分数である。分数は、他の分数によってそれほどよく近似されることはありえない。これが**ディオファントス近似**（Diophantine approximation）の出発点であり、数論のこの分野については Section 2.9 でさらに探究できる。そこでは別の種類の積分から、e にさらに迫るよりよい分数が得られる。

思考のスキル

整数を挟み込む

ある数が無理数であることを証明するには、それが分数であると仮定し、そこから整数でなければならない量を作り、その量が 0 と 1 の間に（両端を除いて）あることを示せ。

腕の見せどころは、その量の選び方にある。ここでは階乗を掛けることで級数の大部分が整数になり、小さいが正である裾が残った。

次の一歩

1 **$1/e$ だけを用いる。** $1/e = p/q$ と仮定し、$1/e$ の交代級数だけを用いて、e が無理数であることを証明せよ。

2 **$\sin 1$ は無理数である。** $\sin 1 = 1 - \dfrac{1}{3!} + \dfrac{1}{5!} - \cdots$ を用いて、$\sin 1$ が無理数であることを証明せよ。（適当な奇数の階乗を掛けよ。）

3 **なぜ π ではうまくいかないのか。** この方法が π に直接は使えない理由を説明せよ。次に、級数の代わりに積分を用いて π が無理数であることを示した、ニーヴン（Niven）による 1 ページの証明（1947 年）を調べよ。これは優秀な A レベル（A level、英国の大学入学資格試験）の生徒の手の届く範囲にある。

4 **どちらか一方は超越数である。** やや難 e と π が $x^2 - (e+\pi)x + e\pi = 0$ の根であることを示せ。係数が代数的数（algebraic number）である多項式の根はそれ自身代数的であること、および π が代数的でないこと（リンデマン）は仮定してよい。$e+\pi$ と $e\pi$ の少なくとも一方が超越数であることを導け。

さらに学ぶために

- **Aigner & Ziegler, *Proofs from THE BOOK***（『天書の証明』）、第 8 章「Some irrational numbers」（いくつかの無理数）。まさにこれらの考え方を用いて、e、e^2、e^4、π^2 が無理数であることを証明している。
- **Ivan Niven, *Irrational Numbers***（Mathematical Association of America）。$\sqrt{2}$ から超越性までを扱う、短い古典的名著である。
- **Julian Havil, *The Irrationals***（Princeton University Press）。無理数の歴史を読みやすく描いた本である。

1.5 無限降下法

問題

STEP III 2022、問 2

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 2022 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/696587-2022-past-papers.zip`

導入

ある方程式が整数解を**もたない**ことは、どうすれば証明できるだろうか。すべての可能性を試すことはできない。候補は無限にあるからである。1630 年代、フェルマー（Fermat）はその方法を見つけた。解が存在すれば、そこから**より小さい**数でできた別の解が得られ、さらにそこからもっと小さい解が得られ、これが果てしなく続くことを示すのである。しかし、正の整数がいつまでも小さくなり続けることはできない。したがって、そもそも解は存在しなかったことになる。

フェルマーはこれを**無限降下法**（method of infinite descent）と呼び、大いに誇りにしていた。これは Section 1.3 で扱った整列原理（well-ordering principle）の裏返しであり、方程式が解をもたないことを証明するための主要な道具の一つとして今も使われている。

取りかかる前に

四つの小問はすべて同じ形をしている。解があると仮定し、それを小さくし、矛盾（contradiction）を導く。問題は、**どうやって**小さくするかである。

? **考えてみよう** 小問 (i) の $a^3 + 2b^3 + 4c^3 = 0$ を見てみよう。三つの項のうち二つは明らかに偶数（even）である。このことから残りの一つについて何がわかるか。

このような観察こそ、あらゆる降下法の出発点である。ある種の整除性（divisibility）が否応なく課されるのである。

順を追って解く

段階 1　最初の降下

$a^3 = -2b^3 - 4c^3$ であるから a^3 は偶数であり、したがって a は偶数である（奇数の 3 乗は奇数だからである）。$a = 2p$ とおく。すると $|p| = |a|/2 < |a|$ であり、代入すると

$$8p^3 + 2b^3 + 4c^3 = 0 \quad \Longrightarrow \quad 4p^3 + b^3 + 2c^3 = 0.$$

となる。

> **考えてみよう**　新しい方程式は $4p^3 + b^3 + 2c^3 = 0$ である。係数は同じで、並びが巡回しただけである。同じ手法をもう一度使えるだろうか。

今度は $b^3 = -4p^3 - 2c^3$ が偶数であるから、$|q| < |b|$ を満たす q を用いて $b = 2q$ と書け、2 で割ると $2p^3 + 4q^3 + c^3 = 0$ を得る。もう一度、c は偶数でなければならない。$|r| < |c|$ を満たす r を用いて $c = 2r$ と書き、2 で割ると

$$p^3 + 2q^3 + 4r^3 = 0.$$

となる。これは a、b、c の代わりに p、q、r を入れた**もとの**方程式である。それぞれの大きさは半分になっており、しかもどれも 0 ではない。0 でない数を半分にしても 0 にはならないからである。

> **手を止めて、やってみよう**　これを、0 でない解が存在しないことの証明にまとめよ。正確には、何が「最小」であると仮定すべきだろうか。

0 でない整数からなるすべての解の中から、$|a|$ ができるだけ小さいものを一つ選ぶ（解が一つでも存在すれば、整列原理によってこれが可能である）。上の議論により、$|p| < |a|$ を満たす 0 でない別の解が得られ、最小性（minimality）に矛盾する。よって、0 でない解は存在しない。 ■

同じことを次のように言い換えることもできる。一つの解から、$|a| > |p| > \cdots$ となる解の無限列を作ることができる。これは正の整数からなる狭義単調減少の無限列であり、そのようなものは存在しない。

段階 2　別の素数

> **考えてみよう**　$9a^3 + 10b^3 + 6c^3 = 0$ では、偶奇性（parity）は明らかには役に立たない。係数 9、10、6 を見よう。そのうち二つを割り切る素数はどれか。

素数 3 は 9 と 6 を割り切るので、3 は $10b^3$ を割り切り、したがって 3 は b を割り切る。

$b = 3q$ とおいて 3 で割ると

$$3a^3 + 90q^3 + 2c^3 = 0.$$

となる。今度は 3 が $2c^3$ を割り切るので $c = 3r$ と書け、再び 3 で割ると $a^3 + 30q^3 + 18r^3 = 0$ を得る。よって 3 は a を割り切る。$a = 3p$ とおき、もう一度 3 で割ると

$$9p^3 + 10q^3 + 6r^3 = 0.$$

となる。これはまさにもとの方程式であり、数はより小さく、しかも 0 でない。同じ降下の議論により、0 でない解は存在しない。 ■

段階 3　3 を法とする平方数

> **考えてみよう**　すべての整数は $3n$、$3n+1$、$3n-1$ のいずれかの形をしている。それらの平方は、3 を法として（modulo）いくつになるか。

$(3n \pm 1)^2 = 9n^2 \pm 6n + 1 = 3(3n^2 \pm 2n) + 1$ であり、これは 3 の倍数より 1 大きい。また $(3n)^2$ は 3 の倍数である。したがって、平方数を 3 で割った余りは 0 または 1 であり、2 になることは決してない。

ここで $a^2 + b^2$ が 3 の倍数であるとすると、余りの組合せは $0+0$、$0+1$、$1+0$、$1+1$ であり、それぞれ 0、1、1、2 となる。3 の倍数になるのは最初の場合だけなので、a と b はともに 3 の倍数でなければならない。

> **考えてみよう**　$a^2 + b^2 = 3c^2$ かつ $a = 3p$、$b = 3q$ のとき、c について何が言えるか。

$9p^2 + 9q^2 = 3c^2$ となるので、$c^2 = 3(p^2 + q^2)$ は 3 の倍数であり、したがって $c = 3r$ と書ける。すると $9p^2 + 9q^2 = 27r^2$ より $p^2 + q^2 = 3r^2$ となる。同じ方程式で、数はより小さい。ここでも降下法が使える。 ■

段階 4　ひとひねり：方程式が変わる

> **考えてみよう**　$a^2 + b^2 + c^2 = 4abc$ では、右辺は 4 の倍数である。4 を法とする平方数はどうなるか。

偶数の平方は 4 の倍数であり、奇数の平方は 4 の倍数より 1 大きい（$(2n+1)^2 = 4n^2 + 4n + 1$）。したがって $a^2 + b^2 + c^2$ を 4 で割った余りは、a、b、c のうち奇数がいくつあるかに応じて 0、1、2、3 のいずれかとなる。右辺は 4 の倍数であるから、奇数のものは**一つもあってはならない**。$a = 2p$、$b = 2q$、$c = 2r$ とおくと

$$4(p^2 + q^2 + r^2) = 32\,pqr \quad \Longrightarrow \quad p^2 + q^2 + r^2 = 8\,pqr.$$

となる。

> **考えてみよう**　これはもとと同じ方程式ではない。4 が 8 になっている。それでも降下法はうまくいくだろうか。

ここでの工夫は、**より強い主張を証明する**ことである。次の形の方程式をすべて考える。

$$x^2 + y^2 + z^2 = 2^m\, xyz \qquad \text{ただし} m \geq 2.$$

このような m ならどれでも右辺は 4 の倍数であるから、まったく同じ議論によって x、y、z はすべて偶数であることがわかる。それらを半分にすると 2^{m+1} の方程式の解が得られ、これもまたこの形をしている。こうして、m の方程式の 0 でない解から、$m+1$ の方程式のより小さい 0 でない解が得られる。この族に属する**どの**方程式の解でもよいので、その中で $|x|$ が最小のものをとれば矛盾が生じる。特に、$a^2 + b^2 + c^2 = 4abc$ は 0 でない解をもたない。 ■

証明したい主張がそれ自身の帰納法（induction）を支えるには弱すぎることがあり、その場合の処方箋は、それ自身を支え**られる**より一般的な主張を証明することである。これは大学で驚くほどよく使われる手法である。

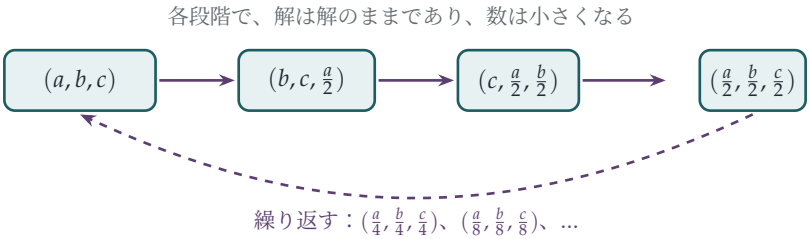


図 1.5.1　小問 (i) の降下。$a^3 + 2b^3 + 4c^3 = 0$ の解から、三つの段階を経て、すべての成分が半分になった別の解が得られる。これを永遠に繰り返すと、正の整数の果てしない減少列 $|a| > |\frac{a}{2}| > |\frac{a}{4}| > \cdots$ が得られることになるが、これは不可能である。したがって、そもそも解は存在しなかったのである。

振り返り

- **降下法には整除性の源が必要である。**毎回、すべての変数を割り切らざるを得ない素数 p（ここでは 2 または 3）を見つけ、それで割った。
- **それを見つけるには n を法として考えればよい。**2、3、4 を法とする余りを調べることで、「何かうまくいくものはあるか」という問いが、短い有限個の確認に変わった。
- **方程式が変わるなら、一般化せよ。**小問 (iv) では、降下の操作で閉じた方程式の

族全体が必要であった。

背後にある数学

フェルマー、降下法、そして最終定理

フェルマーは無限降下法を用いて、$x^4 + y^4 = z^2$ が正の整数解をもたないことを証明した。これは有名な「最終定理」（Last Theorem）のうち彼が証明を残した唯一の場合であり、$x^n + y^n = z^n$ の $n = 4$ の場合を解決するものである。のちにオイラー（Euler）が $n = 3$ の場合に降下法を用いた（その証明には欠陥があったが、後に補われた）。降下法は今でも現代の理論の出発点である。Section 1.9 に出てくるような曲線に関するモーデル–ヴェイユの定理（Mordell–Weil theorem）の証明は、高度に洗練された降下法なのである。

局所的障害

この節の証明はどれも、ある数を法とする余りを調べることで成り立っていた。ある n について方程式が n を法として解をもたないか、あるいは実数解をもたなければ、整数解ももたないことは確かである。このような理由を**局所的障害**（local obstructions）といい、大学では、$p, p^2, p^3, \ldots$ を法とするすべての余りを一度に調べる方法である **p 進数**（p-adic numbers）に出会うことになる。

ハッセ(Hasse)とミンコフスキー(Minkowski)による見事な定理によれば、$a^2 + b^2 = 3c^2$ のような**二次**方程式については、局所的障害が唯一の障害である。すなわち、解をもたない「局所的」な理由がなければ、実際に有理数解が存在する。三次方程式では、これは劇的に破綻する。1951 年、セルマー（Ernst Selmer）は

$$3x^3 + 4y^3 + 5z^3 = 0$$

が任意の整数を法として解をもち、実数解ももつにもかかわらず、0 でない整数解をもたないことを示した。「局所から大域へ」の原理（local-to-global principle）がいつ、なぜ破綻するのかを解明することは、現代の整数論の大きなテーマの一つである。

解をもつ方程式

小問 (iv) には有名な親類がある。$x^2 + y^2 + z^2 = 3xyz$、すなわち**マルコフ方程式**（Markov equation）である。この方程式は正の整数解を無限に多くもち、$(1,1,1)$、$(1,1,2)$、$(1,2,5)$、$(1,5,13)$、$(2,5,29)$ と続く。そしてこれらの解は、無理数が分数によってどれほどよく近似できるかという問題と結びついている。演習 4 を参照せよ。

思考のスキル

無限降下法

方程式が解をもたないことを示すには、任意の解から真に小さい解が得られることを示せばよい。そうすれば、最小の解は存在し得ない。

これを、n を法として考えて降下を推し進める整除性を見つける方法と組み合わせよう。また、主張が降下の操作で保たれない場合には、それを一般化する用意をしておこう。

次の一歩

1. **STEP I の準備運動。**（*STEP I 2010* 問題 *8*）$a^3 + 3b^3 = 9c^3$ の整数解は $a = b = c = 0$ のみであることを示せ。次に、一の位の数字を考えることにより、$p^4 + 2q^4 = 5r^4$ についても同じことを示せ。

2. **降下を必要としない法。** 4 を法として考えるだけで、$x^2 + y^2 = 4z + 3$ が整数解を一つももたないことを示せ。

3. **有理点。** 小問 (iii) を用いて、円 $x^2 + y^2 = 3$ 上には**有理数**座標をもつ点（有理点、rational point）が存在しないことを示せ（$(1,1)$ を含む $x^2 + y^2 = 2$ と対比せよ）。

4. **マルコフの三つ組。** (x, y, z) が $x^2 + y^2 + z^2 = 3xyz$ を満たすならば、$(x, y, 3xy - z)$ もこれを満たすことを示せ。$(1,1,1)$ から出発して、上に挙げた三つ組を生成せよ（この「跳躍」の手法は降下法の逆である）。

さらに学ぶために

- **Harold Davenport, *The Higher Arithmetic***（『数論の高みへ』）、第 2 章および第 5 章。
- **Joseph Silverman, *A Friendly Introduction to Number Theory***（Pearson）（『やさしい数論入門』）。非常に読みやすい。$x^4 + y^4 = z^2$ に対するフェルマーの降下法による証明も載っている。
- **Simon Singh, *Fermat's Last Theorem***（Fourth Estate）（『フェルマーの最終定理』）。フェルマーの余白の書き込みからワイルズ（Wiles）の証明に至るまでの物語を、一般の読者向けに描いている。

1.6 二つの平方数の和

問題

STEP II 2023、問 7

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 2023 年の STEP 過去問一式（zip ファイル）のうち、STEP II の問題用紙にある：

`www.ocr.org.uk/Images/707102-2023-past-papers.zip`

導入

どのような整数が 2 つの平方数の和（sum of two squares）として表せるだろうか。$5 = 1^2 + 2^2$ や $13 = 2^2 + 3^2$ は表せるが、3、7、21 は表せない。ここで不思議な事実がある。$65 = 5 \times 13$ は、$1^2 + 8^2$ と $4^2 + 7^2$ という **2 通り**の異なる方法で 2 つの平方数の和として表せるのである。このような数を 2 つ掛け合わせると、なぜまたこのような数になるのか。そして、なぜ 2 通りになるのか。

答えは思いがけない方向からやってくる。この問題では、整数の世界を離れて**複素数**を扱うことが求められる。複素数の世界では 2 つの平方数の和は単純なものとなり、一見すると不可解な計算もほとんど機械的なものになる。

取りかかる前に

考えてみよう a と b を整数として $z = a + ib$ とするとき、$|z|^2$ は何か。

それは $a^2 + b^2$、すなわち 2 つの平方数の和である。したがって「N は 2 つの平方数の和である」とは、ちょうど「実部と虚部がともに整数であるような複素数 z を用いて $N = |z|^2$ と書ける」ということである。このような複素数は**ガウス整数**（Gaussian integers）とよばれる。この言い換えをしっかり覚えておいてほしい。問題全体がこれにかかっている。

順を追って解く

段階 1　絶対値は掛け算される

考えてみよう　zw を a、b、c、d を用いて書き表せ。$|zw|^2$ について何を示せばよいか。

$zw = (ac - bd) + \mathrm{i}(ad + bc)$ であるから、

$$|zw|^2 = (ac-bd)^2 + (ad+bc)^2 = a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2,$$

となる。交差項 $-2abcd$ と $+2abcd$ が打ち消し合うからである。そしてこれは因数分解できる。

$$a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 = (a^2+b^2)(c^2+d^2) = |z|^2|w|^2.$$

平方根をとって、$|zw| = |z||w|$ を得る。 ■

これを整数についての主張として読んでみよう。

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2. \tag{$\star$}$$

2 つの平方数の和どうしの積は、2 つの平方数の和である。しかも、その 2 つの平方数が何であるかを複素数が正確に教えてくれるのである。

段階 2　これを使う

小問 (ii)：$5 = |2+\mathrm{i}|^2$ であり、$221 = 10^2 + 11^2 = |10 + 11\mathrm{i}|^2$ である。そこで掛け合わせると、

$$(2+\mathrm{i})(10+11\mathrm{i}) = 20 + 22\mathrm{i} + 10\mathrm{i} - 11 = 9 + 32\mathrm{i},$$

となり、$5 \times 221 = 9^2 + 32^2$ を得る。（検算：$81 + 1024 = 1105$。）

考えてみよう　代わりに $10 + 11\mathrm{i}$ に $2 - \mathrm{i}$ を掛けるとどうなるか。これは $2 + \mathrm{i}$ と同じ絶対値（modulus）をもつ。

$(2-\mathrm{i})(10+11\mathrm{i}) = 20 + 22\mathrm{i} - 10\mathrm{i} + 11 = 31 + 12\mathrm{i}$ であるから、$1105 = 31^2 + 12^2$ とも表せる。$2+\mathrm{i}$ を選ぶか、その共役（conjugate）を選ぶかによって、**異なる**表し方が得られるのである。これで導入で述べた 65 の 2 通りの表し方が説明できる（図 1.6.1）。すなわち $65 = |(2+\mathrm{i})(3+2\mathrm{i})|^2 = |4+7\mathrm{i}|^2$ と $65 = |(2-\mathrm{i})(3+2\mathrm{i})|^2 = |8+\mathrm{i}|^2$ である。

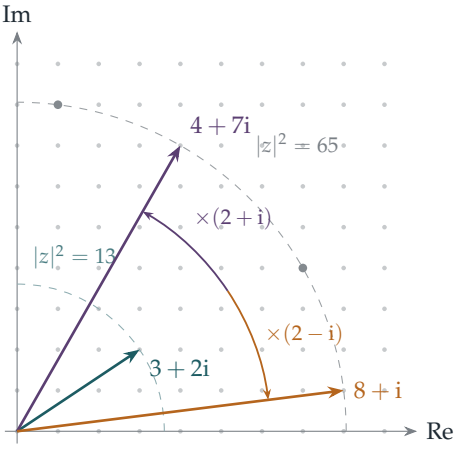


図 1.6.1　$2 \pm \mathrm{i}$ を掛けると、長さは $\sqrt{5}$ 倍され、約 26.6° だけ回転する。回転の向きは $2+\mathrm{i}$ なら反時計回り、$2-\mathrm{i}$ なら時計回りである。円 $|z|^2 = 13$ 上の $3+2\mathrm{i}$ から出発すると、2 通りの選び方によって円 $|z|^2 = 65$ 上の異なる格子点（lattice point）に行き着く。灰色の点は、それらを直線 $y = x$ に関して対称移動したものである。

段階 3　まず因数分解する

考えてみよう　8045 の末尾は 5 である。このことから何がわかるか。

$8045 = 5 \times 1609$ である。1609 を 2 つの平方数の和として表す必要があるが、1609 のすぐ下の平方数を試していけば、すぐに $1609 = 40^2 + 3^2$ が見つかる。すると

$$(2+\mathrm{i})(40+3\mathrm{i}) = 77 + 46\mathrm{i}, \qquad \text{よって} \qquad 8045 = 77^2 + 46^2,$$

となり、共役を用いれば $8045 = 83^2 + 34^2$ も得られる。

小問 (iv) はもっと速く片付く。$36 = 6^2 + 0^2$ であり、6 を掛けることは単に拡大するだけなので、$36 \times 50805 = 612^2 + 1206^2$ となる。

段階 4　3 通りの表し方

考えてみよう　25 は 2 つの平方数の和として 2 通り以上に表せる。符号の違いと入れ替えを除いて、絶対値が 5 のガウス整数はいくつあるか。

$25 = 5^2 + 0^2 = 3^2 + 4^2$ であり、これらは 5、$3+4\mathrm{i}$、$3-4\mathrm{i}$ に対応する。次に 1002082 について考える。$1001^2 = 1002001$ であるから、$1002082 = 1001^2 + 9^2$ である。$1001 + 9\mathrm{i}$

に 3 つのそれぞれを掛けると、次のようになる。

$$\begin{aligned} 5\,(1001+9\mathrm{i}) &= 5005+45\mathrm{i}, \\ (3+4\mathrm{i})(1001+9\mathrm{i}) &= 2967+4031\mathrm{i}, \\ (3-4\mathrm{i})(1001+9\mathrm{i}) &= 3039-3977\mathrm{i}. \end{aligned}$$

よって、3 つの組 (r,s) は $(45,5005)$、$(2967,4031)$、$(3039,3977)$ である。

段階 5　割り算

> **手を止めて、やってみよう**　小問 (vi) では、この仕組みを逆向きに動かす。$109 = 10^2+3^2$ と $1002037 = 1001^2+6^2$ はわかっている。探索をせずに、9193 を 2 つの平方数の和として表すにはどうすればよいだろうか。

ガウス整数を掛けると絶対値が掛け算されるのなら、割ると絶対値も割り算されるはずである。試してみると

$$\frac{1001+6\mathrm{i}}{10+3\mathrm{i}} = \frac{(1001+6\mathrm{i})(10-3\mathrm{i})}{109} = \frac{10028-2943\mathrm{i}}{109} = 92-27\mathrm{i}.$$

割り切れるので、$9193 = 92^2+27^2$ である。（検算：$8464+729=9193$。）

> **考えてみよう**　代わりに $10-3\mathrm{i}$ で割るとどうなるか。

$(1001+6\mathrm{i})(10+3\mathrm{i})/109 = (9992+3063\mathrm{i})/109$ となり、$9992/109$ は整数ではないから、これはガウス整数**ではない**。2 つの「109 の因数」のうち一方だけが $1001+6\mathrm{i}$ を割り切るのであり、これはちょうど、与えられた整数を割り切る素数が一部の素数に限られるのと同じである。ガウス整数には、それ自身の素数とそれ自身の素因数分解があるのである。

振り返り

- **言い換え、解き、言い戻す。**「2 つの平方数の和」は「ガウス整数の絶対値の 2 乗」になった。その言葉で考えると、問題はやさしかった。
- **まず因数分解する。**どの小問も、大きな数をより小さな数に分解し、その表し方を簡単に見つけることから始まった。
- **共役が新しい答えを与える。**表し方の個数は、ある因数とその共役のどちらを選ぶか、その選び方が何通りあるかによって決まる。

背後にある数学

フェルマーの二平方定理

どのような素数が 2 つの平方数の和になるだろうか。$2 = 1^2 + 1^2$、5、13、17、29、37、41 はそうであり、3、7、11、19、23、31 はそうではない。規則はこうである。2 を除けば、素数が 2 つの平方数の和になるのは、それを 4 で割った余りが 1 であるとき、かつそのときに限る。フェルマー（Fermat）は 1640 年にこれを述べ、オイラー（Euler）が 1749 年に証明した。ガウス整数の言葉でいえば、これは次のことを意味する。素数 $p \equiv 1 \pmod 4$ は $p = (a+bi)(a-bi)$ と**分解する**（split）が、素数 $p \equiv 3 \pmod 4$ は素数のままである。たとえば $5 = (2+i)(2-i)$ であるが、3 はまったく因数分解できない。

1990 年、ドン・ザギエ（Don Zagier）は二平方定理の証明を発表した。それはたった 1 文の長さであることで有名である。この証明は解説つきで *Proofs from THE BOOK* に収められている。

独自の素数をもつ新しい数の体系

ガウス（Gauss）は、ガウス整数が通常の整数と驚くほどよく似た振る舞いをすることに気づいた。除法の原理（division algorithm）とユークリッドの互除法（Euclidean algorithm）があり、すべてのガウス整数はガウス素数（Gaussian prime）の積に（± 1 や $\pm i$ を掛ける違いを除いて）**一意的に**分解される。これを $(\star)$ と組み合わせると、ある数が 2 つの平方数の和として何通りに表せるかを、その素因数分解（prime factorisation）だけから正確に数えることができる。

大学では、これは**代数的整数論**（algebraic number theory）への入り口となる。代数的整数論とは、通常の整数を理解するために $\mathbb{Z}[i]$ や $\mathbb{Z}[\sqrt{-5}]$ のような数の体系を研究する分野である。Section 1.7 では、この分野がなぜ生み出される必要があったのかを示す。このような体系のすべてがガウス整数ほど行儀がよいわけではないのである。

四平方とその先

すべての正の整数は **4 つの**平方数の和である（ラグランジュ（Lagrange）、1770 年）。その証明は $(\star)$ の四平方版に基づいており、それは $(\star)$ が複素数から得られるのと同じようにして、ハミルトン（Hamilton）の**四元数**（quaternions）から得られる。これは Section 7.8 で扱う。

思考のスキル

舞台を変える

ある数の体系では扱いにくい問題も、より大きな体系では自然なものになることがある。

2 つの平方数の和は、整数の中では扱いにくいが、複素数の中では単なる絶対値にすぎない。数学者はこのようにして絶えず数の体系を拡張してきた。整数から有理数へ、有理数から実数へ、実数から複素数へ。拡張のたびに、古い問題のいくつかがやさしくなるのである。

次の一歩

1. **障害。** $4k+3$ の形の数は 2 つの平方数の和にならないことを示せ。(4 を法として平方数はどうなるか?)

2. **2 通り。** 65 と 85 をそれぞれ 2 つの平方数の和として 2 通りに表し、その答えをガウス整数を用いて説明せよ。

3. **4 通り。** $1105 = 5 \times 13 \times 17$ である。1105 を 2 つの正の平方数の和として表す 4 通りの異なる方法を求めよ。なぜ 4 通りなのか。

4. **ガウス素数。** やや難 a, b, c, d を整数として $3 = (a+b\mathrm{i})(c+d\mathrm{i})$ ならば、一方の因数の絶対値は 1 であることを示せ。(絶対値の 2 乗をとれ。) これにより、3 がガウス素数であることがわかる。

さらに学ぶために

- **John Stillwell, *Elements of Number Theory***(Springer)。歴史を交えながら、ガウス整数とその先へと積み上げていく。
- **Aigner & Ziegler, *Proofs from THE BOOK***、第 4 章 "Representing numbers as sums of two squares"(数を 2 つの平方数の和として表す)。
- **Joseph Silverman, *A Friendly Introduction to Number Theory***、平方和とガウス整数に関する章。

1.7 因数分解が破綻するとき

問題

STEP I 2016、問 7

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-q7`

導入

1 より大きいすべての整数は、ちょうど 1 通りに素数（prime）の積として書ける。$60 = 2 \times 2 \times 3 \times 5$ であり、これ以外の書き方はない。この事実はあまりに何度も使ってきたので、証明が必要とは思えないほど自明に感じられるだろう。

この問題では、一見まったく自然に見えるのに、その「自明な」事実が成り立たない小さな数の世界を作る。STEP I の問題なので数学的には易しいが、得られる教訓は深い。それはまさに、1847 年にフェルマーの最終定理（Fermat's Last Theorem）の有名な証明の試みを打ち破り、代数学のまったく新しい分野の誕生につながった教訓なのである。

取りかかる前に

考えてみよう S と T の最初のいくつかの要素を書き出せ。小問 (iv) の定義によれば、S のどの要素がS-**素数**（S-prime）か。

$S = \{1, 5, 9, 13, 17, 21, 25, 29, 33, \ldots\}$ であり、$T = \{3, 7, 11, 15, 19, 23, \ldots\}$ である。S の数は、（1 以外の）より小さい S の要素の積として書けないとき、S-素数であるという。3 は S に属さないので、通常の整数では $9 = 3 \times 3$ であるにもかかわらず、9 は S-素数であることに注意せよ。「素数」であるかどうかは、どの数を使ってよいかによって決まるのである。

順を追って解く

段階 1　和集合、共通部分、積

$S \cup T$ は正の奇数全体の集合である。すべての奇数は 4 で割った余りが 1 または 3 だからである。$S \cap T$ は空集合である。2 つの異なる余りをもつ数は存在しないからである。

> **考えてみよう**　S の一般の要素はどのように書けるか。そのような要素 2 つの積は何か。

S の要素は $a \geq 0$ として $4a+1$ の形であり、

$$(4a+1)(4b+1) = 16ab + 4a + 4b + 1 = 4(4ab + a + b) + 1 \in S.$$

よって S は乗法について閉じている（closed under multiplication）。T については

$$(4a+3)(4b+3) = 16ab + 12a + 12b + 9 = 4(4ab + 3a + 3b + 2) + 1,$$

となり、これはT ではなく S に属する。例えば $3 \times 7 = 21 \in S$ である。よって T は乗法について閉じていない。

段階 2　T に属する素因数

> **考えてみよう**　T に属する素数でない数をとる。その素因数はすべて奇数である。もしそれらがすべて S に属していたら、どうなるか。

この数は奇数なので、その素因数はすべて奇数であり、S か T に属する。もしそれらがすべて S に属するならば、S は乗法について閉じているので、それらの積は S に属する。しかしその積は考えている数そのものであり、T に属する。よって、少なくとも 1 つの素因数は T に属する。 ■

段階 3　奇数個の因数

> **考えてみよう**　T の要素を偶数個掛け合わせると、積はどこに属するか。奇数個ならばどうか。

T の数 2 つの積は S の数になり、S の数どうしの積は S の数になるので、偶数個の T の因数の積は S に属する。奇数個の場合は（S の要素）$\times$（T の要素 1 つ）となり、同様の計算によりこれは T に属する。

次に $t \in T$ をとる。t が T-素数ならば、証明は終わりである。そうでなければ、t を T の要素の積として書く。各因数は 1 より大きいので、t より小さい。それらのうち T-素

数でないものはさらに分解でき、以下同様である。因数は毎回小さくなるので、この操作は終わり（ここでも整列性（well-ordering）による）、t は T-素数の積として表される。積は T に属するので、因数の個数は奇数でなければならない。 ■

段階 4　2 通りの因数分解

> **手を止めて、やってみよう**　S-素数への本質的に異なる 2 通りの因数分解をもつ S の数を見つけよ。**ヒント：**9 のように、通常の素因数が S に含まれないというだけの理由で S-素数となっている数を使え。

S-素数は $5, 9, 13, 17, 21, 29, 33, 37, 41, 49, \ldots$ と続く。ここで $21 = 3 \times 7$、$9 = 3 \times 3$、$49 = 7 \times 7$ はいずれも S-素数である。3 と 7 は S に属さないからである。そして

$$441 = 21 \times 21 = 9 \times 49.$$

これは 441 の S-素数への 2 通りの異なる因数分解である（図 1.7.1）。S では素因数分解の一意性（unique factorisation）が成り立たない。 ■

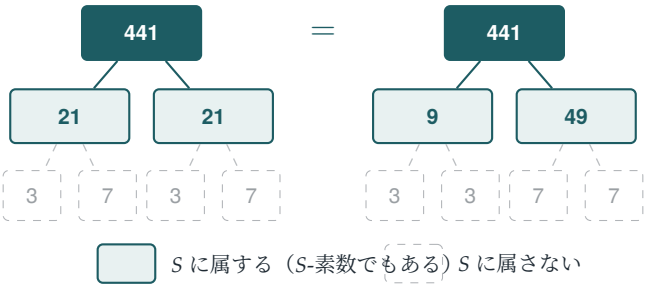


図 1.7.1　441 の S-素数への 2 通りの因数分解。通常の整数ではどちらの木も $3 \times 3 \times 7 \times 7$ まで続くが、3 と 7 は S に属さないので、S の中では因数分解は 2 段目で止まり、しかも両者は異なる。

振り返り

- **「素数」であるかどうかは体系による。**9 と 21 は整数の中では合成数だが、S の中では素数である。それらを因数分解するのに必要な数が欠けているからである。
- **閉じているかどうかが重要である。**S は乗法について閉じているが、T はそうではない。このただ 1 つの違いが、小問 (iii) と (iv) の鍵となった。
- **自明な事実が定理であることもある。**整数における素因数分解の一意性には証明が必要である。この問題はその理由を示している。よく似た体系において、それは偽なのである。

背後にある数学

整数を特別なものにしているもの

通常の整数では、なぜ因数分解がうまくいくのか。鍵となる事実は**ユークリッドの補題**（Euclid's lemma）である。すなわち、素数 p が積 ab を割り切るならば、p は a を割り切るか、または p は b を割り切る。これはユークリッドの互除法（Euclidean algorithm）を用いて証明され、まさに S で成り立たない性質である。そこでは、S-素数 9 は $21 \times 21 = 441$ を割り切る（$441 = 9 \times 49$ だから）が、9 は S において 21 を割り切らない。大学 1 年で、ユークリッドの補題を注意深く証明し、そこから素因数分解の一意性が導かれることを学ぶだろう。

フェルマーの最終定理の誤った証明

1847 年 3 月 1 日、ガブリエル・ラメ（Gabriel Lamé）はパリ科学アカデミーで、フェルマーの最終定理を証明したと発表した。彼のアイデアは、1 の複素冪根（complex roots of unity）を用いて $x^n + y^n$ を

$$x^n + y^n = (x+y)(x+\zeta y)(x+\zeta^2 y)\cdots(x+\zeta^{n-1}y), \qquad \zeta = e^{2\pi \mathrm{i}/n}$$

（n が奇数のとき）と因数分解し、各括弧の素因数について議論するというものであった。ジョゼフ・リウヴィル（Joseph Liouville）はすぐに異議を唱えた。ζ から作られる数が一意に因数分解されると言えるのはなぜか、と。数週間後、エルンスト・クンマー（Ernst Kummer）が、それらがしばしば一意に因数分解されないことをすでに示していたことが明らかになった。最初に破綻するのは $n = 23$ のときである。

クンマーは、素因数分解の一意性を回復させる追加の対象である「理想数」（ideal numbers）を考案して救えるものを救い、広い範囲の指数に対してフェルマーの最終定理を証明した。リヒャルト・デデキント（Richard Dedekind）はクンマーの理想数を**イデアル**（ideals）へと発展させた。これは現代代数学の中心的な概念の 1 つである。

覚えておきたい小さな例

数の体系 $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ において

$$6 = 2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5}),$$

であり、4 つの因数はいずれもこの体系で「素数」である（演習 3）。これを、因数分解が一意である Section 1.6 のガウス整数（Gaussian integers）と比べてみよ。この種の体系のうちどれが素因数分解の一意性をもつかは、深い問題である。ガウス（Gauss）

は、$\mathbb{Z}[\sqrt{-d}]$ の形の体系とその近い仲間のうち、それをもつのは 9 つだけであると予想した。これは最終的に、1952 年から 1967 年にかけて Heegner、Baker、Stark によって証明された。

思考のスキル

当然と思っていることを疑う

ある事実が証明するまでもなく自明に感じられるときは、それが何に依存しているかを問い、それが成り立たない状況を探せ。

反例、すなわち「自明な」事実が偽となる世界を作ることは、証明に本当に必要なものを見つけ出す最良の方法の 1 つである。大学の代数学の多くは、整数のよく知られた性質のうちどれがより一般の体系でも生き残るかを問うことから成っている。

次の一歩

1 **別の例。** 693 が S-素数への 2 通りの異なる因数分解をもつことを示せ。このような例を作る一般的な方法を見つけられるか。

2 **偶数。** $E = \{2, 4, 6, 8, \ldots\}$ とする。どの数が E-素数か。60 が E-素数への因数分解を 2 通り以上もつことを示せ。

3 $\mathbb{Z}[\sqrt{-5}]$。**ノルム** (norm) $N(a + b\sqrt{-5}) = a^2 + 5b^2$ を定義する。$N(zw) = N(z)N(w)$ を示せ。ノルムが 2 または 3 となる元が存在しないことを示すことにより、2、3、$1 \pm \sqrt{-5}$ は $\mathbb{Z}[\sqrt{-5}]$ においてこれ以上因数分解できないことを導け。

4 **ユークリッドの補題の応用。** やや難 ユークリッドの補題（素数が ab を割り切るならば、それは a または b を割り切る）を仮定して、1 より大きいすべての整数は、因数の順序を除いて、ただ 1 通りの素因数分解しかもたないことを証明せよ。

さらに学ぶために

- **Ian Stewart & David Tall, *Algebraic Number Theory and Fermat's Last Theorem*** (CRC Press)。『代数的整数論とフェルマーの最終定理』。冒頭の数章では、ラメ、クンマー、イデアルの物語が、意欲的な大学 1 年生がついていける水準で語られている。

- **John Stillwell, *Elements of Number Theory***。『数論の基礎』。整数とガウス整数における素因数分解の一意性を、並べて比較している。
- **Harold Edwards, *Fermat's Last Theorem: A Genetic Introduction***（Springer）。『フェルマーの最終定理：発生的入門』。意欲的な読者向けで、クンマーの仕事をその歴史を通して解説している。

1.8 有理数を数える

問題

STEP III 2020、問 8

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 2020 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/696589-2020-past-papers.zip`

導入

正の分数をすべて、一つずつ順に並べて、どの分数もちょうど一回ずつ現れるようにできるだろうか。それは不可能に思える。どの二つの分数の間にも無数の分数があるので、書き出すべき「次の」分数というものが存在しないからである。しかしカントール（Cantor）は 1870 年代に、それでも並べることができると示した。これは、ある厳密な意味において、分数は整数より多くはないということを意味する。

カントールのリストは不格好であった。$\frac{1}{2}$ だけでなく $\frac{2}{4}$ も含まれていて、重複を消していく必要があったのである。この問題では、ばかばかしいほど単純な規則をもつ数列から、重複のまったくないリストを作る。このリストは 2000 年に Neil Calkin と Herbert Wilf によって発表されたが、数列そのものは 1858 年に Moritz Stern によって研究されていた。

取りかかる前に

考えてみよう 何かを証明する前に、最初の 15 項ほどを計算してみよう。比 u_n/u_{n+1} について何に気づくだろうか。

数列は

$$1,\ 1,\ 2,\ 1,\ 3,\ 2,\ 3,\ 1,\ 4,\ 3,\ 5,\ 2,\ 5,\ 3,\ 4,\ 1,\ 5,\ \ldots$$

と始まり、比 u_n/u_{n+1} は

$$\frac{1}{1},\ \frac{1}{2},\ \frac{2}{1},\ \frac{1}{3},\ \frac{3}{2},\ \frac{2}{3},\ \frac{3}{1},\ \frac{1}{4},\ \frac{4}{3},\ \frac{3}{5},\ \frac{5}{2},\ \frac{2}{5},\ \frac{5}{3},\ \frac{3}{4},\ \frac{4}{1},\ \ldots$$

となる。どの分数も既約分数（lowest terms）の形で現れ、重複するものはない。この問題は、これが永遠に続くこと、そしてどの正の分数もいずれ現れることを証明せよというものである。

順を追って解く

段階 1　奇数番目が偶数番目に勝る

隣り合う二項は (u_{2k}, u_{2k+1}) または (u_{2k+1}, u_{2k+2}) のいずれかである。

> **考えてみよう**　これらの組をそれぞれ u_k と u_{k+1} を用いて表せ。どちらの項が大きいか。

$(u_{2k}, u_{2k+1}) = (u_k,\ u_k + u_{k+1})$ であり、$(u_{2k+1}, u_{2k+2}) = (u_k + u_{k+1},\ u_{k+1})$ である。すべての項は正の整数である（簡単な帰納法（induction）で示せる）から、$u_k + u_{k+1}$ は u_k と u_{k+1} のどちらよりも大きい。唯一の例外は最初の組 $(u_1, u_2) = (1, 1)$ であり、u_1 は直接定義されているので、どちらの形にも当てはまらない。 ■

段階 2　隣り合う項は互いに素である

> **考えてみよう**　$d > 1$ が u_{2k} と u_{2k+1} の両方、すなわち u_k と $u_k + u_{k+1}$ の両方を割り切るとする。d はほかに何を割り切るか。

d は $(u_k + u_{k+1}) - u_k = u_{k+1}$ を割り切るので、d は数列のより前にある隣り合う組 u_k, u_{k+1} を割り切る。もう一方の場合もまったく同様である。d が $u_k + u_{k+1}$ と u_{k+1} を割り切るならば、d は u_k を割り切る。

したがって、隣り合う組の公約数は、より前の組へ、さらに前の組へと受け渡されていく。位置が永遠に減り続けることはできない（またしても整列性（well-ordering）である）から、最終的に d は最初の組 $u_1 = u_2 = 1$ を割り切らなければならなくなる。これは $d > 1$ に対しては不可能である。よって、隣り合う組はすべて互いに素（coprime）である。 ■

段階 3　同じ組が二度現れることはない

> **手を止めて、やってみよう**　段階 1 から有用なことがわかる。隣り合う組 (a, b) を見れば、a が奇数番目にあるか偶数番目にあるかを判定できるのである。どのようにしてか。さらに、段階 2 の意味で、その直前に来る組を復元できるだろうか。

$a < b$ ならば、（段階 1 により）b は奇数番目にあるので、ある k に対してこの組は $(u_{2k}, u_{2k+1}) = (u_k, u_k + u_{k+1})$ であり、「親」の組 (u_k, u_{k+1}) は $(a,\ b-a)$ である。$a > b$ ならば、この組は (u_{2k+1}, u_{2k+2}) であり、その親は $(a-b,\ b)$ である。$a = b$ ならば、段階 1 よりこの組はまさに最初の組 $(1,1)$ でなければならない。

よって、最初の組以外の隣り合う組はそれぞれ、その親の組と**親の位置**を決定する（この構造は図 1.8.1 の木として見ることができる）。子が $2k$ 番目または $2k+1$ 番目にあるとき、親は k 番目にある。いま、(a,b) が二つの異なる位置に現れたとしよう。するとそれらの親は同じ組が二つの位置に現れたものとなり、**その**親もまた同様であり、以下同様である。これをさかのぼっていくと、最終的に $(1,1)$ が 1 番目以外の位置に見つかることになるが、これは段階 1 により否定される。 ■

段階 4 互いに素な組はすべて現れる

> **考えてみよう** 互いに素なある組 (a,b) が、隣り合う二項として決して現れないとする。そのような組のうち、どれに注目すべきだろうか。

「欠けている」互いに素な組のうち、$a+b$ の値が最小のものをとる。すなわち最小反例（minimal counterexample）である。これは実際に現れる $(1,1)$ ではありえないので、$a \neq b$ である（互いに素かつ等しいならば $a = b = 1$ となる）。

- $a > b$ の場合：組 $(a-b, b)$ は互いに素であり（$a-b$ と b の公約数は a を割り切る）、その和 a は $a+b$ より小さい。最小性によりこの組は現れ、その位置を $k, k+1$ とする。しかしすると $u_{2k+1} = u_k + u_{k+1} = a$ かつ $u_{2k+2} = u_{k+1} = b$ となり、結局 (a,b) は現れることになる。
- $a < b$ の場合：同様に $(a, b-a)$ がある位置 $k, k+1$ に現れ、すると $(u_{2k}, u_{2k+1}) = (a,b)$ となる。

いずれの場合も矛盾である。よって、互いに素な正の整数の組はすべて、隣り合う二項として現れる。 ■

（問題の小問 (iv) は、これを無限降下法（descent）の形で述べている。すなわち、欠けている組があれば、より小さな欠けている組が生じるというものである。これは同じ議論を逆向きに読んだものにほかならない。）

段階 5 すべての分数のリスト

すべての正の有理数（rational number）は、a, b が互いに素であるような既約分数 a/b としてただ一通りに表せる。段階 4 により、(a,b) はある隣り合う組 (u_n, u_{n+1}) として現れるので、$f(n) = a/b$ である。すなわち f の値域はすべての正の有理数である。段階 3 によりそれは一度しか現れず、段階 2 によりすべての値 $f(n)$ はすでに既約分数の

形であるから、異なる二つの n が同じ分数を与えることはない。したがって f は正の整数全体から正の有理数全体への全単射（bijection）であり、逆関数をもつ。 ■

振り返り

- **降下法とその逆。**公約数や重複する組は、数列の始まりへと**さかのぼって**追跡された。欠けている組は、最小反例を用いて**前向きに**組み立てることで処理された。
- **全単射には二つの半分が必要である。**「すべての分数が現れる」（全射（onto））と「どの分数も二度は現れない」（単射（one-to-one））は別々の主張であり、別々に証明される。
- **まず計算せよ。**15 項を書き出したことで主張が信じられるものになり、証明を推し進めた親子構造が見えてきた。

背後にある数学

Calkin–Wilf 木

正の分数を木の形に並べる。一番上に $\frac{1}{1}$ を置き、各分数 $\frac{a}{b}$ に二つの子、すなわち左に $\frac{a}{a+b}$、右に $\frac{a+b}{b}$ を与える。この木を一行ずつ、左から右へ読むと、ちょうどこの問題のリスト $f(1), f(2), f(3), \ldots$ が得られる（図 1.8.1）。段階 3 はすべての分数がただ一つの親をもつことを述べ、段階 4 はすべての分数が木の中にあることを述べている。2003 年に Moshe Newman は、木すら必要ないことを発見した。リストの各分数は、一つ前の分数から

$$x_{n+1} = \frac{1}{2\lfloor x_n \rfloor - x_n + 1}.$$

によって計算できるのである。

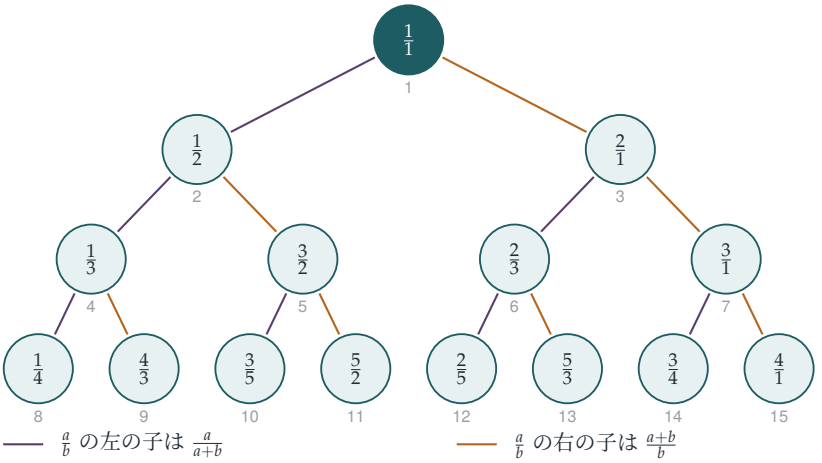


図 1.8.1　Calkin–Wilf 木の最初の 4 行。一行ずつ、左から右へ読むと $f(1), f(2), f(3), \ldots$ が得られる。灰色の小さな数は位置 n である。すべての正の分数が既約分数の形でちょうど一回ずつ現れる。

無限の大きさの違い

このように並べ上げることのできる集合を**可算**（countable）であるという。分数は可算である。分数は整数よりはるかに多いように思えるので、これは驚くべきことである。大学の最初の学期には、カントールの**対角線論法**（diagonal argument）にも出会うだろう。これは**実数**が可算でないこと、すなわち実数のどんなリストも必ずどれかを取りこぼすことを示すものである。したがって、無限には本当に異なる大きさがあり、実数は有理数より真に大きな無限をなす。これは大学 1 年次の講義で出会う結果の中でも、とりわけ驚くべきものの一つである。

Stern の数列

数列 u_n は *Stern* **の二原子数列**（Stern's diatomic sequence）であり、ほかにもさまざまな顔をもつ。たとえば u_{n+1} は、各べきを高々 2 回まで用いて n を 2 のべきの和として表す方法の数に等しい。この数列は *Stern–Brocot* **木**（Stern–Brocot tree）や、無理数の最良有理近似を与える連分数（continued fraction）とも深く関係している。

思考のスキル

全単射を構成する

二つの集合が同じ大きさであることを示すには、両者を過不足なく対応させよ。すなわち、対象の集合のすべての元に対応がつくこと（全射）と、どの元にも二重に対応がつかないこと（単射）を証明せよ。

全単射は有限・無限を問わず数え上げの基礎であり、大学では絶えず用いることになる。ここでは、どちらの半分も、構造をその出発点までさかのぼることで証明された。

次の一歩

1. **分数を見つける。** $f(n) = \frac{3}{5}$ となるのはどの n か。また $f(n) = \frac{5}{3}$ となるのはどの n か。親の規則を用いて $\frac{1}{1}$ までさかのぼれ。

2. **Newman の公式。** $x_1 = 1$ から始めて、Newman の公式がリストの最初の 10 個の分数を生み出すことを確かめよ。

3. **カントールの対角線論法。** 0 と 1 の間のすべての実数を小数で書いたリストがあるとする。リストの n 番目の数と n 桁目が異なるような小数を構成せよ。これがリストの不完全さを示すのはなぜか。（$0.0999\ldots = 0.1$ のような小数にはどのような注意が必要か。）

4. **可算和集合。** やや難 正の整数の組 (m, n) 全体の集合が可算であることを、正の整数全体との全単射を具体的に与えることで示せ。（$2^{m-1}(2n-1)$ を試してみよ。）

さらに学ぶために

- **Neil Calkin & Herbert Wilf,「Recounting the rationals」**（*American Mathematical Monthly*, 2000）。4 ページで、全編が読みやすい。
- **Aigner & Ziegler, *Proofs from THE BOOK***（邦訳『天書の証明』）、第 17 章「Sets, functions, and the continuum hypothesis」（集合、関数、連続体仮説）。Calkin–Wilf 木が取り上げられている。
- **Ian Stewart & David Tall, *The Foundations of Mathematics***（Oxford University Press）。大学 1 年次の講義と同様に、可算性、カントール、実数を扱う。

1.9 三次曲線の接線

問題

STEP I 2009、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/09-s1-q2`

導入

一見すると、これはありふれた座標幾何の問題である。微分して接線（tangent）を求め、三次方程式（cubic equation）を解く。ところが最後の一行では、ある立方数（cube）をほかの三つの立方数の和として表すことが求められ、幾何がまるで魔法のようにそれを生み出してくれる。

曲線上の既知の点を通る直線を引いて新しい点を見つけるというこの技法は、3 世紀のアレクサンドリアのディオファントス（Diophantus）にまでさかのぼる。現代の数学者の手によって、それは**楕円曲線**（elliptic curves）の理論となった。この理論は現代の数論（number theory）の中心に位置し、フェルマーの最終定理（Fermat's Last Theorem）の証明の土台となり、さらに世界のインターネット通信の大部分の安全を支えている。

取りかかる前に

考えてみよう 点 $(-a, b)$ はこの曲線上にある。なぜか。また、そのことは立方数の和とどう関係するのか。

代入すると $(-a)^3 + a^3 + b^3 = b^3$ となるので、確かに曲線上にある。$y^3 = x^3 + a^3 + b^3$ 上の**有理数**（rational）座標をもつ点こそ、まさに求めたいものである。$x = q/s'$、$y = p/s'$ ならば、分母を払うことで立方数どうしの関係式が得られる。方針は、見つけやすい一つの点から出発し、幾何を用いてもっと見つけにくい点を探すことである。

順を追って解く

段階 1　接線

$y^3 = x^3 + a^3 + b^3$ を陰関数微分（implicit differentiation）すると $3y^2\dfrac{dy}{dx} = 3x^2$ であるから、$\dfrac{dy}{dx} = \dfrac{x^2}{y^2}$ となる。$(-a, b)$ における傾き（gradient）は a^2/b^2 であるから、接線は

$$y - b = \frac{a^2}{b^2}(x + a) \quad\Longrightarrow\quad b^2 y - b^3 = a^2 x + a^3 \quad\Longrightarrow\quad b^2 y - a^2 x = a^3 + b^3. \qquad \blacksquare$$

段階 2　接線が曲線と再び交わる点

$a = 1$、$b = 2$ のとき、曲線は $y^3 = x^3 + 9$ であり、$(-1, 2)$ における接線は $4y - x = 9$、すなわち $y = \dfrac{x + 9}{4}$ である。これを曲線の式に代入すると

$$\frac{(x+9)^3}{64} = x^3 + 9 \quad\Longrightarrow\quad x^3 + 27x^2 + 243x + 729 = 64x^3 + 576,$$

となり、整理すると $63x^3 - 27x^2 - 243x - 153 = 0$、両辺を 9 で割ると $7x^3 - 3x^2 - 27x - 17 = 0$ を得る。 $\blacksquare$

段階 3　三次方程式を解く

> **考えてみよう**　この三次方程式の根の一つは、計算をしなくてもすでにわかっている。それはどれか。また、なぜそれは**二重に**現れるはずなのか。

接線は $x = -1$ で曲線に接しており（図 1.9.1）、「接する」とは重根（repeated root）をもつということである。これは、放物線の接線が放物線と二次方程式の重根で交わるのとまったく同じである。したがって $(x+1)^2$ が因数になるはずである。確かめると、$7(-1)^3 - 3(1) - 27(-1) - 17 = -7 - 3 + 27 - 17 = 0$ であり、導関数 $21x^2 - 6x - 27$ も $x = -1$ で 0 になる。割り算をすると

$$7x^3 - 3x^2 - 27x - 17 = (x + 1)^2(7x - 17).$$

> **手を止めて、やってみよう**　したがって、接線は $x = \frac{17}{7}$ で再び曲線と交わる。y を求め、この点を立方数どうしの関係式に書き直せ。

$y = \dfrac{17/7 + 9}{4} = \dfrac{80/7}{4} = \dfrac{20}{7}$ である。点 $\left(\frac{17}{7}, \frac{20}{7}\right)$ は $y^3 = x^3 + 9$ 上にあるから

$$\frac{20^3}{7^3} = \frac{17^3}{7^3} + 9 \quad\Longrightarrow\quad 20^3 = 17^3 + 9 \times 7^3.$$

考えてみよう 9×7^3 を二つの立方数の和として表したい。9 がどこから来たのかを思い出そう。

$9 = a^3 + b^3 = 1^3 + 2^3$ であるから、$9 \times 7^3 = 7^3 + 14^3$ となる。したがって

$$20^3 = 17^3 + 14^3 + 7^3.$$

検算：$8000 = 4913 + 2744 + 343$。 ■

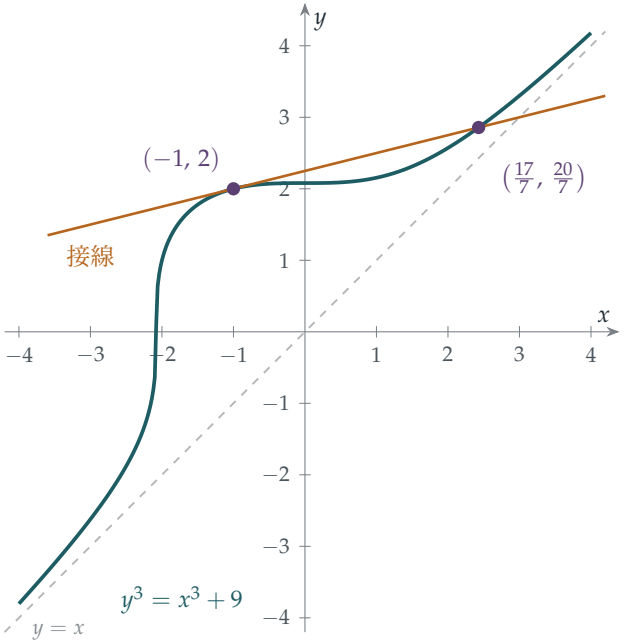


図 1.9.1 曲線 $y^3 = x^3 + 9$（青緑）は、原点から遠く離れたところで直線 $y = x$ に近づく。有理点 $(-1, 2)$ における接線（琥珀色）はその点で曲線に接しており、これは二重の交点として数えられる。そして接線はもう一度、別の有理点 $\left(\frac{17}{7}, \frac{20}{7}\right)$ で曲線と交わる。

振り返り

- **接することは重根を意味する。**これにより、明らかな根が見当たらない三次方程式が、すぐに因数分解できるものに変わった。
- **新しい根は自動的に有理数になる。**三つの根のうち二つが有理数であれば（ここではどちらも -1）、根の和 $\frac{3}{7}$ が有理数であることから、三つ目の根も有理数でなければならない。これがこの方法の核心である。
- **幾何が数論の答えを生み出した。**立方数を探し回ったわけではない。一本の接線が

それを見つけてくれたのである。

背後にある数学

弦と接線の方法

$y^3 = x^3 + 9$ や、より標準的な形 $y^2 = x^3 + Ax + B$ のような三次曲線を考える。その上にある有理数座標の点を二つ知っていれば、それらを通る直線は曲線とちょうどもう一点で交わり、その点も有理数座標をもつ（**振り返り**での議論による）。一点しか知らなければ、代わりにその点での接線を使えばよい。いずれにしても、既知の有理点から新しい有理点が生まれる。

驚くべきことに、この「弦（chord）と接線」による構成は、曲線上の点を**足し合わせる**方法に仕立てることができ、そのとき有理点全体は**群**（group）をなす。群とは、大学 1 年次で学ぶ代数的構造である。Louis Mordell は 1922 年に、この群が有限個の点で生成されることを証明した。すなわち、有理点がどれだけたくさんあっても、そのすべては有限個の点から弦と接線を用いて作り出せる。彼の証明は、Section 1.5 で扱ったフェルマー（Fermat）の無限降下法（descent）の一種である。

今日の楕円曲線

このような曲線は**楕円曲線**とよばれる（楕円であるからではなく、楕円の弧長との歴史的なつながりによる）。楕円曲線は現代数学のいたるところに現れる。

- **フェルマーの最終定理。** 1980 年代、Gerhard Frey は、$x^n + y^n = z^n$ の解が存在すれば、非常に奇妙な楕円曲線が生じることに気づいた。1994 年、アンドリュー・ワイルズ（Andrew Wiles）はそのような奇妙な曲線が存在しえないことを証明し、こうしてフェルマーの最終定理を証明した。
- **バーチ・スウィンナートン＝ダイアー予想（Birch and Swinnerton-Dyer conjecture）。** 有理点のなす群には、生成元（generator）がいくつ必要なのだろうか。1960 年代に、ケンブリッジで行われた数学における最初期のコンピュータ実験をもとに立てられた予想は、素数を法として点を数えることから作られる関数を用いて、その答えを予言している。これは七つのミレニアム懸賞問題（Millennium Prize Problems）の一つである。
- **暗号（cryptography）。** 有限の数の体系の上の楕円曲線では、点 P を自分自身に n 回足す計算は、n が何百桁もあっても速く行える（高い累乗を二乗の繰り返しで計算するのと同じように、P を繰り返し 2 倍すればよい）。ところが、P と結果 nP が与えられたとき、n を求めることはきわめて難しいと考えられている。これが**楕円曲**

線離散対数問題（elliptic-curve discrete logarithm problem）である。この非対称性が、今日のオンライン通信の多くを守っている。

同じ次数の累乗の和

三つの正の立方数の和となる最小の立方数は $6^3 = 3^3 + 4^3 + 5^3$ である。接線の方法で見つかった $20^3 = 7^3 + 14^3 + 17^3$ はその倍数ではなく、この方法を繰り返すと新しい恒等式が次々に得られる（ただし負の数を含むものもある）。ある k 乗数を作るには、k 乗数がいくつ必要だろうか。オイラー（Euler）は 1769 年に、ある k 乗数を作るには少なくとも k 個の k 乗数が必要であると予想した。4 乗と 5 乗については、この予想は誤りであった。1966 年、Leon Lander と Thomas Parkin はコンピュータによる探索で

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5$$

を発見し、1988 年には Noam Elkies が楕円曲線を用いて 4 乗の場合の反例を見つけた。

思考のスキル

幾何で数論を解く

方程式の整数解や有理数解を求めるには、方程式を曲線とみなし、既知の点を通る直線を探せ。

その背後にある代数は単純である。有理数係数の多項式の根が一つを除いてすべて有理数であれば、残りの根も有理数である。このように図と式の間を行き来することは、数学者がもちうる最も強力な習慣の一つである。

次の一歩

1. **円上の有理点。** $(-1, 0)$ を通り傾きが t の直線は、円 $x^2 + y^2 = 1$ ともう一点で交わる。その点が $\left(\dfrac{1 - t^2}{1 + t^2}, \dfrac{2t}{1 + t^2}\right)$ であることを示し、これを用いてピタゴラス数（Pythagorean triples）を無数に作れ。

2. **交わらない弦。** 点 $(1, 2)$ と $(2, 1)$ は $x^3 + y^3 = 9$ 上にある。これらを通る直線は、曲線とほかの点では交わらないことを示せ。「三つ目の点」はどこへ行ったのだろうか。（無限遠点（point at infinity）について調べてみよ。）

3. **技法を繰り返す。** $\left(\frac{17}{7}, \frac{20}{7}\right)$ における $y^3 = x^3 + 9$ の接線と、それが曲線と交わる三つ目の点を求めよ。（数式処理システム（computer algebra system）を使うとよい。

数がいかに急速に大きくなるかに注目せよ。）

4 **タクシー数（taxicab numbers）。** $1729 = 1^3 + 12^3 = 9^3 + 10^3$ である。$(1, 12)$ と $(9, 10)$ を通る直線が曲線 $x^3 + y^3 = 1729$ と交わる三つ目の点を求め、$p^3 = q^3 + r^3 + s^3$ の形の新しい恒等式を導け。

さらに学ぶために

- **Joseph Silverman & John Tate, *Rational Points on Elliptic Curves***（Springer）。邦題『楕円曲線論入門』。学部生向けに書かれており、第 1 章は A レベル（A level、英国の大学入学資格試験）を超える知識を必要としない。
- **Avner Ash & Robert Gross, *Elliptic Tales***（Princeton University Press）。バーチ・スウィンナートン＝ダイアー予想へと至る一般向けの解説書。
- **Simon Singh, *Fermat's Last Theorem***。邦題『フェルマーの最終定理』。楕円曲線が 350 年来の難問を解決するに至った経緯を描く。

本章で学んだこと

本章の冒頭で、整数について三つの問いを立て、その根底に流れる四つ目のテーマ、すなわち「どのように証明するか」を扱うと約束した。九つの STEP の問題を通して、どこまで到達できたかを確かめてみよう。

1. 素数はいくつあり、どのように分布しているか

Section 1.1 では、新しい素数（prime）を一つも見つけることなく、素数が無限に存在することを証明した。互いに共通の因数をもたない数の無限族、すなわちフェルマー（Fermat）数（Fermat numbers）を構成したのである。そのため、それぞれの数は自分だけの素数を必要とする。これは大きさではなく**構造**についての証明である。

Section 1.2 ではさらに進んで、n 以下のすべての素数の積が 4^n より小さいことを示した。これは本章で初めての**定量的**（quantitative）な主張であり、素数がどれほど密に詰まりうるかを制限するものである。対数をとると、これは $\sum_{p \le n} \ln p < 1.39\, n$ を意味する。一方、素数定理（Prime Number Theorem）によれば、真の値はおよそ n である。STEP レベルの議論でも、すでにかなり近いところまで迫っていたのである。

まだ**行っていない**のは、素数がどのように分布しているかを正確に求めることである。これはリーマン（Riemann）ゼータ関数（Riemann zeta function）によって支配されており、それを精密に述べたものがリーマン予想（Riemann Hypothesis）、すなわち数学で最も有名な未解決問題である。読者はいまや、それが何についての問題なのかを理解するのに十分な知識をもっている。

2. ある数が分数でないことはどのように証明できるか

まったく異なる三つの方法を見た。

- **最小のものをとる**（Section 1.3）。もし $\sqrt{2}$ が分数であれば、$k\sqrt{2}$ を整数にする最小の正の整数 k が存在する。しかしそのとき $(\sqrt{2}-1)k$ はそれより小さな整数となる。同じ議論で立方根も扱うことができた。
- **整数を 0 と 1 の間に閉じ込める**（Section 1.4）。もし e や e^2 が分数であれば、階乗を掛けることで 0 と 1 の間に厳密に挟まれた整数が得られてしまう。これは、e と π が超越数（transcendental）であることを示したエルミート（Hermite）とリンデ

マン（Lindemann）の証明の背後にある考え方である。

- **起こりえない整除関係を見つける**（Section 1.5、演習 3）。$x^2 + y^2 = 3$ 上に有理点（rational point）が存在しないことを示すのは、x が有理数のとき $\sqrt{3 - x^2}$ が決して有理数にならないことを示すのと同じである。

そして、まだわかっていないことがどれほど多いかも学んだ。$e + \pi$ が無理数（irrational）であることさえ、いまだに誰も証明できていないのである。

3. どの方程式が整数解をもつか

答えが**存在しない**である場合もある。Section 1.5 では、それを証明するフェルマーの方法を見た。すなわち、どんな解からもより小さな解が際限なく作られてしまうというものである。うまく選んだ素数を法（modulo）として考えることで、どの整除関係を利用すればよいかがわかった。

答えが**存在し、しかもそれを作り出す仕組みがある**という場合もある。Section 1.6 では、複素数によって二つの平方数の和が乗法の規則に変わった。Section 1.9 では、三次曲線の接線から $20^3 = 17^3 + 14^3 + 7^3$ が得られた。

そして、正しい一手が**数の体系を変えること**である場合もある。ガウス整数（Gaussian integers）を用いると、二つの平方数の和は簡単に扱えた。しかし Section 1.7 は警告を与えた。一見まったく妥当に見える体系でも、数が二通りの異なる方法で「素数」に分解されうるのである。1847 年に無視されたこの警告は、イデアル（ideal）と現代代数学の誕生へとつながった。

Section 1.8 はさらに独自のひねりを加えた。整数よりはるかに多く存在するように思える分数も、一つずつ並べ上げることができるのである。無限には、最初に見えるよりも多くの構造がある。

4. 証明の道具箱

本章で用いた方法を以下にまとめる。これらはどれも、大学の数学の講義で何度も繰り返し現れるものである。

方法	用いた箇所
数学的帰納法（induction）と強い帰納法（strong induction）	フェルマー数（1.1）、素数の積（1.2）
整列性（well-ordering）、最小反例（minimal counterexample）	$\sqrt{2}$ と $\sqrt[3]{2}$（1.3）、分数の列挙（1.8）
無限降下法（infinite descent）	解をもたない方程式（1.5）、互いに素な組（1.8）
背理法（proof by contradiction）	全体を通して、特に 1.3 と 1.4
n を法とする計算	1.5、1.7
評価とはさみうち（bounding and squeezing）	1.2、1.4
全単射（bijection）の構成	1.8
反例（counterexample）の構成	一意的でない因数分解（1.7）
舞台を変える	複素数（1.6）、幾何（1.9）

問題を振り返ると、STEP の出題者がしばしば最初の一歩を与えてくれていたことに気づくだろう。「二項展開（binomial expansion）を考えることにより…」「複素数 $2+i$ と $10+11i$ を考えることにより…」といった具合である。大学では、こうした手助けは次第になくなり、正しい最初の一歩を**見つけること**そのものが求められる技能となる。最良の準備は、まさにこれまで行ってきたことである。すなわち、問題を解き終えたら、そのヒントが**なぜ**うまくいったのかを自問し、次回は自分で思いつけるようにすることである。

次はどこへ

本章のいくつかの話題は、本書の別の箇所でも続いていく。

- 分数による e の近似は Section 2.9 で再び登場し、リーマンゼータ関数は Section 2.4 で $\zeta(2) = \pi^2/6$ として現れる。
- ラメ（Lamé）の誤った証明に現れた 1 の冪根（roots of unity）は Chapter 5 の主題であり、Section 1.1 で約束したガウス（Gauss）による正 17 角形の作図は Section 6.2 で扱う。
- Section 1.6 の恒等式（identity）の四平方版は、四元数（quaternion）を通じて Section 7.8 に登場する。

大学入学前にさらに先へ進みたい人へ

- **Harold Davenport, *The Higher Arithmetic***：初等整数論（elementary number theory）への入門書として、一冊選ぶならこれが最良である。

- **Aigner & Ziegler, *Proofs from THE BOOK***：第 1–4 章、第 8 章、第 17 章は本章と直接つながっている。
- **Joseph Silverman, *A Friendly Introduction to Number Theory***：本章の内容のほぼすべてとそれ以上を、ゆっくりとしたペースで扱っている。
- **Marcus du Sautoy, *The Music of the Primes***（邦題『素数の音楽』）と **Simon Singh, *Fermat's Last Theorem***（邦題『フェルマーの最終定理』）：数学の背後にある人間の物語である。

整数論には人を引き込む性質がある。その問いは初日に尋ねられるほど単純でありながら、一生をかけて取り組めるほど深い。本章のいくつかの節を読んで、この先どうなるのかを知りたくなったのであれば、それこそがまさに本章の狙いである。

「次の一歩」の解答

ここに示すのは簡潔な答えとヒントであり、完全な解答ではない。結果と鍵となる段階を示してあるので、自分の答えを確かめるのに使ってほしい。見る前に、それぞれの演習問題にきちんと取り組むこと。

1.1 素数を生み出す工場

1. 素数（prime）が $p_1, \dots, p_k$ ですべてだと仮定すると、$p_1 \cdots p_k + 1$ はこのリストにない素因数（prime factor）をもち、矛盾（contradiction）が生じる。フェルマー数（Fermat number）を用いた証明は構成的（constructive）である。どの 2 つも互いに素（pairwise coprime）な無限個の数 $F_0, F_1, \dots$ を具体的に示し、そのそれぞれが新しい素数を与えるからである。

2. $n \geq 2$ のとき 2^n は 4 の倍数なので $2^{2^n} = 16^{2^{n-2}}$ であり、16 の累乗はどれも一の位が 6 である。したがって F_n の一の位は 7 である。

3. (a) 数学的帰納法（induction）による：$a_{n+1} - 1 = a_n(a_n - 1) = a_n \cdot a_1 \cdots a_{n-1}$。(b) a_m と a_n（$m < n$）の公約数（common factor）は $a_1 \cdots a_{n-1} = a_n - 1$ と a_n をともに割り切るので 1 である。よって各項は、他のどの項とも共有しない素因数をもつ。(c) $\frac{1}{a_n} = \frac{1}{a_n - 1} - \frac{1}{a_{n+1} - 1}$ であり、和は次々に打ち消し合って（telescoping）$1 - \frac{1}{a_{n+1} - 1}$ となる。

4. (a) $p \mid F_n$ より $2^{2^n} \equiv -1$ である。両辺を 2 乗すると $2^{2^{n+1}} \equiv 1$ となる。(b) d は $2^e \equiv 1$ を満たすすべての e を割り切るので $d \mid 2^{n+1}$ である。また（p は奇数なので）$2^{2^n} \equiv -1 \not\equiv 1$ であるから $d \nmid 2^n$ である。よって $d = 2^{n+1}$ である。(c) $2^{p-1} \equiv 1$ なので $2^{n+1} \mid p - 1$ である。(d) $641 = 64 \times 10 + 1$。641 未満で $64k + 1$ の形の素数は 193、257、449、577 である。試すべき候補はわずか 4 つであり、こうしてオイラー（Euler）は 641 を見つけた。

5. n 番目の素数は、$F_0, \dots, F_{n-1}$ の素因数のうち最大のもの以下であるから、$p_n \leq F_{n-1} = 2^{2^{n-1}} + 1$ である。$n = 5$ のときこの上界は 65 537 であるが、$p_5 = 11$ である。正しいが、極めて弱い評価である。

1.2 素数はどれほどまばらか？

1. $P_{1,10} = 210$、$P_{1,20} = 9\,699\,690$、$P_{1,30} = 6\,469\,693\,230$ である。$4^{30} \approx 1.15 \times 10^{18}$ および $e^{30} \approx 1.07 \times 10^{13}$ と比べると、この積は 4^n よりはるかに小さく、おおよそ e^n のように増大する（実際 $\ln P_{1,n} \sim n$ であり、これは素数定理（Prime Number Theorem）の一つの形である）。

2. $\binom{2m}{k+1} / \binom{2m}{k} = \frac{2m-k}{k+1}$ であり、これはちょうど $k < m$ のときに 1 を超えるので、二項係数（binomial coefficient）は中央まで増加し、その後減少する。和が 4^m となる $2m+1$ 個の項のうち最大のものは、それらの平均以上である。

3. $(\sqrt{n}, n]$ に含まれる素数はどれも $\sqrt{n}$ を超え、それらの積は 4^n より小さいので、$(\sqrt{n})^{\pi(n)-\pi(\sqrt{n})} < 4^n$ である。両辺の対数をとればよい。$2\ln 4 \approx 2.77$ かつ $\pi(\sqrt{n}) \le \sqrt{n}$ なので、求める評価が従う。この評価は正しい形 $n/\ln n$ をもつが、定数は真の値 1 ではなく 2.8 である。

4. 素数 $2, 3, 5, 7, 13, 23, 43, 83$ を用いる。どれも直前の素数の 2 倍より小さい。$n \le 50$ である任意の n に対して、このリストで n より大きい最初の素数は、直前の素数（これは n 以下である）の 2 倍より小さいので、n と $2n$ の間にある。

1.3 最小の反例

1. $k\sqrt{3}$ が整数となる最小の正の整数 k があるとすると、$k' = (\sqrt{3}-1)k$ はそれより小さい正の整数であり、しかも $k'\sqrt{3} = 3k - k\sqrt{3}$ は整数である。ここでは数 $\sqrt{3}-1$ が $\sqrt{2}-1$ の役割を果たしている。

2. $0 < \sqrt{N} - m < 1$ とすると、$k' = (\sqrt{N}-m)k$ は k より小さい正の整数であり、$k'\sqrt{N} = kN - mk\sqrt{N}$ は整数である。これは矛盾である。

3. $N = 4$ のとき $m = 2 = \sqrt{4}$ なので $\sqrt{N} - m = 0$ となり、$k' = 0$ は正の整数ではない。「$0 < \sqrt{N} - m$」という段階が成り立たない。

4. 図において、一辺 a の正方形の内部で重なり合う一辺 b の 2 つの正方形は、一辺 $2b - a$ の中央の正方形を 2 重に覆い、一辺 $a - b$ の 2 つの正方形を覆わずに残す。代数的には $(2b-a)^2 - 2(a-b)^2 = 2b^2 - a^2 = 0$ である。

1.4 e は無理数であり、e^2 もまた無理数である

1. $\frac{1}{e} = \frac{p}{q}$ とすると、$\frac{1}{e} = \sum_{k \ge 0} \frac{(-1)^k}{k!}$ の両辺に $q!$ を掛ける。$k \le q$ の項は整数であり、残りの和 $\sum_{k>q} (-1)^k q!/k!$ は項が減少する交代級数（alternating series）なので、その絶対値は 0 と $\frac{1}{q+1}$ の間に厳密にある。よって $q!/e$ は整数ではなく、矛盾である。

2. $\sin 1 = \frac{p}{q}$ とすると、$2n+1 \geq q$ として両辺に $(2n+1)!$ を掛ける。左辺は整数であり、級数の $\frac{1}{(2n+1)!}$ までの項も整数である。残りの和は交代級数で、その初項の大きさは $\frac{1}{(2n+2)(2n+3)} < 1$ なので、整数ではない。

3. この方法には、$\frac{1}{k!}$ のように、残りの和が分母の増大よりも速く小さくなる、有理数の項からなる級数が必要である。π についてはそのような級数は知られていない。ニーヴン（Niven）の証明は $\int_0^\pi \frac{x^n(\pi-x)^n}{n!} \sin x \, \mathrm{d}x$ を用いる。もし π が有理数ならば、これは十分大きな n に対して 1 より小さい正の整数となってしまう。

4. $x^2 - (e+\pi)x + e\pi$ の根は e と π である。$e+\pi$ と $e\pi$ がともに代数的（algebraic）であれば、π は代数的な係数をもつ多項式の根となり、したがって代数的となって、リンデマン（Lindemann）の定理に矛盾する。

1.5 無限降下法

1. $3 \mid a$ である。$a = 3a_1$ とおくと $9a_1^3 + b^3 = 3c^3$ となるので $3 \mid b$、さらに $3a_1^3 + 9b_1^3 = c^3$ となるので $3 \mid c$ であり、(a_1, b_1, c_1) はより小さい解となる。これが無限降下法（descent）である。$p^4 + 2q^4 = 5r^4$ について：4 乗数は 5 を法として（modulo）0 か 1 である（一の位が 0、1、5、6 のいずれかである）ので、$p^4 + 2q^4 \equiv 0$ から $5 \mid p$ かつ $5 \mid q$ が導かれる。すると $5^4 \mid 5r^4$ なので $5 \mid r$ となり、再び無限降下法が使える。

2. 平方数は 4 を法として 0 か 1 なので、$x^2 + y^2$ は 0、1、2 のいずれかであり、3 になることはない。

3. 有理点（rational point）$(\frac{a}{c}, \frac{b}{c})$ があれば、$c \neq 0$ で $a^2 + b^2 = 3c^2$ となるが、これは小問 (iii) で否定されている。

4. x、y を固定すると、この方程式は 2 次方程式 $z^2 - 3xyz + (x^2 + y^2) = 0$ であり、その 2 つの根の和は $3xy$ である。$(1,1,1)$ から $(1,1,2)$ が得られる。$(1,2)$ の反対側にある 1 を置き換えると $3 \cdot 1 \cdot 2 - 1 = 5$ となり、$(1,2,5)$ が得られる。続いて $(1,5,13)$ と $(2,5,29)$ が得られる。

1.6 二つの平方数の和

1. 平方数は 4 を法として 0 か 1 なので、2 つの平方数の和が 4 を法として 3 になることはない。

2. $65 = 1^2 + 8^2 = 4^2 + 7^2$、$85 = 2^2 + 9^2 = 6^2 + 7^2$ である。$65 = (2+\mathrm{i})(2-\mathrm{i})(3+2\mathrm{i})(3-2\mathrm{i})$ と分解すると、$(2+\mathrm{i})(3+2\mathrm{i}) = 4+7\mathrm{i}$、$(2+\mathrm{i})(3-2\mathrm{i}) = 8-\mathrm{i}$ となる。同様に 85 については、$(2+\mathrm{i})(4\pm\mathrm{i})$ から $7+6\mathrm{i}$ と $9-2\mathrm{i}$ が得られる。

3. $1105 = 4^2 + 33^2 = 9^2 + 32^2 = 12^2 + 31^2 = 23^2 + 24^2$ である。5、13、17 はそれぞ

れ、ガウス整数（Gaussian integer）とその共役（conjugate）の積に分解する。各組から因数を 1 つずつ選ぶと 8 個の積が得られ、それらは互いに共役なもの同士（同じ平方和を与える）で対になるので、4 個が残る。

4. 絶対値の 2 乗をとると $9 = (a^2+b^2)(c^2+d^2)$ となる。3 は 2 つの平方数の和ではないので、一方の因数は 1 である。

1.7 因数分解が破綻するとき

1. $693 = 9 \times 77 = 21 \times 33$ であり、4 つの因数はすべて S 素数である。作り方：$4k+3$ の形の 4 つの素数 p, q, r, s をとる。すると $(pq)(rs) = (pr)(qs)$ により、S 素数への 2 通りの分解が得られる。

2. E 素数は $2 \pmod 4$ である数である（2 つの偶数の積にはなりえないからである）。$60 = 2 \times 30 = 6 \times 10$。

3. $N(zw) = N(z)N(w)$ は $(ac-5bd)^2 + 5(ad+bc)^2$ を展開すれば確かめられる。a^2+5b^2 が 2 や 3 になることはない。$N(2) = 4$、$N(3) = 9$、$N(1 \pm \sqrt{-5}) = 6$ なので、単数（unit）でない元への分解には、ノルム（norm）が 2 または 3 の因数が必要になる。

4. 2 通りの異なる分解 $p_1 \cdots p_r = q_1 \cdots q_s$ をもつ最小の数を n とする。ユークリッド（Euclid）の補題により p_1 はある q_j を割り切るので、$p_1 = q_j$ である。これを約すと、2 通りの異なる分解をもつより小さい数が得られ、矛盾する。

1.8 有理数を数える

1. $\frac{3}{5}$：親をたどると $(3,5) \leftarrow (3,2) \leftarrow (1,2) \leftarrow (1,1)$ となり、位置は $1 \to 2 \to 5 \to 10$ なので $f(10) = \frac{3}{5}$ である。$\frac{5}{3}$：$(5,3) \leftarrow (2,3) \leftarrow (2,1) \leftarrow (1,1)$ であり、位置は $1 \to 3 \to 6 \to 13$ なので $f(13) = \frac{5}{3}$ である。

2. Newman の規則 $x_{n+1} = \frac{1}{2\lfloor x_n \rfloor - x_n + 1}$ からは 1、$\frac{1}{2}$、2、$\frac{1}{3}$、$\frac{3}{2}$、$\frac{2}{3}$、3、$\frac{1}{4}$、$\frac{4}{3}$、$\frac{3}{5}$ が得られ、これは $f(1), \ldots, f(10)$ と一致する。

3. n 番目の数の小数第 n 位が 5 でなければ、新しい数の小数第 n 位を 5 とし、5 ならば 4 とする。こうしてできる小数はリストのどの数とも異なり、しかも 0 と 9 を避けているので小数展開がただ 1 通りであるから、確かに異なる数である。

4. すべての正の整数は、2 の累乗と奇数の積 $2^{m-1}(2n-1)$ としてただ 1 通りに表せるので、$(m,n) \mapsto 2^{m-1}(2n-1)$ は全単射（bijection）である。

1.9 三次曲線の接線

1. $y = t(x+1)$ を $x^2 + y^2 = 1$ に代入すると $(1+t^2)x^2 + 2t^2x + t^2 - 1 = 0$ となり、その根は -1 と $\frac{1-t^2}{1+t^2}$ である。$t = \frac{q}{p}$ とするとその点は $\left(\frac{p^2-q^2}{p^2+q^2}, \frac{2pq}{p^2+q^2}\right)$ となり、三つ組 $(p^2-q^2, 2pq, p^2+q^2)$ が得られる。

2. 直線は $x + y = 3$ であり、$x^3 + (3-x)^3 = 9$ は $9x^2 - 27x + 18 = 0$ に帰着する。3 次の項が打ち消し合い、$x = 1, 2$ だけが残るのである。この直線は漸近線（asymptote）$y = -x$ に平行であり、第 3 の交点は無限遠にある。

3. 接線（tangent）の傾きは $\frac{x^2}{y^2} = \frac{289}{400}$ であり、接線は曲線と再び $\left(-\frac{188479}{90391}, -\frac{36520}{90391}\right)$ で交わる。分母を払うと $188479^3 = 36520^3 + 90391^3 + 180782^3$ となる。

4. この直線は $x^3 + y^3 = 1729$ と再び $\left(-\frac{37}{3}, \frac{46}{3}\right)$ で交わるので、$46^3 = 37^3 + 27 \times 1729 = 37^3 + 3^3 + 36^3$ である（$27 = 3^3$ と $27 \times 1728 = 36^3$ を用いた）。

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 1 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.