解答例

STEP I 1996、第 3 問

純粋数学 • 整数の整除性

> **STEP I 1996、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/96-s1-q3

鍵となる考え方

24 のような合成数（composite number）による割り切れやすさを扱うには、素数の冪（prime power）ごとに一つずつ考えるのが最も簡単である。$24 = 3 \times 8$ であり、3 と 8 は互いに素（coprime）であるから、3 で割り切れることと 8 で割り切れることを別々に示せばよい。因数分解（factorisation）すると連続する整数（consecutive integers）の積が現れ、任意の k 個の連続する整数の中には必ず k の倍数が一つ含まれる。残りの二つの小問も同じ習慣で解ける。すなわち、因数分解するか、あるいは n をその余り（remainder）が見える形に書くのである。

解答

小問 (i)

共通因数をくくり出し、平方の差（difference of two squares）の公式を用いると、

$$n^5 - n^3 = n^3(n^2 - 1) = n^3(n-1)(n+1) = n^2\,(n-1)\,n\,(n+1).$$

3 で割り切れること。 $n-1$、n、$n+1$ は連続する三つの整数であるから、そのうちちょうど一つが 3 の倍数である。よって $3 \mid (n-1)n(n+1)$ であり、したがって $3 \mid n^5 - n^3$ である。

8 で割り切れること。 n の偶奇（parity）で場合分けする。

- n が偶数のとき、$n = 2m$ とおくと $n^3 = 8m^3$ であり、これは 8 の倍数である。
- n が奇数のとき、$n-1$ と $n+1$ は連続する二つの偶数である。連続する二つの偶数

のうち一方は 4 の倍数で、もう一方は 2 の倍数であるから、$8 \mid (n-1)(n+1)$ である。

いずれの場合も $8 \mid n^3(n-1)(n+1) = n^5 - n^3$ である。

考えてみよう $3 \mid N$ かつ $8 \mid N$ であることから、なぜ $24 \mid N$ が導かれるのか。$4 \mid N$ かつ $6 \mid N$ からも同じことが言えるだろうか。

3 と 8 には共通因数がないので、$8 \mid N$ ならば $N = 8a$ と書け、このとき $3 \mid 8a$ から $3 \mid a$ が従う（3 は素数であり、8 を割り切らないからである）。よって $N = 24b$ となる。4 と 6 は因数 2 を共有するので、この議論は成り立たない。実際、数 12 はどちらでも割り切れるが、24 では割り切れない。

以上より、すべての正の整数 n に対して $n^5 - n^3$ は 24 で割り切れる。これが示すべきことであった。

小問 (ii)

$2^{2n} = 4^n$ と書く。因数分解 $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$ に $x = 4$ を代入すると、

$$2^{2n} - 1 = 4^n - 1 = (4-1)\left(4^{n-1} + 4^{n-2} + \cdots + 4 + 1\right) = 3\left(4^{n-1} + \cdots + 1\right).$$

括弧の中は整数であるから、$2^{2n} - 1$ は 3 で割り切れる。

同じことを合同式の算術（modular arithmetic）で述べると次のようになる。$4 \equiv 1 \pmod 3$ であるから、$4^n \equiv 1^n = 1 \pmod 3$ である。数学的帰納法（induction）による証明も可能である。$4^k - 1 = 3a$ ならば、$4^{k+1} - 1 = 4(4^k - 1) + 3 = 3(4a + 1)$ となる。

小問 (iii)

$3 \mid n - 1$ であるから、ある整数 $k \geq 0$ を用いて $n = 3k + 1$ と書ける。次のように因数分解する。

$$n^3 - 1 = (n-1)(n^2 + n + 1).$$

第一の因数は $n - 1 = 3k$ である。第二の因数については、

$$\begin{aligned} n^2 + n + 1 &= (9k^2 + 6k + 1) + (3k + 1) + 1 \\ &= 9k^2 + 9k + 3 \\ &= 3(3k^2 + 3k + 1). \end{aligned}$$

したがって、各因数がそれぞれ 3 を一つずつもたらす。

$$n^3 - 1 = 3k \cdot 3(3k^2 + 3k + 1) = 9k(3k^2 + 3k + 1),$$

これは 9 で割り切れる。これが示すべきことであった。（$n = 1$ のときは $k = 0$ であり、$n^3 - 1 = 0$ となるが、これも 9 で割り切れる。）

要点は、$n - 1$ が与える 3 の因数は一つだけであり、二つ目は $n^2 + n + 1$ から来るということである。この二つ目の因数を見るうまい方法は、$n^2 + n + 1 = (n-1)^2 + 3n$ と書くことである。$3 \mid n - 1$ のとき、これは 3 の倍数二つの和になっている。

検算

- 小問 (i)：$n = 2$ のとき $32 - 8 = 24$、$n = 3$ のとき $243 - 27 = 216 = 9 \times 24$ である。$n = 2$ のときちょうど 24 になるので、すべての $n^5 - n^3$ を割り切るこれより大きな数は存在しない。よって 24 は最良である。
- 小問 (ii)：$n = 1, 2, 3$ のとき、それぞれ 3、15、63 となる。
- 小問 (iii)：$n = 4$ のとき $63 = 7 \times 9$、$n = 7$ のとき $342 = 38 \times 9$ であり、それぞれ $k = 1$、$k = 2$ のときの $9k(3k^2 + 3k + 1)$ と一致する。

三つの結果はいずれも、5000 未満のすべての n について（小問 (ii) は $n < 2000$ について）コンピュータで確かめた。また、$n^5 - n^3$ の値の最大公約数（highest common factor）がちょうど 24 であることも確認した。

よくある間違い

- 「$(n-1)n(n+1)$ は 6 で割り切れ、n^2 は ...」と論じて、因数 8 がどこから来るのかを見失うこと。偶数の場合には n だけでなく n^3 が必要である。
- 4 で割り切れることと 6 で割り切れることから、24 で割り切れると結論すること。因数は互いに素でなければならない。
- 小問 (iii) で、「$n - 1$ は 3 で割り切れるので、$n^3 - 1 = (n-1)(\dots)$ は 3 で割り切れる」で止まってしまうこと。これでは 3 の因数が一つしか得られない。

STEP のその先へ

三つの小問はいずれも、本質的には合同式の算術における命題である。m を法とする整数全体は環（ring）をなし、小問 (iii) は $n \equiv 1 \pmod 3$ ならば $n^3 \equiv 1 \pmod 9$ であることを述べている。これは**指数持ち上げ**（lifting the exponent）と呼ばれる一般的な現象の第一歩である。すなわち、$p \mid n - 1$ ならば $p^{j+1} \mid n^{p^j} - 1$ が成り立つ。フェルマー（Fermat）の小定理（Fermat's little theorem）（$n^p \equiv n \pmod p$）は小問 (i) の説

明にもなる。この定理から直ちに $3 \mid n^3 - n$ が得られるからである。Davenport の *The Higher Arithmetic*（『高等算術』）は、これらの考え方への美しい入門書である。

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。