풀이

STEP II 2005, 문제 2

순수수학 • 오일러 피 함수

> **STEP II 2005, 2번 문제**
>
> 더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:
>
> step.maths.org/questions/05-s2-q2

핵심 아이디어

모든 것은 N을 소인수분해(prime factorisation)한 꼴로 쓰는 데서 나온다. 각 인수 $(1-\frac{1}{p}) = \frac{p-1}{p}$는 분모에 p를 가지고 있고, N에는 이를 약분할 p가 적어도 하나는 반드시 들어 있다. $\mathrm{f}(N)$을 소수의 거듭제곱들에 대한 곱으로 쓰고 나면, $\mathrm{f}(m)\mathrm{f}(n)$과 $\mathrm{f}(mn)$이 언제 같은지 정확히 알 수 있다. 그것은 m과 n이 공통인 소인수를 가지는지에 달려 있다.

풀이

소문항 (i)

(a) $12 = 2^2 \cdot 3$을 나누는 소수(prime)는 2와 3이므로

$$\mathrm{f}(12) = 12\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4.$$

$180 = 2^2 \cdot 3^2 \cdot 5$를 나누는 소수는 2, 3, 5이므로

$$\mathrm{f}(180) = 180 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 48.$$

(b) $N = 1$이면 소인수가 없으므로 곱은 빈 곱이 되고, $\mathrm{f}(1) = 1$이다. $N \geq 2$이면

$$N = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

으로 쓰자. 여기서 p_i는 N을 나누는 서로 다른 소수들이고, 모든 $a_i \geq 1$이다. 그러면

$$\begin{aligned}\mathrm{f}(N) &= p_1^{a_1} \cdots p_k^{a_k} \cdot \frac{p_1 - 1}{p_1} \cdots \frac{p_k - 1}{p_k} \\ &= p_1^{a_1 - 1}(p_1 - 1)\, p_2^{a_2 - 1}(p_2 - 1) \cdots p_k^{a_k - 1}(p_k - 1).\end{aligned}$$

각 $a_i \geq 1$이므로 모든 지수 $a_i - 1$은 음이 아닌 정수이고, 따라서 각 인수 $p_i^{a_i-1}(p_i - 1)$은 양의 정수이다. 그러므로 모든 N에 대하여 $\mathrm{f}(N)$은 정수이다. 이 문제의 나머지 부분에서는 다음 공식

$$\mathrm{f}(N) = \prod_{i=1}^{k} p_i^{a_i-1}(p_i - 1), \qquad (*)$$

을 사용한다.

소문항 (ii)

(a) 이 명제는 거짓이다. $m = n = 2$로 잡자. 그러면 $\mathrm{f}(2) = 2 \cdot \frac{1}{2} = 1$이므로 $\mathrm{f}(2)\mathrm{f}(2) = 1$이지만, $\mathrm{f}(4) = 4 \cdot \frac{1}{2} = 2$이다.

문제는 인수 $(1 - \frac{1}{2})$가 좌변에는 두 번 나타나지만 우변에는 한 번만 나타난다는 점이다. 2는 4의 소인수로서 한 번만 세어지기 때문이다.

(b) 이 명제는 참이다. p와 q가 서로 다른 소수이면 $\mathrm{f}(p) = p(1 - \frac{1}{p}) = p - 1$이고, 마찬가지로 $\mathrm{f}(q) = q - 1$이다. pq를 나누는 소수는 정확히 p와 q이고 이 둘은 서로 다르므로

$$\mathrm{f}(pq) = pq\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) = (p-1)(q-1) = \mathrm{f}(p)\mathrm{f}(q).$$

(c) 주장은 $\mathrm{f}(p)\mathrm{f}(q) = \mathrm{f}(pq)$가 p와 q가 서로 다른 소수일 **때에만** 성립할 수 있다는 것, 즉 이 등식이 성립하면 p와 q는 반드시 서로 다른 소수라는 것이다. 이 명제는 거짓이다. $p = 3$, $q = 4$로 잡자. 등식이 의미를 가지기 위해 둘 다 소수일 필요는 없다. 그러면 소문항 (i)(a)에 의해

$$\mathrm{f}(3)\mathrm{f}(4) = 2 \cdot 2 = 4 = \mathrm{f}(12),$$

이지만 4는 소수가 아니다. (더 간단한 예는 $p = 1$이다. 모든 q에 대하여 $\mathrm{f}(1)\mathrm{f}(q) = \mathrm{f}(q)$이기 때문이다.)

> **생각해 보기** 소수라는 성질이 아니라면, 이 등식을 실제로 성립하게 만드는 것은 무엇일까?

중요한 것은 p와 q가 공통인 소인수를 갖지 않는다는 것이다. $\gcd(m, n) = 1$이면 m에 들어 있는 소수의 거듭제곱과 n에 들어 있는 소수의 거듭제곱이 서로 다르므로, mn의 소인수분해는 두 소인수분해를 나란히 놓은 것일 뿐이고, $(*)$에 의해 $\mathrm{f}(mn) = \mathrm{f}(m)\mathrm{f}(n)$이다. 어떤 소수 r이 둘을 모두 나누면 인수 $(1 - \frac{1}{r})$가 $\mathrm{f}(m)\mathrm{f}(n)$에는 두 번, $\mathrm{f}(mn)$에는 한 번 나타나므로 $\mathrm{f}(m)\mathrm{f}(n) < \mathrm{f}(mn)$이다. 따라서 등식은 정확히 $\gcd(m, n) = 1$일 때 성립하며, 3, 4는 소수의 쌍이 아닌 서로소(coprime)인 쌍의 한 예일 뿐이다.

한편 소문항 (ii) 전체에서 p와 q가 소수를 나타낸다고 읽는다면, (c)는 $p = q$인 경우가 가능한지만을 묻는 것이 되고, 그런 경우는 불가능하다. $\mathrm{f}(p)^2 = (p-1)^2$이고

$f(p^2) = p(p-1)$인데, $p - 1 \neq p$이므로 이 둘은 결코 같지 않다. 이렇게 읽으면 (c)는 참이다. 그러나 위의 반례(counterexample)와 함께 일반적으로 읽는 쪽이 더 자연스럽다.

소문항 (iii)

$(*)$에 의해 소수의 거듭제곱에 대하여

$$f(p^m) = p^{m-1}(p-1).$$

이다. $14641 = 121^2 = 11^4$이므로 목표값을 소인수분해하면 $146410 = 10 \times 14641 = 2 \cdot 5 \cdot 11^4$이다. 이것은 이미 $p = 11$일 때 $p^{m-1}(p-1)$의 꼴이다. $11^4 \cdot 10 = 11^4(11-1)$이므로 $m - 1 = 4$이다. 따라서

$$p = 11, \quad m = 5: \qquad f(11^5) = 11^4 \cdot 10 = 146410.$$

사실 이것이 유일한 답이다. $m \geq 2$이면 p는 146410을 나누므로 $p \in \{2, 5, 11\}$이다. $p = 2$로 잡으면 $2^{m-1} = 146410$이 되어야 하는데, 146410은 홀수인 소인수를 가지므로 불가능하다. $p = 5$로 잡으면 $4 \cdot 5^{m-1} = 146410$이 되어야 하는데, 146410은 4로 나누어떨어지지 않으므로 불가능하다. 남은 것은 $p = 11$이고, 이때 $m = 5$이다. $m = 1$이면 $p = 146411$이 소수여야 하지만, $146411 = 41 \times 3571$이다.

검산

- 이 함수는 오일러(Euler)의 피 함수(Euler's totient function)이다. 즉 $f(N)$은 $\{1, \ldots, N\}$에 속하는 정수 중 N과 서로소인 것의 개수를 센다. 예를 들어 $N = 12$일 때 그러한 수는 $1, 5, 7, 11$의 네 개이다. 컴퓨터로 $N < 2000$인 모든 N에 대하여 곱 공식이 이 개수와 일치하고 정수임을 확인하였다.
- 문제에 주어진 예시는 $f(80) = 80 \cdot \frac{1}{2} \cdot \frac{4}{5} = 32 = 2^3(2-1) \cdot 5^0(5-1)$이며, 이는 $(*)$와 일치한다.
- 컴퓨터로 $m, n \leq 400$인 무작위 쌍 20 000개를 검사한 결과, $f(m)f(n) = f(mn)$은 정확히 $\gcd(m, n) = 1$일 때 성립하였다. $p \leq 146411$인 모든 소수를 탐색한 결과, (iii)의 해는 $(p, m) = (11, 5)$뿐이었다.

흔한 실수

- 곱에 같은 소수를 두 번 이상 넣는 것. $180 = 2^2 \cdot 3^2 \cdot 5$의 경우 인수는 다섯 개가 아니라 세 개이다.
- "일 때에만(only if)"을 "이면(if)"으로 다루는 것. (b)는 "이면" 방향이고 (c)는 그 역(converse)으로, 서로 다른 명제이다.

▶ (iii)에서 $14641 = 11^4$임을 놓치는 것. $11^2 = 121$이고 $121^2 = 14641$임을 알아차리거나, 파스칼(Pascal)의 삼각형의 행 $1, 4, 6, 4, 1$을 알아보면 빨리 찾을 수 있다.

STEP 너머

이 함수는 오일러의 피 함수 φ이며, 소문항 (ii)의 사실들은 이 함수가 **곱셈적**(*multiplicative*)이라는 것, 즉 일반적으로는 아니지만 $\gcd(m, n) = 1$일 때마다 $\varphi(mn) = \varphi(m)\varphi(n)$임을 말해 준다. 이 함수는 n과 서로소인 a에 대하여 $a^{\varphi(n)} \equiv 1 \pmod{n}$이라는 오일러 정리(Euler's theorem)에 등장하는데, 이 정리는 페르마(Fermat)의 소정리(Fermat's little theorem)를 일반화한 것이며 RSA 암호의 바탕이 된다. 군론(group theory)에서 $\varphi(n)$은 법 n에 대한 단위군(group of units)의 위수(order)이다. Davenport의 *The Higher Arithmetic*(고등 산술)은 이 모든 내용을 아름답게 전개한다.

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.