풀이

STEP III 1987, 문제 1

순수수학 • 계승의 나누어떨어짐

> **STEP III 1987, 1번 문제**
>
> 더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:
>
> step.maths.org/questions/87-s3-q1

핵심 아이디어

계승(factorial) $(n-1)! = 1 \times 2 \times \cdots \times (n-1)$에는 n보다 작은 모든 자연수가 들어 있다. n을 n보다 작은 서로 **다른** 두 수의 곱으로 나타낼 수 있다면, 두 수가 모두 이 계승에 나타나므로 n은 계승을 나눈다. 따라서 이 문제는 사실 어떤 n이 그렇게 쪼개질 수 **없는가**에 관한 것이다. 소수(prime)는 분명히 쪼개질 수 없고, 소수의 제곱은 좀 더 자세히 살펴보아야 한다. 처음 열두 개 정도의 값을 손으로 확인해 보면 답이 곧바로 보인다.

풀이

먼저 실험하기

간단한 표를 만들어 볼 만하다.

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

나누지 못하는 경우는 $2, 3, 4, 5, 7$이다. 즉 지금까지 나온 소수들과 4이다. 이제 이 규칙이 계속 성립함을 증명한다.

주장. n이 $(n-1)!$을 나누지 않을 필요충분조건은 n이 소수이거나 $n = 4$인 것이다.

$n = 1$

이때 $(n-1)! = 0! = 1$이고, 1은 1을 나눈다. 따라서 $n = 1$은 구하는 집합에 속하지 **않는다**.

$n = p$ prime

$(p-1)!$의 각 인수 $1, 2, \ldots, p-1$은 p보다 작은 양수이므로, 어느 것도 p로 나누어떨어지지 않는다. p는 소수이므로, p가 곱을 나눈다면 인수 중 하나를 나누어야 한다(유클리드(Euclid)의 보조정리(Euclid's lemma)). 따라서 $p \nmid (p-1)!$이고, 모든 소수는 구하는 집합에 속한다.

n이 합성수(composite)인 경우

n의 가장 작은 소인수를 p라 하고 $n = pm$으로 쓰자. n이 합성수이므로 $m > 1$이고, m의 모든 소인수는 p 이상이므로 $m \geq p$이다. 두 가지 경우가 있다.

경우 1: $m > p$. 이때 $1 < p < m < n$이므로 p와 m은 목록 $1, 2, \ldots, n-1$에 있는 서로 다른 두 수이다. 따라서 그 곱 $pm = n$은 $(n-1)!$을 나눈다.

경우 2: $m = p$, **즉** $n = p^2$.

> **생각해 보기** 경우 1의 논증이 여기서는 왜 통하지 않는가? 그리고 무엇으로 대신할 수 있는가?

인수 p는 목록 $1, \ldots, n-1$에 한 번만 나타나므로 두 번 쓸 수 없다. 대신 p와 $2p$를 쓴다. $p \geq 3$이면

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

이므로 p와 $2p$는 목록 $1, 2, \ldots, n-1$에 있는 서로 다른 두 수이다. 따라서 그 곱 $2p^2 = 2n$은 $(n-1)!$을 나누고, n 역시 마찬가지이다.

$p = 2$이면 이 논증은 통하지 않는다. $2p = 4 = n$이 목록에 없기 때문이다. 실제로 $n = 4$이면 $3! = 6$이고 $4 \nmid 6$이다. 따라서 4는 구하는 집합에 속한다.

결론

4가 아닌 모든 합성수 n은 $(n-1)!$을 나누고, $n = 1$도 마찬가지이다. 그러므로 구하는 집합은

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

이다.

검산

위의 표는 $n \leq 8$에 대하여 주장과 일치한다. 소수의 제곱도 확인해 보자. $n = 9$이면 $8! = 40320 = 9 \times 4480$이고, 이는 경우 2에서 예측한 대로이다(인수 3과 6을 이용). $n \leq 2000$인 모든 경우에 대해 $(n-1)! \bmod n$을 직접 계산하는 컴퓨터 검사를 해 보아도 주장에 어긋나는 예외는 없다.

흔한 실수

- $a \neq b$라는 조건을 고집하지 않고 "$a, b < n$이 되도록 $n = ab$로 쓰면 $ab \mid (n-1)!$"이라고 논증하는 것. 이 논증은 $4 \mid 3!$을 잘못 "증명"한다.
- $n = 1$을 빠뜨리는 것. $0! = 1$이므로 이것은 구하는 집합에 속하지 않는다.
- 소수 p가 $(p-1)!$을 나누지 못하는 이유를 "p가 인수 중 하나가 아니기 때문"이라고 말하는 것. 진짜 이유는 p가 소수이고 어떤 인수도 나누지 않는다는 것이다. 합성수는 곱의 인수 중 하나가 아니면서도 그 곱을 나눌 수 있다.

STEP 너머

소수에 대해서는 윌슨의 정리(Wilson's theorem)라고 불리는 더 날카로운 사실이 있다. 즉 $(p-1)! \equiv -1 \pmod{p}$이다. 이 문제와 함께 생각하면 (매우 느린) 소수 판정법(primality test)을 얻는다. $n > 1$이 소수일 필요충분조건은 $(n-1)! \equiv -1 \pmod{n}$이다. 윌슨의 정리는 각 수를 법 p에 대한 역원(inverse)과 짝지어 증명하는데, 이는 법 p에 대한 정수들이 이루는 군(group) 구조를 처음 맛보는 경험이다. Davenport의 *The Higher Arithmetic*(고등 산술)이 이 내용을 훌륭하게 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.