解答例

STEP II 1994、第 1 問

純粋数学 ・ 整除性と十進数の各位の数字

> **STEP II 1994、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/94-s2-q1

鍵となる考え方

積の下何桁かは因数の下何桁かだけで決まる。したがって、ここでの議論はすべて 10 のべきを法とする（modulo）算術である。末尾が 1, 3, 7, 9 のいずれかである数は 10 と共通の因数をもたず、そのため 10 を法として**可逆**（invertible）であり、実は 10 の任意のべきを法としても可逆である。中盤の小問では、n から因数 2 と 5 を取り除き、それらを末尾の 0 に変える。最後の小問では、10^{10} を法とする可逆性を用いて、積の下 10 桁を好きな数字の並びにできることを示す。

解答

小問 1：末尾が 1 になる倍数

$n \times m$ の一の位は、（n の一の位）×（m の一の位）の一の位に等しい。他の桁からの寄与はすべて 10 の倍数だからである。n の末尾は 5 でも偶数でもないので、1, 3, 7, 9 のいずれかであり、

$$1 \times 1 = 1, \qquad 3 \times 7 = 21, \qquad 7 \times 3 = 21, \qquad 9 \times 9 = 81.$$

となる。そこで、それぞれ $m = 1, 7, 3, 9$ とすればよい。このとき $n \times m$ の末尾は 1 となり、求める結果が得られる。

小問 2：任意の n

$$n = 2^a \, 5^b \, k,$$

と表す。ここで $a, b \geq 0$ であり、k は 2 でも 5 でも割り切れない。すると k の末尾は 5 でも偶数でもないので、小問 1 より、km' の末尾が 1 となる m' が存在する。ここで

$$m = 2^b\, 5^a\, m'.$$

とおく。すると

$$n \times m = 2^{a+b}\, 5^{a+b}\, km' = 10^{a+b}\, (km').$$

となる。10^{a+b} を掛けることは、km' の後ろに $a+b$ 個の 0 を付け加えることにすぎない。よって $n \times m$ の末尾は、$a+b=0$ ならば 1、そうでなければ 1 の後に $a+b$ 個の 0 が続く形である。これが示すべきことであった。

例えば $n = 40 = 2^3 \cdot 5$ のとき $k = 1$ であるから、$m = 2 \cdot 5^3 = 250$ となり、$n \times m = 10\,000$ である。

小問 3：10 種類すべての数字

$n = 10^r q$ と表す。ただし $r \geq 0$ であり、q の末尾は 1 である。末尾に 0 を付け加えても既存の数字が消えることはないので、$q \times m$ がすべての数字を含むような m を見つければ十分である。そうすれば $n \times m = 10^r (qm)$ もすべての数字を含む。

$N = 10^{10}$、$X = 1234567890$ とおく。X はすべての数字を含む。目標は

$$qm \equiv X \pmod{N},$$

すなわち、qm の下 10 桁を 1234567890 にすることである。

> **考えてみよう** q のある倍数を 10^{10} で割った余りが X になるのはなぜか？

N 個の数 $q \times 0,\ q \times 1,\ \ldots,\ q \times (N-1)$ と、それらを N で割った余りを考える。仮にそのうち 2 つが等しく、$0 \leq t < s \leq N-1$ について $qs \equiv qt \pmod{N}$ であったとする。このとき 10^{10} は $q(s-t)$ を割り切る。ところが q の末尾は 1 なので奇数であり、5 の倍数でもない。したがって $10^{10} = 2^{10}5^{10}$ と共通の素因数をもたない。ゆえに $2^{10}5^{10}$ は $s-t$ を割り切るが、$0 < s-t < N$ であるからこれは不可能である。よって N 個の余りはすべて異なる。余りとしてありうる値は $0, 1, \ldots, N-1$ の N 個しかないので、そのすべてが現れる。特に、$0 \leq m \leq N-1$ を満たすある m について $qm \equiv X \pmod{N}$ が成り立つ。

$X \neq 0$ であるから、この m は 0 ではない。よって qm は正の倍数であり、$qm \geq X \geq 10^9$ を満たす。したがって、その下 10 桁はちょうど $1, 2, 3, 4, 5, 6, 7, 8, 9, 0$ であり、X の先頭の 1 も確かに現れている。以上より、$q \times m$、したがって $n \times m$ は、すべての数字 $0, 1, \ldots, 9$ を含む。

例えば $n = 21$ のとき $m = 7\,201\,646\,090$ とすることができ、このとき $21 \times m = 151\,234\,567\,890$ である。

考えてみよう n に関する仮定（hypothesis）はどこで使われたか？　また、なぜそれが必要だったのか？

この仮定は、q が因数 2 も 5 ももたないことを知るためだけに使った。それがなければ、余り $qm \bmod 10^{10}$ はすべての値をとることができない。例えば、2 の倍数はすべて偶数なので、末尾が $\ldots 1$ になることはありえない。積の**末尾**を思いどおりに定められるのは、この仮定のおかげである。（小問 2 により、任意の n はこの形の倍数をもつことがわかるので、小問 3 と合わせれば、**すべての** n が 10 種類すべての数字を含む倍数をもつことになる。）

検算

- 小問 1 の手計算による確認：$13 \times 7 = 91$、$29 \times 9 = 261$。
- コンピュータによる検証で、末尾が 5 でも偶数でもないすべての $n \leq 20\,000$ について、小問 1 の手順が正しいことを確認した。小問 2 の構成については、すべての $n \leq 20\,000$ と、10^{15} 以下の無作為な 20 000 個の n について確認した。さらに、末尾に 0 がいくつも並ぶものも含め、条件を満たす形の 10 000 個を超える n の値について小問 3 の乗数を計算し、いずれの場合も $n \times m$ が 10 種類すべての数字を含むことを確かめた。例：$21 \times 7\,201\,646\,090 = 151\,234\,567\,890$、$11 \times 4\,657\,687\,990 = 51\,234\,567\,890$。

よくある間違い

- 小問 3 で、並び 1234567890 が本当に完全な形で現れることの確認を忘れる。先頭の 1 が現れるには $qm \geq 10^9$ が必要であり、これは $qm \equiv X$ かつ $qm > 0$ であることから成り立つ。
- 小問 2 で、$2^b 5^a$ の代わりに 10^{a+b} を掛けてしまう。これでは 0 は付け加わるが、n にもともと含まれていた 2 と 5 はそのまま残ってしまう。

STEP のその先へ

小問 3 の鳩の巣原理（pigeonhole principle）による議論は、一般的な事実を証明している。すなわち、$\gcd(q, N) = 1$ ならば、q は N を法とする乗法逆元（multiplicative inverse）をもつ。可逆な剰余類（residue）は群（group）をなし、$(\mathbb{Z}/N\mathbb{Z})^\times$ と書かれる。これは初等整数論の出発点であり、RSA 暗号（RSA cryptography）の出発点でもある。別の工夫を用いると、最後の小問が任意の n について成り立つことが示せる。$10^k \geq n$ となれば、n のある倍数が $X \cdot 10^k$ と $X \cdot 10^k + 10^k$ の間にあり、そのような倍

数は 1234567890 で始まるのである。Davenport の *The Higher Arithmetic*（『高等算術』）は、合同式（congruence）と剰余類へのすばらしい入門書である。

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。