1.1 소수 공장

학습지

문제

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

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** 마지막 줄은 **무한히 많은 소수**에 대해 묻는다. 가운데 부분은 **공약수**에 대해 묻는다. "두 페르마 수(Fermat number)는 공약수를 갖지 않는다"는 사실과 "소수는 무한히 많다"는 사실은 도대체 어떻게 연결될 수 있을까?

1단계 수에 대한 감 잡기

다루는 내용: 처음 네 개의 페르마(Fermat) 수(Fermat number)

> ? **생각해 보기** 거듭제곱이 겹쳐 있는 꼴에 주의한다. 2^{2^n}은 $2^{(2^n)}$을 뜻한다. 먼저 $n = 0, 1, 2, 3$에 대하여 2^n을 계산하고, 그다음에 2를 그 수만큼 거듭제곱한다.

2단계 항등식 확인하기

다루는 내용: $k = 1, 2, 3$일 때의 $(*)$

생각해 보기 $k = 1, 2, 3$일 때 $(*)$의 좌변은 각각 페르마 수 한 개, 두 개, 세 개의 곱이다. 각 곱을 계산하여 $F_k - 2$와 비교해 본다.

3단계 항등식(identity) 증명하기

다루는 내용: 모든 $k \geq 1$에 대한 $(*)$

생각해 보기 수학적 귀납법(induction)이 자연스러운 도구이다. $(*)$가 k에 대하여 성립한다면, $k+1$일 때의 좌변을 얻으려면 양변에 무엇을 곱해야 할까?

생각해 보기 그 단계를 거치고 나면 $(F_k - 2)\,F_k = F_{k+1} - 2$를 보여야 한다. $F_k - 2$와 F_k를 각각 2의 거듭제곱에서 1을 빼거나 더한 꼴로 써 본다.

잠깐, 직접 해 보기 $(a-1)(a+1) = a^2 - 1$이다. $a = 2^{2^k}$로 놓으면 a^2은 2의 몇 제곱인가?

4단계 공약수(common factor)가 없다

생각해 보기 $m < n$이고 d가 F_m과 F_n을 모두 나누어떨어지게 한다고 가정한다. $k = n$으로 놓고 $(*)$를 이용한다. F_m은 그 좌변의 인수 가운데 하나인가?

잠깐, 직접 해 보기 그러면 d는 F_n뿐만 아니라 $F_n - 2$도 나눈다. 그렇다면 d는 무엇을 나누어야 하는가? 가능한 경우 가운데 어느 것을 배제할 수 있으며, 그 이유는 무엇인가?

5단계 소수(prime)는 무한히 많다

생각해 보기 각 페르마 수는 적어도 하나의 소인수(prime factor)를 가진다. 각 페르마 수마다 소인수를 하나씩 고른다.

잠깐, 직접 해 보기 F_m에 대하여 고른 소수가 F_n에 대하여 고른 소수와 같을 수 있을까? 앞 문항의 결과를 이용한다.

숨은 수학

페르마는 옳았을까?

아니다. 1732년에 레온하르트 오일러(Leonhard Euler)는 다음을 보였다.

$$F_5 = 2^{32} + 1 = 4\,294\,967\,297 = 641 \times 6\,700\,417.$$

오일러가 641을 운 좋게 찾아낸 것은 아니다. 그는 F_n의 소인수가 반드시 매우 특별한 꼴이어야 함을 증명했고($n = 5$인 경우에는 64의 배수보다 1만큼 커야 한다), 이로써 후보를 크게 줄였다. 이 사실은 연습문제 4에서 직접 증명해 볼 수 있다.

그 뒤로 지금까지 누군가 판정에 성공한 페르마 수는 F_5부터 F_{32}까지 모두 합성

수(composite)로 밝혀졌다. 알려진 바로는 F_0부터 F_4까지가 **유일한** 페르마 소수일지도 모르지만, 아무도 이를 증명하지 못했다. 이것은 진정한 미해결 문제이다.

유쾌한 반전은 우리의 증명이 이런 것에 전혀 개의치 않는다는 점이다. 소수이든 합성수이든, 페르마 수들은 여전히 무한히 많은 소수를 만들어 낸다.

페르마 소수와 다각형의 작도

페르마 소수는 꽤 뜻밖의 곳에서 등장한다. 고대 그리스인들은 자와 컴퍼스로 정삼각형과 정오각형을 작도하는 방법을 알고 있었는데, $3 = F_0$이고 $5 = F_1$임에 주목하자. 이천 년 동안 아무도 변의 개수가 소수인 다른 정다각형을 작도하지 못했다. 그러다 1796년, 열아홉 살이던 카를 프리드리히 가우스(Carl Friedrich Gauss)가 **정십칠각형**을 작도하는 방법을 보였는데, $17 = F_2$이다.

가우스는 더 나아갔다. 정N각형을 자와 컴퍼스로 작도할 수 있는 것은 정확히 N이 2의 거듭제곱에 **서로 다른 페르마 소수**들을 곱한 수일 때이다. (Pierre Wantzel이 1837년에 이 증명을 완성했다.) 따라서 어떤 다각형을 작도할 수 있는지는 페르마 소수가 몇 개인지에 달려 있다. 가우스의 정십칠각형 뒤에 숨은 핵심 계산은 Section 6.2(STEP II 1991, 문제 4)에서 만나게 되며, 전체 이야기는 학부 과정의 백미 가운데 하나인 **갈루아 이론**(*Galois theory*)에 속한다.

하나의 정리, 여러 가지 증명

수학자들은 왜 같은 정리를 굳이 여러 번 증명할까? 증명이 다르면 드러나는 것도 다르기 때문이다. 흔히 크리스티안 골드바흐(Christian Goldbach)가 1730년에 오일러에게 보낸 편지에서 나온 것으로 알려진 이 증명은, 1보다 큰 자연수들로 이루어진 쌍마다 서로소인 수열이라면 **어떤** 것이든 무한히 많은 소수를 강제한다는 것을 보여 준다. 페르마 수는 편리한 예 가운데 하나일 뿐이다. (연습문제 3에서 또 다른 예를 볼 수 있다.)

이 증명은 유클리드의 증명보다 더 많은 것을 알려 주기도 한다. 소수 $p_0, p_1, \ldots, p_{n-1}$은 n개의 **서로 다른** 소수이고, 각각은 F_{n-1} 이하이다. 따라서 $2^{2^{n-1}} + 1$보다 크지 않은 소수가 적어도 n개 있다. 이것은 소수가 어떻게 분포하는지에 대한 **정량적**(*quantitative*) 명제이다. 매우 약한 결과이지만(실제로는 훨씬 더 좋다), 소수가 얼마나 드물어지는지를 정확히 기술하는 19세기 수학의 위대한 결과 가운데 하나인 **소수 정리**(*Prime Number Theorem*)를 향한 첫걸음이다. Section 1.2에서 그다음 걸음을 내디딘다.

더 도전하기

---

1 **유클리드의 증명.** 소수가 무한히 많다는 유클리드의 증명을 적어 보자. 그 증명은 어떤

의미에서 "귀류법(by contradiction)"이고, 페르마 수를 이용한 증명은 어떤 의미에서 "구성적(constructive)"인가?

2 **일의 자리 숫자.** $n \geq 2$일 때 페르마 수 F_n의 일의 자리 숫자가 7임을 보여라.

3 **실베스터 수열(Sylvester's sequence).** $a_1 = 2$, $a_{n+1} = a_n^2 - a_n + 1$로 정의하면, 수열은 $2, 3, 7, 43, 1807, \ldots$로 시작한다.

(a) $a_{n+1} - 1 = a_1 a_2 \cdots a_n$임을 보여라.

(b) 이 수열의 항들이 쌍마다 서로소임을 이끌어 내고, 이를 이용하여 소수가 무한히 많다는 또 다른 증명을 제시하여라.

(c) 심화 $\dfrac{1}{a_1} + \dfrac{1}{a_2} + \cdots + \dfrac{1}{a_n} = 1 - \dfrac{1}{a_{n+1} - 1}$임을 보여라.

4 **오일러의 기법.** 이 문제에는 페르마의 소정리(*Fermat's Little Theorem*)가 필요하다: p가 소수이고 $p \nmid a$이면 $a^{p-1} \equiv 1 \pmod{p}$이다. 소수 p가 F_n을 나눈다고 하자.

(a) $2^{2^n} \equiv -1 \pmod{p}$임을 보이고, 이로부터 $2^{2^{n+1}} \equiv 1 \pmod{p}$임을 보여라.

(b) d를 $2^d \equiv 1 \pmod{p}$를 만족하는 가장 작은 양의 정수라 하자. d가 2^{n+1}은 나누지만 2^n은 나누지 않음을 보이고, $d = 2^{n+1}$이라고 결론지어라.

(c) 페르마의 소정리를 이용하여 d가 $p - 1$을 나눔을 보여라. 이로부터 $p \equiv 1 \pmod{2^{n+1}}$임을 이끌어 내어라.

(d) $n = 5$일 때, 이 결과는 F_5의 모든 소인수가 $64k + 1$ 꼴임을 말해 준다. 641이 이 꼴임을 확인하여라. 641보다 작은 이 꼴의 소수는 몇 개인가?

5 **소수의 상계.** 하나의 정리, 여러 가지 증명의 논증을 이용하여 n번째 소수가 $2^{2^{n-1}} + 1$ 이하임을 보여라. $n = 5$일 때 이 상계는 얼마나 좋은가?

더 읽을거리

- **Martin Aigner & Günter M. Ziegler, *Proofs from THE BOOK*** (Springer), 제1장 "Six proofs of the infinity of primes"(소수가 무한함에 대한 여섯 가지 증명). 이 증명을 유클리드의 증명 및 다른 네 가지 증명과 함께 싣고 있으며, 그 가운데 하나는 위상수학(topology)을 이용한다. 대학 입학 전에 읽을 수 있는 최고의 책 가운데 하나이다.
- **Harold Davenport, *The Higher Arithmetic*** (Cambridge University Press), 제1–2장. 소수와 소인수분해에 대한 아름답게 쓰인 입문서로, 대학 입학 전 여름에 읽기에 이상적이다.
- **Michal Křížek, Florian Luca & Lawrence Somer, *17 Lectures on Fermat Numbers*** (Springer, 2001). 오일러의 인수분해부터 가우스의 다각형까지, 페르마 수에 관한 모든 것을 담고 있다. 앞쪽 장들을 골라 읽어 보자.

- **Ian Stewart, *Why Beauty Is Truth*** (Basic Books), 가우스에 관한 장. 일반 독자를 위해 풀어 쓴 정십칠각형 이야기이다.

안내에 따른 전체 풀이는 제 1.1절에 있다:
https://beyondstep.keithmcnulty.org/ko/ch01/fermat-numbers.html

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