解答例

STEP III 2016、第 5 問

純粋数学 • 素数の積

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

この問題は、*Beyond STEP* の第 1.2 節「素数はどれほどまばらか？」で詳しく解説されている：https://beyondstep.keithmcnulty.org/ja/ch01/prime-distribution.html

鍵となる考え方

中央の二項係数（binomial coefficient）$\binom{2m+1}{m}$ は小さい（これとその双子である $\binom{2m+1}{m+1}$ は、ほかの項とともに合計 2^{2m+1} を分け合っている）が、$m+1$ と $2m+1$ の間にあるすべての素数で割り切れる。したがって、それらの素数の積も小さい。$2m+1$ 以下の素数を「$m+1$ 以下」と「$m+1$ より大きい」に分けると、強い数学的帰納法（strong induction）の準備が整う。偶数は（2 を除いて）決して素数にならないので、偶数の場合は何の手間もかからない。

解答

小問 (i)

$(1+x)^{2m+1}$ の二項展開（binomial expansion）に $x=1$ を代入すると

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

左辺の各項はすべて正である。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二つの項である。$m\geq 1$ であるから、項 $\binom{2m+1}{0}=1$ はこれらとは異なる第三の項である。よって

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

したがって $\binom{2m+1}{m} < 2^{2m}$ となり、示すべきことが得られた。

小問 (ii)

次のように書く。

$$\binom{2m+1}{m} = \frac{(2m+1)!}{m!\,(m+1)!}, \qquad \text{よって} \qquad m!\,(m+1)!\binom{2m+1}{m} = (2m+1)!.$$

p を $m+1 < p \leq 2m+1$ を満たす素数とする。このとき p は $(2m+1)!$ の因数の一つであるから、p は右辺を割り切る。一方、$m!\,(m+1)!$ の因数はどれも $m+1 < p$ 以下であるから、素数 p はそのどれも割り切らず、したがって $p \nmid m!\,(m+1)!$ である。積 ab を割り切る素数は a または b を割り切らなければならないので、$p \mid \binom{2m+1}{m}$ である。

> **考えてみよう** このような素数はそれぞれこの係数を割り切る。では、なぜそれらの積も割り切るのだろうか。

これらの素数は相異なるので、どの二つも互いに素（coprime）であり、どの二つも互いに素な数たちで割り切れる数は、それらの積で割り切れる。（同じことであるが、素因数分解の一意性（unique factorisation）により、これらの素数はそれぞれ $\binom{2m+1}{m}$ の素因数分解に現れる。）よって $P_{m+1,2m+1}$ は $\binom{2m+1}{m}$ を割り切る。そのような素数が存在しない場合は $P_{m+1,2m+1} = 1$ であり、これはあらゆる数を割り切る。

正の整数の正の約数はその数以下であるから、小問 (i) より

$$P_{m+1,2m+1} \leq \binom{2m+1}{m} < 2^{2m}.$$

小問 (iii)

$m \geq 1$ であるから $1 < m+1 < 2m+1$ が成り立つ。$p \leq 2m+1$ を満たす素数はすべて、$p \leq m+1$ または $m+1 < p \leq 2m+1$ のいずれか一方のみを満たすので

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

また（$m \geq 1$ より）$2 \leq m+1 \leq 2m$ であるから、$k = m+1$ は仮定が適用される値の一つであり、$P_{1,m+1} < 4^{m+1}$ が得られる。小問 (ii) と合わせて

$$P_{1,2m+1} < 4^{m+1} \cdot 2^{2m} = 4^{m+1} \cdot 4^m = 4^{2m+1}.$$

小問 (iv)

n に関する強い数学的帰納法を用いる。$S(n)$ を命題 $P_{1,n} < 4^n$ とする。

基本の場合。 $P_{1,2} = 2 < 16 = 4^2$ である。

帰納段階。 $n \geq 3$ とし、$k = 2, 3, \ldots, n-1$ に対して $S(k)$ が成り立つと仮定する。

- n が奇数のとき、$m \geq 1$ として $n = 2m+1$ と書く。このとき $n-1 = 2m$ であるから、$k = 2, \ldots, 2m$ に対して $S(k)$ が成り立つ。小問 (iii) より $P_{1,2m+1} < 4^{2m+1}$ が得られ、これは $S(n)$ そのものである。
- n が偶数のとき、$n \geq 4$ は 2 より大きい偶数であるから素数ではない。よって n 以下の素数はちょうど $n-1$ 以下の素数と一致し

$$P_{1,n} = P_{1,n-1} < 4^{n-1} < 4^n.$$

> **考えてみよう** なぜすべての n に対して小問 (iii) をそのまま使うことができないのだろうか。

小問 (iii) が扱えるのは奇数 $2m+1$ だけである。偶数 n に対しては別の議論が必要であり、2 より大きい偶数は積に新しい素数を加えないので、上の議論は簡単に済む。

よってどちらの場合も $S(n)$ が成り立ち、強い数学的帰納法により、すべての $n \geq 2$ に対して $P_{1,n} < 4^n$ である。

検算

- $m = 3$：$\binom{7}{3} = 35 < 64 = 2^6$ である。$(4, 7]$ に含まれる素数は 5 と 7 であり、$P_{4,7} = 35$ は 35 をちょうど割り切る。
- $m = 5$：$\binom{11}{5} = 462 = 2 \cdot 3 \cdot 7 \cdot 11$ であり、これは $P_{6,11} = 77$ で割り切れる。また $462 < 1024$ である。
- $P_{1,10} = 2 \cdot 3 \cdot 5 \cdot 7 = 210$ であり、$4^{10} = 1\,048\,576$ をはるかに下回る。コンピュータによる確認でも、2 から 1500 までのすべての n に対して $P_{1,n} < 4^n$ が成り立つ。

よくある間違い

- 小問 (i) で $<$ ではなく $\leq$ と書いてしまう。狭義の不等号にするには、中央の二つの項のほかに、$\binom{2m+1}{0}$ のような第三の正の項が必要である。
- 小問 (iii) で、$m+1$ が仮定の適用される範囲 $2, \ldots, 2m$ に入っていることの確認を忘れる。
- 小問 (iv) で、奇数の n しか扱わない、あるいは基本の場合 $n = 2$ を忘れる。

STEP のその先へ

これは、評価 $\prod_{p\le n} p < 4^n$ に対するエルデシュ（Erdős）の初等的な証明である。対数をとると、これはチェビシェフ（Chebyshev）の関数 $\theta(n) = \sum_{p\le n} \ln p$ が $n \ln 4$ より小さいことを意味する。これは、n 以下の素数の個数が $n/\ln n$ のオーダーであるというチェビシェフの定理の半分にあたる。エルデシュは同種の二項係数の議論を用いて、ベルトランの仮説（Bertrand's postulate）、すなわち n と $2n$ の間には常に素数が存在することを証明した。初等整数論を次に学ぶには、ダベンポート（Davenport）の *The Higher Arithmetic*（『高等算術』）がよい。

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