풀이

# STEP II 견본 문제지, 문제 8

순수수학 • 모듈러 군에서의 위수

> **STEP II 견본 문제지, 8번 문제**
>
> 더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:
>
> step.maths.org/questions/spec-s2-q8

## 핵심 아이디어

$N$을 법(modulo)으로 하면 수 $N-1$은 그냥 $-1$이고, $m+n=N$은 $n \equiv -m$이라는 뜻이다. 따라서 $n$의 모든 거듭제곱은 부호를 제외하면 $m$의 거듭제곱이다: $n^k \equiv (-1)^k m^k$. $k$가 짝수인지 홀수인지에 따라 그 부호가 의미를 갖는지가 결정되고, 세 소문항은 위수(order)의 홀짝성이 결합할 수 있는 세 가지 경우에 해당한다. 마지막 소문항에서는 이 사실들을 이용해 모든 거듭제곱을 계산하지 않고도 위수를 구한다.

## 풀이

이 풀이 전체에서 $\equiv$는 $N$을 법으로 하는 합동(congruent)을 뜻한다. 문제의 의도대로 $G$의 항등원(identity)은 1로 본다. (사실 $N-1 \in G$이면 이는 저절로 성립한다: $e$가 항등원이면 $e(N-1) \equiv N-1$, 즉 $-e \equiv -1$이므로 $e=1$이다.)

### $N-1$의 위수

다음이 성립한다.

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

또 $N \geq 3$이므로 $N-1 \neq 1$이다. 따라서 $(N-1)^1$은 항등원이 아니지만 $(N-1)^2$은 항등원이다. 즉 $N-1$의 위수는 2이다.

### 소문항 준비

$m+n=N$이므로 $n \equiv -m$이고, 따라서 모든 양의 정수 $k$에 대하여

$$n^k \equiv (-1)^k m^k, \qquad \text{동치로} \qquad m^k \equiv (-1)^k n^k.$$

이다. 또 $G$는 $n$과 $m^{-1}$을 포함하는 군(group)이므로 $N-1 \equiv -1 \equiv n\,m^{-1}$은 $G$에 속한다. 따라서 $-1$은 $G$의 원소이고, $N \geq 3$이므로 $-1 \neq 1$이다. 또한 $x$의 위수가 $r$이고 $x^k = 1$이면 $r \mid k$라는 잘 알려진 사실을 이용한다($0 \leq b < r$인 $b$로 $k = ar + b$라 쓰면 $x^b = 1$이므로, $r$의 최소성에 의해 $b = 0$이다).

**소문항 (i)**

$p$와 $q$가 모두 짝수라 하자. 그러면

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

이므로 $q \mid p$이다. 같은 방법으로 $m^q \equiv (-1)^q n^q = n^q \equiv 1$이므로 $p \mid q$이다. 서로를 나누는 두 양의 정수는 같으므로 $p = q$이다.

**소문항 (ii)**

$p$가 짝수이고 $q$가 홀수라 하자. $p$가 짝수이므로 $n^p \equiv m^p \equiv 1$이고, 따라서 $q \mid p$이다. 또 $2q$는 짝수이므로

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

이고, 이로부터 $p \mid 2q$를 얻는다. $p = kq$라 쓰면 $kq \mid 2q$이므로 $k \mid 2$이고 $k = 1$ 또는 $2$이다. 그런데 $k = 1$이면 $p = q$가 홀수가 되는데, 그렇지 않다. 따라서 $k = 2$이고 $p = 2q$이다.

> ? **생각해 보기** 왜 단순히 $m^q \equiv -n^q \equiv -1$이므로 "$p$는 $2q$이어야 한다"고 논증할 수 없는가?

그 계산은 옳고 $m^q \neq 1$이면서 $m^{2q} \equiv 1$임을 보여 주지만, 그것만으로는 $p \mid 2q$이고 $p \nmid q$라는 것만 알 수 있을 뿐 $p$가 정확히 결정되지는 않는다(예를 들어 선험적으로는 $q = 3$일 때 $p$가 2일 수도 있다). 이 틈을 메우는 것은 $p$가 짝수라는 데서 나오는 추가적인 나누어떨어짐 $q \mid p$이다.

**소문항 (iii)**

모순을 이끌어 내기 위해 $p$와 $q$가 모두 홀수라고 가정하고, $r = pq$라 하자. $r$은 홀수이다. 그러면

$$n^r = (n^q)^p \equiv 1, \qquad \text{이지만 또한} \qquad n^r \equiv (-1)^r m^r = -(m^p)^q \equiv -1.$$

이다. 따라서 $1 \equiv -1$, 즉 $N \mid 2$인데, $N \geq 3$이므로 이는 불가능하다. 따라서 $p$와 $q$가 모두 홀수일 수는 없다.

(대칭성에 의해, 소문항 (ii)로부터 $q$가 짝수이고 $p$가 홀수이면 $q = 2p$임도 얻는다. 따라서 어느 경우에나 $m$과 $N - m$의 위수는 서로 같은 짝수이거나, 한쪽이 홀수인 다른 쪽의 두 배이다.)

### 21을 법으로 하는 군

2와 5의 거듭제곱을 차례로 21을 법으로 줄이면 다음과 같다.

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

(예를 들어 $2^5 = 32 \equiv 11$, $5^2 = 25 \equiv 4$, $5^4 \equiv 4^2 = 16$, $5^5 \equiv 80 \equiv 17$). 두 행 모두에서 처음으로 1이 나타나는 것은 $k = 6$일 때이므로, 2와 5의 위수는 모두 6이다.

이제 표에서 위수를 읽어 낸다. $x$의 위수가 6이면 $x^k$의 위수는 $6/\gcd(k,6)$이다. 따라서

- $11 = 2^5$와 $17 = 5^5$의 위수는 6이다.
- $4 = 2^2$와 $16 = 2^4$의 위수는 3이다.
- $8 = 2^3$과 $20 = 5^3$의 위수는 2이다($20 = N - 1$이므로 이는 첫 번째 소문항에서 이미 알고 있다).
- 1의 위수는 1이다.

남은 것은 10, 13, 19이고, 이들은 각각 이미 아는 원소와 짝을 지어 합이 21이 된다.

- $13 = 21 - 8$이고, 8의 위수는 짝수 2이다. (iii)과 그 뒤의 설명에 의해 13의 위수는 2(같은 짝수)이거나 1(2의 절반)이다. $13 \neq 1$이므로 위수는 1이 아니고, 따라서 13의 위수는 2이다. (확인: $13^2 = 169 = 8 \cdot 21 + 1$.)
- $19 = 21 - 2$이고 $10 = 21 - 11$이며, 2와 11의 위수는 6이다. 따라서 19와 10의 위수는 각각 6 또는 3이다.

그러므로 $G$의 모든 원소의 위수는 6 이하이다. 위수가 12인 순환군(cyclic group)에는 생성원(generator), 즉 위수가 12인 원소가 있고, 동형사상(isomorphism)은 원소의 위수를 보존한다. $G$에는 위수가 12인 원소가 없으므로, $G$는 위수가 12인 순환군과 동형이 아니다.

마무리하는 두 번째 방법도 있다. $G$에는 위수가 2인 원소가 8, 13, 20의 세 개 있지만, 위수가 12인 순환군에는 정확히 하나만 있다($g$가 생성원이면 $g^k$의 위수가 2인 것은 $k = 6$일 때뿐이다).

## 검산

컴퓨터로 확인하면 $G$의 위수 전체 목록은 다음과 같다: 1의 위수는 1이고, 8, 13, 20의 위수는 2, 4, 16의 위수는 3, 2, 5, 10, 11, 17, 19의 위수는 6이다. (직접 계산하면 $10^3 = 1000 \equiv 13$이고 $19^3 \equiv (-2)^3 = -8 \equiv 13$이므로, 둘 다 위수가 3이 아니다.) 개수의 합 $1 + 3 + 2 + 6 = 12$는 $G$의 크기와 일치한다. 또한 소문항 (i)–(iii)을 $N < 60$인 모든 $N$에 대하여, 최대 두 원소로

생성되는 단원군(group of units)의 모든 부분군에서 모든 쌍 $m$, $N-m$에 대해 검사했다. 거의 1900개의 쌍에서 예외는 없었다.

## 흔한 실수

- 이유를 밝히지 않고 $N-1 \in G$라고 가정하는 것. 이는 주어진 조건이 아니지만, $N-1 \equiv n\,m^{-1}$이므로 $m, n \in G$로부터 따라 나온다.
- (ii)에서 $p \mid 2q$만 증명하는 것. 등식을 얻으려면 나누어떨어짐 하나가 더 필요하다.
- 특이한 경우에 항등원을 당연하게 여기는 것. 예를 들어 6을 법으로 하는 부분집합 $\{3\}$은 곱셈에 대해 닫혀 있고 항등원은 3이며, $m = n = 3$이면 (iii)에 어긋난다. 논증은 항등원이 1이라는 데 의존하고, 문제의 의도도 분명히 그렇다.

## STEP 너머

$G$는 21을 법으로 하는 단원군이고, 중국인의 나머지 정리(Chinese remainder theorem)에 의해 3을 법으로 하는 단원군과 7을 법으로 하는 단원군의 곱, 즉 $C_2 \times C_6$과 동형이다. 이것이 $G$에 위수가 2인 원소가 세 개 있고 위수가 12인 원소는 없는 이유이다. $N$을 법으로 하는 단원들이 정확히 언제 순환군을 이루는지 결정하는 것(정확히 $p$가 홀수인 소수일 때 $N = 2, 4, p^k, 2p^k$인 경우, 즉 "원시근(primitive root)"이 존재하는 경우)은 대학 1학년 정수론의 고전적인 결과이다. Davenport의 *The Higher Arithmetic*(고등 산술)은 원시근을 다루고, Allenby의 *Rings, Fields and Groups*(환, 체, 군)는 군론을 다룬다.

Beyond STEP 풀이: https://beyondstep.keithmcnulty.org/ko/. 풀이 글은 CC0 1.0이다. 문제 자체의 저작권은 © Cambridge University Press & Assessment에 있으며 여기에 싣지 않는다. 영어 원문을 기계 번역하였으며 아직 검토되지 않았다.