1.2 소수는 얼마나 드문드문 흩어져 있는가?

학습지

문제

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

힌트

먼저 혼자 힘으로 문제를 풀어 보자. 막히면 힌트를 **하나씩** 읽고, 힌트를 하나 읽을 때마다 다시 문제로 돌아가자. **잠깐, 직접 해 보기**라고 표시된 힌트가 핵심 단계이다. 각 힌트 뒤에는 풀이를 적을 공간이 있다.

생각해 보기 문항 (iv)는 **모든** $n \geq 2$에 대하여 어떤 명제를 증명하라고 한다. 문항 (iii)은 $2m$ 이하의 모든 k에 대하여 그 명제가 성립한다고 가정한다. 이것은 어떤 종류의 귀납법(induction)인가?

1단계 이항계수는 너무 크지 않다

다루는 내용: 소문항 (i)

생각해 보기 2^{2m+1}은 어디에서 나오는가? $(1+x)^{2m+1}$의 이항전개(binomial expansion)에 $x=1$을 대입해 본다.

생각해 보기 그 합의 항은 모두 양수이다. 그 가운데 $\binom{2m+1}{m}$과 같은 두 항은 무엇인가?

잠깐, 직접 해 보기 $\binom{2m+1}{m}$의 두 배는 전체 합보다 크지 않은데, 필요한 것은 엄격한 부등식(strict inequality)이다. 아직 쓰지 않은 항이 있는가?

2단계 그 이항계수를 나누는 소수는 무엇인가?

다루는 내용: 소문항 (ii)

생각해 보기 $\binom{2m+1}{m}$을 계승(factorial)으로 나타내고, 분수가 없어지도록 양변에 곱한다.

생각해 보기 $m+1 < p \le 2m+1$인 소수(prime) p를 잡는다. p는 $(2m+1)!$을 나누는가? 인수가 모두 $m+1$ 이하인 $m!\,(m+1)!$을 p가 나눌 수 있는가?

잠깐, 직접 해 보기 따라서 그러한 소수는 각각 $\binom{2m+1}{m}$을 나눈다. 그 소수들의 곱도 이것을 나누는 이유는 무엇이며, 소문항 (i)로 이 소문항을 어떻게 마무리하는가?

3단계 곱 나누기

다루는 내용: 소문항 (iii)

생각해 보기 $2m+1$ 이하의 소수를 $m+1$ 이하인 것과 $m+1$보다 큰 것으로 나눈다. 그러면 $P_{1,2m+1}$은 어떻게 되는가?

잠깐, 직접 해 보기 한 인수에는 이 소문항의 가정을, 다른 인수에는 소문항 (ii)를 쓴다. 두 상계를 모두 4의 거듭제곱으로 나타낸다.

4단계 모든 n

다루는 내용: 소문항 (iv)

생각해 보기 n에 대한 강한 귀납법(strong induction)을 쓴다. 소문항 (iii)은 n이 어떤 값일 때를 다루는가?

잠깐, 직접 해 보기 나머지 n의 값에 대해서는: 2보다 큰 짝수가 소수일 수 있는가? 이것으로 $P_{1,n}$과 $P_{1,n-1}$을 비교하면 무엇을 알 수 있는가?

숨은 수학

4^n에서 소수 정리까지

결과에 로그(logarithm)를 취하면 $\ln P_{1,n} < n \ln 4$, 곧

$$\sum_{p \le n} \ln p < (\ln 4)\, n \approx 1.39\, n.$$

1850년대에 체비쇼프(Pafnuty Chebyshev)는 바로 이런 종류의 상계와 **하계**를 증명하여, $\sum_{p \le n} \ln p$가 n에 비례하여 증가함을 보였다. 가우스(Gauss)는 약 15세 무렵 이미 표를 보고 n 이하의 소수의 개수가 대략 $n / \ln n$이라고 추측했다. 이것이 **소수 정리**(Prime

Number Theorem)가 되었으며, 1896년 아다마르(Jacques Hadamard)와 드 라 발레 푸생(Charles de la Vallée Poussin)이 복소해석학(complex analysis)을 이용하여 마침내 증명하였다. 로그 형태로 쓰면 소수 정리는

$$\sum_{p \le n} \ln p \sim n,$$

을 말하며, 따라서 n 이하의 소수의 곱은 대략 e^n이다. 우리가 얻은 상계 4^n은 전혀 동떨어진 값이 아니다. 그림 1.2.1에 세 가지를 모두 나타내었다.

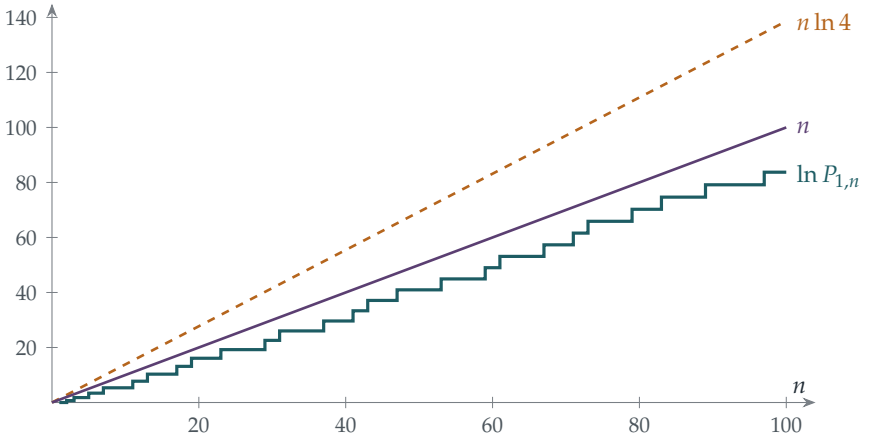

그림 1.2.1 n 이하의 모든 소수의 곱의 로그(청록색). 각 소수 p에서 $\ln p$만큼 뛰어오른다. 이 절에서는 이 값이 $n \ln 4$(호박색, 점선) 아래에 머문다는 것을 증명한다. 소수 정리에 따르면 이 값은 n(자주색)처럼 증가한다.

베르트랑 공준

1845년 베르트랑(Joseph Bertrand)은 모든 $n \ge 1$에 대하여 n과 $2n$ 사이에 항상 소수가 존재한다고 추측했다. 체비쇼프는 1852년에 이를 증명했다. 80년 뒤, 약관 19세의 에르되시가 아름다운 초등적 증명을 찾아냈다. 그 핵심 재료는 이 문제의 보조정리와, **가운데** 이항계수 $\binom{2n}{n}$을 나누는 소수가 무엇인지에 대한 세심한 분석이다. Martin Aigner와 Günter Ziegler는 수학에서 가장 우아한 증명들을 모은 책 *Proofs from THE BOOK*의 제2장으로 이 증명을 골랐다.

이 다음은

소수의 정확한 분포는 리만 제타 함수(Riemann zeta function)

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots,$$

의 영점에 의해 결정된다. 이 함수는 Section 2.4에서 훨씬 소박한 모습으로 만나게 되는데, 거기서 $\zeta(2) = \pi^2/6$이다. 그 영점들이 정확히 어디에 있는지 예측하는 **리만 가설**(Riemann Hypothesis)이 참이라면, 소수 정리의 오차를 가능한 한 가장 정밀하게 잡아낼 수 있다. 리만 가설은 아마도 수학에서 가장 유명한 미해결 문제이며, 밀레니엄 문제(Millennium Prize Problems) 가운데 하나이다.

더 도전하기

1 **수를 느껴 보기.** $n = 10, 20, 30$에 대하여 $P_{1,n}$을 계산하고, 4^n 및 e^n과 비교하여라. (여기서는 계산기를 써도 좋다.)

2 **가운데 이항계수.** $\binom{2m}{m}$이 $(1+1)^{2m}$의 전개에 나오는 $2m+1$개의 항 가운데 가장 큼을 보이고, 이로부터 $\binom{2m}{m} \geq \dfrac{4^m}{2m+1}$임을 유도하여라.

3 **소수는 너무 많지 않다.** $\pi(n)$을 n 이하의 소수의 개수라 하자. $\sqrt{n}$과 n 사이의 모든 소수는 $\sqrt{n}$보다 크고, 그들의 곱은 많아야 $P_{1,n} < 4^n$이다. 이로부터

$$\pi(n) - \pi(\sqrt{n}) < \frac{2\ln 4}{\ln n}\, n,$$

임을 유도하고, 따라서 $\pi(n) < 2.8\, n/\ln n + \sqrt{n}$임을 보여라. 이를 소수 정리의 $\pi(n) \approx n/\ln n$과 비교하여라.

4 **베르트랑 확인하기.** $n = 1, 2, \ldots, 50$ 각각에 대하여 n과 $2n$ 사이의 소수를 찾아 베르트랑 공준(Bertrand's postulate)을 확인하여라. 각 소수가 바로 앞 소수의 두 배보다 작은 짧은 소수 목록을 이용하여 효율적으로 할 수 있는가?

더 읽을거리

- **Aigner & Ziegler, *Proofs from THE BOOK***, 제2장, "Bertrand's postulate"(베르트랑 공준).
- **Marcus du Sautoy, *The Music of the Primes*** (Fourth Estate). 소수 정리와 리만 가설의 역사를 다룬 대중서이다.
- **G. J. O. Jameson, *The Prime Number Theorem*** (Cambridge University Press). 엄밀하면서도 친절하며 학부생을 위해 쓰였다. 앞쪽 장들은 A 레벨(A level, 영국의 대학 입학 자격 시험) 수준의 미적분만 있으면 읽을 수 있다.

안내에 따른 전체 풀이는 제 1.2절에 있다:

https://beyondstep.keithmcnulty.org/ko/ch01/prime-distribution.html

매주 STEP 문제 하나를 끝까지 풀어 본다. The STEP Up은 이메일로 무료로 받아 볼 수 있다: keithmcnulty.substack.com