解答例

STEP III 1987、第 1 問

純粋数学 • 階乗の整除性

> **STEP III 1987、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/87-s3-q1

鍵となる考え方

階乗（factorial）$(n-1)! = 1 \times 2 \times \cdots \times (n-1)$ には、n より小さいすべての自然数が含まれている。n が n より小さい 2 つの**相異なる**数の積として表せるならば、その 2 数はどちらも階乗の中に現れるので、n はそれを割り切る。したがって、この問題の本質は、どのような n がそのように分解**できない**かという点にある。素数（prime）が分解できないのは明らかであり、素数の平方についてはもう少し詳しく調べる必要がある。最初の十数個の値を手で試してみれば、答えはすぐに見えてくる。

解答

まず実験する

簡単な表を作ってみる価値がある。

n	1	2	3	4	5	6	7	8
$(n-1)!$	1	1	2	6	24	120	720	5040
$n \mid (n-1)!$?	はい	いいえ	いいえ	いいえ	いいえ	はい	いいえ	はい

割り切れないのは $2, 3, 4, 5, 7$ であり、これはここまでの素数と 4 である。以下、このパターンが続くことを証明する。

主張。 n が $(n-1)!$ を割り切らないのは、n が素数であるか $n = 4$ であるときであり、またそのときに限る。

$n = 1$

このとき $(n-1)! = 0! = 1$ であり、1 は 1 を割り切る。よって $n = 1$ は求める集合に含まれない。

$n = p$ が素数のとき

$(p-1)!$ の各因数 $1, 2, \ldots, p-1$ はいずれも p より小さい正の数であるから、どれも p で割り切れない。p は素数なので、p が積を割り切るならば、因数のいずれかを割り切らなければならない（ユークリッド（Euclid）の補題（Euclid's lemma））。したがって $p \nmid (p-1)!$ であり、すべての素数は求める集合に含まれる。

n が合成数のとき

n の最小の素因数を p とし、$n = pm$ と書く。n は合成数（composite number）であるから $m > 1$ であり、m の素因数はどれも p 以上なので $m \geq p$ である。2 つの場合に分ける。

場合 1：$m > p$ のとき。 このとき $1 < p < m < n$ であるから、p と m は $1, 2, \ldots, n-1$ の中の 2 つの相異なる数である。よって、それらの積 $pm = n$ は $(n-1)!$ を割り切る。

場合 2：$m = p$、すなわち $n = p^2$ のとき。

> **考えてみよう** 場合 1 の議論がここで使えないのはなぜか。また、何で置き換えればよいか。

因数 p は $1, \ldots, n-1$ の中に一度しか現れないので、2 回使うことはできない。そこで代わりに p と $2p$ を用いる。$p \geq 3$ ならば

$$2p < p \cdot p = n,$$

であるから、p と $2p$ は $1, 2, \ldots, n-1$ の中の 2 つの相異なる数である。したがって、それらの積 $2p^2 = 2n$ は $(n-1)!$ を割り切り、よって n も $(n-1)!$ を割り切る。

$p = 2$ のときは、$2p = 4 = n$ が列に含まれないので、この議論は成り立たない。実際、$n = 4$ のとき $3! = 6$ であり、$4 \nmid 6$ である。よって 4 は求める集合に含まれる。

結論

4 以外のすべての合成数 n は $(n-1)!$ を割り切り、$n = 1$ も同様である。したがって、求める集合は

$$\{ n : n \text{ は素数} \} \cup \{4\} = \{2, 3, 4, 5, 7, 11, 13, 17, \ldots\}.$$

である。

検算

上の表は $n \leq 8$ について主張と一致している。素数の平方も試してみよう。$n = 9$ のとき $8! = 40320 = 9 \times 4480$ であり、場合 2 の予測どおりである（因数 3 と 6 を用いる）。$n \leq 2000$ のすべての n について $(n-1)! \bmod n$ を直接計算するコンピュータによる確認でも、主張の例外は見つからない。

よくある間違い

- $a \neq b$ を要求せずに「$a, b < n$ として $n = ab$ と書けば $ab \mid (n-1)!$」と論じること。この議論では $4 \mid 3!$ が誤って「証明」されてしまう。
- $n = 1$ を忘れること。$0! = 1$ であるから、$n = 1$ は集合に含まれない。
- 素数 p が $(p-1)!$ を割り切らない理由を「p が因数の 1 つではないから」とすること。本当の理由は、p が素数であり、どの因数も割り切らないことである。合成数は、因数の 1 つでなくても積を割り切ることがある。

STEP のその先へ

素数については、ウィルソンの定理（Wilson's theorem）と呼ばれる、より精密な事実がある。すなわち $(p-1)! \equiv -1 \pmod{p}$ である。この問題と合わせると、（非常に遅い）素数判定法（primality test）が得られる。すなわち、$n > 1$ が素数であるのは $(n-1)! \equiv -1 \pmod{n}$ であるとき、またそのときに限る。ウィルソンの定理は、各数を p を法とする逆元（inverse）と組にすることで証明される。これは p を法とする整数の群構造（group structure）に初めて触れる機会となる。Davenport の *The Higher Arithmetic*（『高等算術』）は、この内容を見事に解説している。

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。