解答例

STEP II 2005、第 2 問

純粋数学 • オイラーのトーシェント関数

> **STEP II 2005、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/05-s2-q2

鍵となる考え方

すべては N を素因数分解（prime factorisation）の形で書くことから導かれる。各因子 $(1-\frac{1}{p}) = \frac{p-1}{p}$ は分母に p をもつが、N にはそれを約分する p が少なくとも 1 つは必ず含まれている。$\mathrm{f}(N)$ を素数冪（prime power）ごとの積として書き表してしまえば、$\mathrm{f}(m)\mathrm{f}(n)$ と $\mathrm{f}(mn)$ がどのようなときに一致するかが正確にわかる。それは m と n が共通の素因数をもつかどうかで決まるのである。

解答

小問 (i)

(a) $12 = 2^2 \cdot 3$ を割り切る素数は 2 と 3 であるから、

$$\mathrm{f}(12) = 12\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4.$$

$180 = 2^2 \cdot 3^2 \cdot 5$ を割り切る素数は 2、3、5 であるから、

$$\mathrm{f}(180) = 180 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 48.$$

(b) $N = 1$ のときは素因数が存在せず、積は空積（empty product）となるので $\mathrm{f}(1) = 1$ である。$N \geq 2$ のときは

$$N = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

と書く。ここで p_i は N を割り切る相異なる素数であり、すべての $a_i \geq 1$ である。こ

のとき

$$\begin{aligned} f(N) &= p_1^{a_1} \cdots p_k^{a_k} \cdot \frac{p_1 - 1}{p_1} \cdots \frac{p_k - 1}{p_k} \\ &= p_1^{a_1 - 1}(p_1 - 1)\, p_2^{a_2 - 1}(p_2 - 1) \cdots p_k^{a_k - 1}(p_k - 1). \end{aligned}$$

各 $a_i \geq 1$ であるから、指数 $a_i - 1$ はすべて非負整数であり、したがって各因子 $p_i^{a_i - 1}(p_i - 1)$ は正の整数である。ゆえに、すべての N について $f(N)$ は整数である。この問題の残りの部分では、次の公式

$$f(N) = \prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1), \qquad (*)$$

を用いる。

小問 (ii)

(a) これは偽である。$m = n = 2$ とする。このとき $f(2) = 2 \cdot \frac{1}{2} = 1$ であるから $f(2)f(2) = 1$ となるが、$f(4) = 4 \cdot \frac{1}{2} = 2$ である。

問題は、因子 $(1 - \frac{1}{2})$ が左辺には 2 回現れるのに右辺には 1 回しか現れないことにある。2 は 4 の素因数として 1 回しか数えられないからである。

(b) これは真である。p と q が相異なる素数ならば、$f(p) = p(1 - \frac{1}{p}) = p - 1$ であり、同様に $f(q) = q - 1$ である。pq を割り切る素数はちょうど p と q であり、これらは異なるから、

$$f(pq) = pq\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) = (p - 1)(q - 1) = f(p)f(q).$$

(c) 主張は、$f(p)f(q) = f(pq)$ が成り立つのは p と q が相異なる素数のときに限る、すなわちこの等式が成り立てば p と q は必ず相異なる素数になる、というものである。これは偽である。$p = 3$、$q = 4$ とする。等式が意味をもつためにこれらが素数である必要はない。このとき

$$f(3)f(4) = 2 \cdot 2 = 4 = f(12),$$

が小問 (i)(a) より成り立つが、4 は素数ではない。（さらに簡単な例は $p = 1$ である。すべての q について $f(1)f(q) = f(q)$ となるからである。）

> **考えてみよう** 素数であることでないとすれば、等式を成り立たせている本当の理由は何だろうか。

重要なのは、p と q が共通の素因数をもたないことである。$\gcd(m, n) = 1$ ならば、m に含まれる素数冪と n に含まれる素数冪は互いに異なるので、mn の素因数分解は 2 つの素因数分解を単に並べたものになり、$(*)$ より $f(mn) = f(m)f(n)$ が得られる。あ

る素数 r が両方を割り切るならば、因子 $(1-\frac{1}{r})$ は $\mathrm{f}(m)\mathrm{f}(n)$ には 2 回現れるが $\mathrm{f}(mn)$ には 1 回しか現れないので、$\mathrm{f}(m)\mathrm{f}(n) < \mathrm{f}(mn)$ となる。したがって、等式が成り立つのはちょうど $\gcd(m,n)=1$ のときであり、3、4 は素数の組ではない互いに素（coprime）な組の一例にすぎない。

一方、小問 (ii) 全体を通じて p と q が素数を表すと読むならば、(c) は $p=q$ となりうるかどうかだけを問うていることになり、その答えは否である。$\mathrm{f}(p)^2=(p-1)^2$ であるのに対し $\mathrm{f}(p^2)=p(p-1)$ であり、$p-1\neq p$ であるからこれらは決して等しくならない。この読み方のもとでは (c) は真である。上の反例（counterexample）を伴う一般的な読み方のほうが、より自然である。

小問 (iii)

$(*)$ より、素数冪については

$$\mathrm{f}(p^m)=p^{m-1}(p-1).$$

である。目標の数を素因数分解すると、$14641=121^2=11^4$ であるから $146410=10\times 14641=2\cdot 5\cdot 11^4$ となる。これはすでに $p=11$ とした $p^{m-1}(p-1)$ の形をしている。実際 $11^4\cdot 10=11^4(11-1)$ であるから $m-1=4$ である。ゆえに

$$p=11,\quad m=5:\qquad \mathrm{f}(11^5)=11^4\cdot 10=146410.$$

実はこれが唯一の答えである。$m\geq 2$ ならば p は 146410 を割り切るので、$p\in\{2,5,11\}$ である。$p=2$ とすると $2^{m-1}=146410$ となるが、146410 は奇数の素因数をもつので不可能である。$p=5$ とすると $4\cdot 5^{m-1}=146410$ となるが、146410 は 4 で割り切れないので不可能である。残るのは $p=11$ であり、このとき $m=5$ となる。$m=1$ ならば $p=146411$ が素数でなければならないが、$146411=41\times 3571$ である。

検算

- この関数はオイラー（Euler）のトーシェント関数（totient function）である。すなわち $\mathrm{f}(N)$ は $\{1,\dots,N\}$ に含まれる整数のうち N と互いに素なものの個数を数える。たとえば $N=12$ に対しては、そのような 4 つの数は $1,5,7,11$ である。コンピュータにより、すべての $N<2000$ について、積の公式がこの個数と一致し、かつ整数になることが確かめられた。
- 問題文中の例では $\mathrm{f}(80)=80\cdot\frac{1}{2}\cdot\frac{4}{5}=32=2^3(2-1)\cdot 5^0(5-1)$ であり、これは $(*)$ と一致する。
- コンピュータで $m,n\leq 400$ の無作為な組を 20 000 個調べたところ、$\mathrm{f}(m)\mathrm{f}(n)=$

$\mathrm{f}(mn)$ となるのはちょうど $\gcd(m,n) = 1$ のときであった。また、すべての素数 $p \leq 146411$ を探索したところ、(iii) の解は $(p,m) = (11,5)$ のみであった。

よくある間違い

- 積の中に同じ素数を 2 回以上含めてしまうこと。$180 = 2^2 \cdot 3^2 \cdot 5$ に対しては、因子は 5 個ではなく 3 個である。
- 「のときに限り（only if）」を「ならば（if）」と取り違えること。小問 (b) は「ならば」の向きであり、小問 (c) はその逆（converse）であって、別の命題である。
- (iii) で $14641 = 11^4$ に気づかないこと。$11^2 = 121$ かつ $121^2 = 14641$ であることに気づくか、パスカルの三角形（Pascal's triangle）の行 $1, 4, 6, 4, 1$ であると見抜けば、すぐに見つかる。

STEP のその先へ

この関数はオイラーのトーシェント関数 φ であり、小問 (ii) の事実は、これが**乗法的**（multiplicative）であることを述べている。すなわち、一般には成り立たないものの、$\gcd(m,n) = 1$ のときには常に $\varphi(mn) = \varphi(m)\varphi(n)$ が成り立つ。この関数はオイラーの定理（Euler's theorem）、すなわち n と互いに素な a に対する $a^{\varphi(n)} \equiv 1 \pmod{n}$ に現れる。この定理はフェルマー（Fermat）の小定理（Fermat's little theorem）を一般化したものであり、RSA 暗号（RSA encryption）の基礎となっている。群論（group theory）では、$\varphi(n)$ は n を法とする単数群（group of units）の位数（order）である。Davenport の *The Higher Arithmetic*（『高等算術』）は、これらすべてを見事に展開している。

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