풀이

STEP III 2016, 문제 5

순수수학 • 소수의 곱

> **STEP III 2016, 5번 문제**
>
> 더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:
>
> step.maths.org/questions/16-s3-q5

이 문제는 *Beyond STEP*의 1.2 절 소수는 얼마나 드문드문 흩어져 있는가?에서 단계별 안내와 함께 자세히 다룬다: https://beyondstep.keithmcnulty.org/ko/ch01/prime-distribution.html

핵심 아이디어

가운데 이항계수(binomial coefficient) $\binom{2m+1}{m}$은 작다(이 수와 그 쌍둥이 $\binom{2m+1}{m+1}$이 다른 항들과 함께 합계 2^{2m+1}을 나누어 가진다). 그런데도 이 수는 $m+1$과 $2m+1$ 사이의 모든 소수(prime)로 나누어떨어진다. 따라서 그 소수들의 곱도 작다. $2m+1$ 이하의 소수를 "$m+1$ 이하"와 "$m+1$ 초과"로 나누면 강한 귀납법(strong induction)을 세울 수 있다. 짝수는 (2를 제외하면) 결코 소수가 아니므로 아무 부담도 되지 않는다.

풀이

소문항 (i)

$(1+x)^{2m+1}$의 이항전개(binomial expansion)에 $x=1$을 대입하면

$$\sum_{k=0}^{2m+1}\binom{2m+1}{k}=2^{2m+1}.$$

좌변의 모든 항은 양수이다. 대칭성에 의해 $\binom{2m+1}{m}=\binom{2m+1}{m+1}$이고, 이 둘은 합에서 서로 다른 두 항이다. $m\geq 1$이므로 항 $\binom{2m+1}{0}=1$은 이들과 다른 세 번째 항이다. 따라서

$$2\binom{2m+1}{m}=\binom{2m+1}{m}+\binom{2m+1}{m+1}<2^{2m+1},$$

이므로 요구한 대로 $\binom{2m+1}{m}<2^{2m}$이다.

소문항 (ii)

다음과 같이 쓴다.

$$\binom{2m+1}{m} = \frac{(2m+1)!}{m!\,(m+1)!}, \qquad \text{따라서} \qquad m!\,(m+1)!\binom{2m+1}{m} = (2m+1)!.$$

p를 $m+1 < p \le 2m+1$인 소수라 하자. 그러면 p는 $(2m+1)!$의 인수 중 하나이므로 p는 우변을 나눈다. 그런데 $m!\,(m+1)!$의 모든 인수는 $m+1 < p$ 이하이므로 소수 p는 그 어느 것도 나누지 못하고, 따라서 $p \nmid m!\,(m+1)!$이다. 곱 ab를 나누는 소수는 a나 b를 나누어야 하므로 $p \mid \binom{2m+1}{m}$이다.

> **생각해 보기** 이러한 소수 각각이 이 계수를 나눈다. 그렇다면 왜 그들의 곱도 이 계수를 나누는가?

이 소수들은 서로 다르므로 쌍마다 서로소(coprime)이고, 쌍마다 서로소인 수들로 각각 나누어떨어지는 수는 그들의 곱으로도 나누어떨어진다. (같은 말로, 소인수분해의 유일성(unique factorisation)에 의해 이 소수들은 각각 $\binom{2m+1}{m}$의 소인수분해에 나타난다.) 따라서 $P_{m+1,2m+1}$은 $\binom{2m+1}{m}$을 나눈다. 그러한 소수가 없으면 $P_{m+1,2m+1} = 1$이고, 이는 모든 수를 나눈다.

양의 정수의 양의 약수는 그 수보다 크지 않으므로, 소문항 (i)에 의해

$$P_{m+1,2m+1} \le \binom{2m+1}{m} < 2^{2m}.$$

소문항 (iii)

$m \ge 1$이므로 $1 < m+1 < 2m+1$이다. $p \le 2m+1$인 모든 소수는 $p \le m+1$ 또는 $m+1 < p \le 2m+1$ 중 정확히 하나를 만족하므로

$$P_{1,2m+1} = P_{1,m+1}\,P_{m+1,2m+1}.$$

또한 ($m \ge 1$이므로) $2 \le m+1 \le 2m$이어서 $k = m+1$은 가정이 적용되는 값 중 하나이고, 따라서 $P_{1,m+1} < 4^{m+1}$이다. 소문항 (ii)와 합치면

$$P_{1,2m+1} < 4^{m+1} \cdot 2^{2m} = 4^{m+1} \cdot 4^m = 4^{2m+1}.$$

소문항 (iv)

n에 대한 강한 귀납법을 쓴다. $S(n)$을 명제 $P_{1,n} < 4^n$이라 하자.

기저 단계(*base case*). $P_{1,2} = 2 < 16 = 4^2$.

귀납 단계(*inductive step*). $n \ge 3$이라 하고, $k = 2, 3, \ldots, n-1$에 대해 $S(k)$가 성립한다고 가정하자.

- n이 홀수이면 $m \geq 1$인 m으로 $n = 2m+1$이라 쓴다. 그러면 $n-1 = 2m$이므로 $k = 2, \ldots, 2m$에 대해 $S(k)$가 성립한다. 소문항 (iii)에 의해 $P_{1,2m+1} < 4^{2m+1}$이고, 이것이 곧 $S(n)$이다.
- n이 짝수이면 $n \geq 4$는 2보다 큰 짝수이므로 소수가 아니다. 따라서 n 이하의 소수는 정확히 $n-1$ 이하의 소수이고,

$$P_{1,n} = P_{1,n-1} < 4^{n-1} < 4^n.$$

? **생각해 보기** 왜 모든 n에 대해 그냥 소문항 (iii)을 쓸 수 없는가?

소문항 (iii)은 홀수 $2m+1$에만 적용된다. 짝수 n에 대해서는 별도의 논증이 필요한데, 위의 논증은 쉽다. 2보다 큰 짝수는 곱에 새로운 소수를 더하지 않기 때문이다.

따라서 두 경우 모두 $S(n)$이 성립하고, 강한 귀납법에 의해 모든 $n \geq 2$에 대해 $P_{1,n} < 4^n$이다.

검산

- $m = 3$: $\binom{7}{3} = 35 < 64 = 2^6$. $(4, 7]$에 있는 소수는 5와 7이고, $P_{4,7} = 35$는 35를 정확히 나눈다.
- $m = 5$: $\binom{11}{5} = 462 = 2 \cdot 3 \cdot 7 \cdot 11$이고, 이는 $P_{6,11} = 77$로 나누어떨어진다. 또한 $462 < 1024$이다.
- $P_{1,10} = 2 \cdot 3 \cdot 5 \cdot 7 = 210$으로, $4^{10} = 1\,048\,576$보다 훨씬 작다. 컴퓨터로 확인하면 2부터 1500까지의 모든 n에 대해 $P_{1,n} < 4^n$이 성립한다.

흔한 실수

- 소문항 (i)에서 $<$ 대신 $\leq$로 쓰는 것: 엄격한 부등호를 얻으려면 가운데 두 항 외에 $\binom{2m+1}{0}$과 같은 세 번째 양의 항이 필요하다.
- 소문항 (iii)에서 $m+1$이 가정이 적용되는 범위 $2, \ldots, 2m$에 속하는지 확인하는 것을 잊는 것.
- 소문항 (iv)에서 홀수 n만 다루거나, 기저 단계 $n = 2$를 잊는 것.

STEP 너머

이것은 부등식 $\prod_{p \leq n} p < 4^n$에 대한 에르되시(Erdős)의 초등적 증명이다. 로그를 취하면, 이는 체비쇼프(Chebyshev) 함수 $\theta(n) = \sum_{p \leq n} \ln p$가 $n \ln 4$보다 작다는 뜻이다. 이는 n 이

하의 소수의 개수가 $n/\ln n$ 정도의 크기라는 체비쇼프 정리의 절반에 해당한다. 에르되시는 같은 종류의 이항계수 논증으로 베르트랑 공준(Bertrand's postulate), 즉 n과 $2n$ 사이에는 언제나 소수가 존재한다는 사실을 증명하였다. Davenport의 *The Higher Arithmetic*(고등 산술)은 초등 정수론을 더 공부하기 위한 좋은 다음 단계이다.

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.