풀이

STEP II 2002, 문제 3

순수수학 • 페르마 수와 소수

> **STEP II 2002, 3번 문제**
>
> 더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:
>
> step.maths.org/questions/02-s2-q3

이 문제는 *Beyond STEP*의 1.1 절 **소수 공장**에서 단계별 안내와 함께 자세히 다룬다: https://beyondstep.keithmcnulty.org/ko/ch01/fermat-numbers.html

핵심 아이디어

$F_k - 2 = 2^{2^k} - 1$로 쓴다. 이것에 $F_k = 2^{2^k} + 1$을 곱하면 제곱의 차(difference of two squares)가 되는데, 바로 이것이 귀납법(induction)에 필요한 단계이다. 곱셈 공식이 성립하고 나면, 두 페르마 수(Fermat number)의 공약수는 모두 2의 약수여야 한다. 모든 페르마 수는 홀수이므로 그 공약수는 1일 수밖에 없다.

풀이

처음 네 개의 페르마 수

$2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8$이므로

$$F_0 = 2^1 + 1 = 3, \qquad F_1 = 2^2 + 1 = 5, \qquad F_2 = 2^4 + 1 = 17, \qquad F_3 = 2^8 + 1 = 257.$$

이제 k의 처음 세 값에 대하여 $(*)$을 확인한다.

$$\begin{aligned} k = 1: &\quad F_0 = 3 = 5 - 2 = F_1 - 2, \\ k = 2: &\quad F_0 F_1 = 15 = 17 - 2 = F_2 - 2, \\ k = 3: &\quad F_0 F_1 F_2 = 15 \times 17 = 255 = 257 - 2 = F_3 - 2. \end{aligned}$$

모든 $k \geq 1$에 대한 $(*)$의 증명

k에 대한 귀납법을 쓴다. $k = 1$인 경우는 위에서 확인하였다.

어떤 $k \geq 1$에 대하여 $(*)$이 성립한다고 가정하자. 즉 $F_0 F_1 \cdots F_{k-1} = F_k - 2$이다. 그러면

$$\begin{aligned} F_0 F_1 \cdots F_{k-1} F_k &= (F_k - 2)\, F_k \\ &= \left(2^{2^k} - 1\right)\left(2^{2^k} + 1\right) \\ &= \left(2^{2^k}\right)^2 - 1 \\ &= 2^{2 \cdot 2^k} - 1 = 2^{2^{k+1}} - 1 \\ &= F_{k+1} - 2. \end{aligned}$$

따라서 $(*)$은 $k+1$에 대해서도 성립하고, 귀납법에 의하여 모든 $k \geq 1$에 대하여 성립한다.

? **생각해 보기** $\left(2^{2^k}\right)^2$이 $2^{2^{2k}}$나 다른 무엇이 아니라 $2^{2^{k+1}}$과 같은 이유는 무엇인가?

거듭제곱을 제곱하면 지수(exponent)가 두 배가 된다. 즉 $\left(2^a\right)^2 = 2^{2a}$이다. 여기서 $a = 2^k$이고 $2a = 2 \cdot 2^k = 2^{k+1}$이다. 귀납 단계에서 하는 일의 대부분은 이처럼 지수가 겹겹이 쌓인 식을 조심스럽게 다루는 것이다.

어떤 두 페르마 수도 공약수를 갖지 않는다

서로 다른 두 페르마 수 F_m과 F_n을 잡고 $m < n$이라 하자. 그러면 $n \geq 1$이고, F_m은 $k = n$일 때 $(*)$의 인수 $F_0, \ldots, F_{n-1}$ 중 하나이다. 따라서

$$F_n - 2 = F_m \times (\text{정수}),$$

즉 F_m은 $F_n - 2$를 나눈다.

이제 양의 정수 d가 F_m과 F_n을 모두 나눈다고 가정하자. $d \mid F_m$이고 $F_m \mid F_n - 2$이므로 $d \mid F_n - 2$이다. d는 F_n도 나누므로 그 차도 나눈다.

$$d \mid F_n - (F_n - 2) = 2,$$

따라서 $d = 1$ 또는 $d = 2$이다. 그런데 $F_m = 2^{2^m} + 1$은 짝수에 1을 더한 수이므로 홀수이다($2^m \geq 1$임에 주의한다). 그러므로 $d \neq 2$이고, 따라서 $d = 1$이다. 결국 어떤 두 페르마 수도 1보다 큰 공약수를 갖지 않는다.

무한히 많은 소수

각 F_n은 3 이상이므로 적어도 하나의 소인수(prime factor)를 갖는다. 그중 하나를 골라 p_n이라 하자. 그러면 각 $n = 0, 1, 2, \ldots$에 대하여 소수가 하나씩 생긴다.

생각해 보기 서로 다른 두 페르마 수가 같은 소수를 줄 수도 있지 않을까?

그렇지 않다. $m \neq n$인데 $p_m = p_n$이라면, 그 소수는 F_m과 F_n을 모두 나눈다. 그러면 그것은 1보다 큰 공약수가 되는데, 이는 앞 부분에서 배제하였다. 따라서 소수 $p_0, p_1, p_2, \ldots$은 모두 다르다. 페르마 수는 무한히 많으므로 서로 다른 소수도 무한히 많다.

F_n 자체가 소수일 필요는 전혀 없었다는 점에 주목하자. 필요한 것은 각 페르마 수가 다른 어떤 페르마 수와도 공유하지 않는 **어떤** 소인수를 갖는다는 사실뿐이다.

검산

- $k = 4$일 때의 $(*)$: $255 \times 257 = 65535 = 65537 - 2 = F_4 - 2$. 또한 12 이하의 모든 k에 대하여 컴퓨터로 $(*)$을 정확히 확인하였다.
- $F_0, \ldots, F_5$의 가장 작은 소인수는 $3, 5, 17, 257, 65537, 641$로, 논증이 예측한 대로 모두 다르다. $F_5 = 4294967297 = 641 \times 6700417$은 소수가 아닌 최초의 페르마 수이다.
- $0 \leq m < n \leq 10$인 모든 경우에 $\gcd(F_m, F_n) = 1$임을 수치적으로 확인하였다.

흔한 실수

- 2^{2^n}을 $(2^2)^n = 4^n$으로 읽는 것. 지수는 2^n이므로 $F_3 = 2^8 + 1$이지 $4^3 + 1$이 아니다.
- $d \mid 2$를 얻은 뒤 $d = 2$를 배제하는 것을 잊는 것. 논증을 마무리하는 것은 페르마 수가 홀수라는 사실이다.
- 모든 페르마 수가 소수라고 가정하는 것. 마지막 부분은 이 가정 없이도 성립하며, 어차피 이 가정은 거짓이다$(641 \mid F_5)$.

STEP 너머

이 증명은 폴리아(Pólya)가 제시한 것이다. 이는 소수가 무한히 많음을 보이는 증명들의 한 갈래에 속한다. 이 증명들은 모두 쌍마다 서로소(pairwise coprime)인 정수들의 무한수열을 만들고, 그러면 각 항이 저마다 새로운 소수를 하나씩 내놓는다. 유클리드(Euclid)의 증명도 같은 방식으로 읽을 수 있다. 페르마 수는 정수론 강의에서 다시 등장한다. 가우스(Gauss)는 정n각형을 자와 컴퍼스로 작도할 수 있는 것은 n이 2의 거듭제곱과 서로 다른 페르마 소수들의 곱을 곱한 꼴일 때, 그리고 그때뿐임을 보였다. 그리고 F_4보다 큰 페르마 소수는 알려져 있지 않다. 더 알고 싶다면 Davenport의 *The Higher Arithmetic*(고등 산술)을 읽어 보라.

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.