解答例

STEP II 見本問題、第 8 問

純粋数学 • 剰余群における位数

> **STEP II 見本問題、問 8**
>
> 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/spec-s2-q8

鍵となる考え方

N を法として（modulo）考えると、数 $N-1$ は -1 にほかならず、$m+n=N$ は $n\equiv -m$ を意味する。したがって n のどの累乗も、符号を除けば m の累乗であり、$n^k\equiv(-1)^k m^k$ となる。この符号が効くかどうかは k が偶数か奇数かで決まり、三つの小問は位数（order）の偶奇の三通りの組み合わせ方に対応している。最後の部分では、これらの事実を用いて、すべての累乗を計算することなく位数を求める。

解答

以下、$\equiv$ は N を法とする合同（congruent）を表す。問題の意図に従い、G の単位元（identity）を 1 とする。（実際、$N-1\in G$ であれば必ずそうなる。e が単位元ならば $e(N-1)\equiv N-1$、すなわち $-e\equiv -1$ であるから $e=1$ である。）

$N-1$ の位数

次が成り立つ。

$$(N-1)^2=N^2-2N+1\equiv 1,$$

また $N-1\neq 1$ である。$N\geq 3$ だからである。よって $(N-1)^1$ は単位元ではないが $(N-1)^2$ は単位元である。すなわち $N-1$ の位数は 2 である。

小問の準備

$m+n=N$ より $n\equiv -m$ であるから、すべての正の整数 k に対して

$$n^k\equiv(-1)^k m^k,\qquad \text{同値な形で}\qquad m^k\equiv(-1)^k n^k.$$

が成り立つ。また $N-1 \equiv -1 \equiv n\,m^{-1}$ は G に属する。G は n と m^{-1} を含む群（group）だからである。よって -1 は G の元であり、しかも $-1 \neq 1$ である（$N \geq 3$ による）。さらに、x の位数が r で $x^k = 1$ ならば $r \mid k$ であるという標準的な事実も用いる（$k = ar + b$、$0 \leq b < r$ と書くと $x^b = 1$ となり、r の最小性より $b = 0$ である）。

小問 (i)

p と q がともに偶数であるとする。このとき

$$n^p \equiv (-1)^p m^p = m^p \equiv 1,$$

であるから $q \mid p$ である。同様に $m^q \equiv (-1)^q n^q = n^q \equiv 1$ であるから $p \mid q$ である。互いに他を割り切る二つの正の整数は等しいので、$p = q$ である。

小問 (ii)

p が偶数、q が奇数であるとする。p は偶数なので $n^p \equiv m^p \equiv 1$ であり、$q \mid p$ である。また $2q$ は偶数なので

$$m^{2q} \equiv n^{2q} = (n^q)^2 \equiv 1,$$

となり、$p \mid 2q$ を得る。$p = kq$ と書くと $kq \mid 2q$ であるから $k \mid 2$ であり、$k = 1$ または 2 である。しかし $k = 1$ とすると $p = q$ が奇数となってしまうが、そうではない。ゆえに $k = 2$ であり、$p = 2q$ である。

> **考えてみよう** なぜ単純に $m^q \equiv -n^q \equiv -1$ だから「p は $2q$ でなければならない」と論じることはできないのか？

この計算は正しく、$m^q \neq 1$ かつ $m^{2q} \equiv 1$ であることを示している。しかしそれだけでは $p \mid 2q$ と $p \nmid q$ がわかるにすぎず、p は確定しない（たとえば先験的には、p が 2 で $q = 3$ ということもありうる）。追加の整除関係 $q \mid p$ は p が偶数であることから従い、これこそがこの隙間を埋めるのである。

小問 (iii)

背理法（proof by contradiction）のため、p と q がともに奇数であると仮定し、$r = pq$ とおく。これは奇数である。このとき

$$n^r = (n^q)^p \equiv 1, \qquad \text{しかし一方で} \qquad n^r \equiv (-1)^r m^r = -(m^p)^q \equiv -1.$$

よって $1 \equiv -1$、すなわち $N \mid 2$ となるが、これは $N \geq 3$ なので不可能である。ゆえに p と q がともに奇数であることはない。

（対称性により、小問 (ii) からは $q = 2p$ も得られる。ただし q が偶数で p が奇数のときである。したがってどの場合も、m と $N - m$ の位数は、等しくかつ偶数であるか、一方が他方の二倍で、その他方が奇数であるかのいずれかである。）

21 を法とする群

2 と 5 の累乗を順に 21 を法として簡約すると、次のようになる。

k	1	2	3	4	5	6
2^k	2	4	8	16	11	1
5^k	5	4	20	16	17	1

（たとえば $2^5 = 32 \equiv 11$、$5^2 = 25 \equiv 4$、$5^4 \equiv 4^2 = 16$、$5^5 \equiv 80 \equiv 17$ である。）両方の行で最初に 1 が現れるのは $k = 6$ であるから、2 と 5 はともに位数 6 をもつ。

では表から位数を読み取ろう。x の位数が 6 ならば、x^k の位数は $6/\gcd(k, 6)$ である。よって

- $11 = 2^5$ と $17 = 5^5$ の位数は 6 である。
- $4 = 2^2$ と $16 = 2^4$ の位数は 3 である。
- $8 = 2^3$ と $20 = 5^3$ の位数は 2 である（$20 = N - 1$ であるから、これは最初の部分からすでにわかっている）。
- 1 の位数は 1 である。

残るのは 10、13、19 であり、いずれも既知の元と組になって和が 21 となる。

- $13 = 21 - 8$ であり、8 は偶数の位数 2 をもつ。(iii) とその後の注意により、13 の位数は 2（等しく偶数）か 1（2 の半分）のいずれかである。位数は 1 ではない。$13 \neq 1$ だからである。よって 13 の位数は 2 である。（検算：$13^2 = 169 = 8 \cdot 21 + 1$。）
- $19 = 21 - 2$、$10 = 21 - 11$ であり、2 と 11 の位数は 6 である。よって 19 と 10 の位数はそれぞれ 6 または 3 である。

したがって G のすべての元の位数は高々 6 である。位数 12 の巡回群（cyclic group）には生成元（generator）、すなわち位数 12 の元が存在し、同型写像（isomorphism）は元の位数を保つ。G には位数 12 の元が存在しないので、位数 12 の巡回群とは同型でない。

別の締めくくり方もある。G には位数 2 の元が三つ、すなわち 8、13、20 があるが、位数 12 の巡回群にはちょうど一つしかない（g が生成元ならば、g^k の位数が 2 となるのは $k = 6$ のときに限る）。

検算

コンピュータで確認すると、G における位数の完全な一覧は次のとおりである。1 の位数は 1、8, 13, 20 の位数は 2、4, 16 の位数は 3、2, 5, 10, 11, 17, 19 の位数は 6 である。（直接計算すると $10^3 = 1000 \equiv 13$、$19^3 \equiv (-2)^3 = -8 \equiv 13$ であるから、どちらも位数 3 ではない。）個数 $1+3+2+6 = 12$ は G の大きさに一致する。さらに小問 (i)–(iii) を、すべての組 m、$N-m$ について検証した。対象は、高々二つの元で生成される単元群（group of units）のあらゆる部分群であり、$N < 60$ のすべてにわたる。約 1900 組を調べ、例外はなかった。

よくある間違い

- 理由を述べずに $N-1 \in G$ を仮定すること。これは与えられていないが、$m, n \in G$ から従う。$N-1 \equiv n\,m^{-1}$ だからである。
- (ii) において $p \mid 2q$ だけを示すこと。等号を得るには、もう一つの整除関係が必要である。
- 奇妙な場合に単位元を当然視すること。たとえば部分集合 $\{3\}$ は、6 を法として乗法について閉じており、その単位元は 3 である。そして $m = n = 3$ とすると (iii) に反してしまう。議論は単位元が 1 であることに依拠しているが、意図されているのは明らかにそちらである。

STEP のその先へ

G は 21 を法とする単元群であり、中国剰余定理（Chinese remainder theorem）により、3 を法とする単元群と 7 を法とする単元群の直積、すなわち $C_2 \times C_6$ と同型である。これが、位数 2 の元が三つあり、位数 12 の元が存在しない理由である。N を法とする単元群がどのようなときに巡回群になるかを正確に決定すること（答えはちょうど $N = 2, 4, p^k, 2p^k$ の場合であり、ここで p は奇素数である。これは「原始根（primitive root）」が存在する場合にあたる）は、大学一年次の整数論の古典的な結果である。Davenport の *The Higher Arithmetic* は原始根を扱っており、Allenby の *Rings, Fields and Groups* は群論を扱っている。

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。