풀이

STEP I 1996, 문제 3

순수수학 • 정수의 나누어떨어짐

> **STEP I 1996, 3번 문제**
>
> 더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:
>
> step.maths.org/questions/96-s1-q3

핵심 아이디어

24와 같은 합성수(composite number)로 나누어떨어짐을 다룰 때는 소수의 거듭제곱 하나씩 따로 보는 것이 가장 쉽다. $24 = 3 \times 8$이고 3과 8은 서로소(coprime)이므로, 3으로 나누어떨어짐과 8로 나누어떨어짐을 따로 보이면 된다. 인수분해(factorisation)를 하면 연속한 정수들의 곱이 나오는데, 연속한 정수 k개 중에는 반드시 k의 배수가 하나 있다. 나머지 두 소문항도 같은 습관으로 해결된다. 인수분해를 하거나, n을 그 나머지가 드러나는 꼴로 쓰는 것이다.

풀이

소문항 (i)

공통인수를 묶어 내고 제곱의 차 공식을 쓰면

$$n^5 - n^3 = n^3(n^2 - 1) = n^3(n-1)(n+1) = n^2\,(n-1)\,n\,(n+1).$$

3으로 나누어떨어짐. $n-1$, n, $n+1$은 연속한 세 정수이므로 이 중 정확히 하나가 3의 배수이다. 따라서 $3 \mid (n-1)n(n+1)$이고, 그러므로 $3 \mid n^5 - n^3$이다.

8로 나누어떨어짐. n의 홀짝성(parity)에 따라 경우를 나눈다.

- n이 짝수이면, $n = 2m$이라 할 때 $n^3 = 8m^3$이므로 8의 배수이다.
- n이 홀수이면, $n-1$과 $n+1$은 연속한 두 짝수이다. 연속한 두 짝수 중 하나는 4의 배수이고 다른 하나는 2의 배수이므로 $8 \mid (n-1)(n+1)$이다.

어느 경우든 $8 \mid n^3(n-1)(n+1) = n^5 - n^3$이다.

생각해 보기 $3 \mid N$과 $8 \mid N$을 알면 왜 $24 \mid N$이 되는가? $4 \mid N$과 $6 \mid N$으로도 같은 결론을 얻을 수 있는가?

3과 8은 공통인수가 없으므로, $8 \mid N$이면 $N = 8a$이고, 이때 $3 \mid 8a$이면 반드시 $3 \mid a$이다(3은 소수이고 8을 나누지 않기 때문이다). 따라서 $N = 24b$이다. 이 논증은 공통인수 2를 가지는 4와 6에 대해서는 성립하지 않는다. 12는 둘 다로 나누어떨어지지만 24로는 나누어떨어지지 않는다.

그러므로 모든 양의 정수 n에 대하여 $n^5 - n^3$은 24로 나누어떨어진다.

소문항 (ii)

$2^{2n} = 4^n$으로 쓴다. 인수분해 $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$에 $x = 4$를 대입하면

$$2^{2n} - 1 = 4^n - 1 = (4-1)\left(4^{n-1} + 4^{n-2} + \cdots + 4 + 1\right) = 3\left(4^{n-1} + \cdots + 1\right).$$

괄호 안은 정수이므로 $2^{2n} - 1$은 3으로 나누어떨어진다.

같은 내용을 합동식(modular arithmetic)으로 쓰면 다음과 같다. $4 \equiv 1 \pmod 3$이므로 $4^n \equiv 1^n = 1 \pmod 3$이다. 수학적 귀납법(induction)으로 증명할 수도 있다. $4^k - 1 = 3a$이면 $4^{k+1} - 1 = 4(4^k - 1) + 3 = 3(4a + 1)$이다.

소문항 (iii)

$3 \mid n - 1$이므로 어떤 정수 $k \geq 0$에 대하여 $n = 3k + 1$로 쓴다. 다음과 같이 인수분해한다.

$$n^3 - 1 = (n-1)(n^2 + n + 1).$$

첫째 인수는 $n - 1 = 3k$이다. 둘째 인수는

$$\begin{aligned} n^2 + n + 1 &= (9k^2 + 6k + 1) + (3k + 1) + 1 \\ &= 9k^2 + 9k + 3 \\ &= 3(3k^2 + 3k + 1). \end{aligned}$$

따라서 각 인수가 3을 하나씩 내놓는다.

$$n^3 - 1 = 3k \cdot 3(3k^2 + 3k + 1) = 9k(3k^2 + 3k + 1),$$

이는 9로 나누어떨어진다. ($n = 1$일 때는 $k = 0$이고 $n^3 - 1 = 0$이며, 이 역시 9로 나누어떨어진다.)

핵심은 $n - 1$이 3을 하나만 내놓는다는 것이다. 두 번째 3은 $n^2 + n + 1$에서 나온다. 이 두 번째 인수를 깔끔하게 보는 방법은 $n^2 + n + 1 = (n-1)^2 + 3n$으로 쓰는 것인데, $3 \mid n - 1$이면 이는 3의 배수 두 개의 합이다.

검산

- 소문항 (i): $n = 2$이면 $32 - 8 = 24$이고, $n = 3$이면 $243 - 27 = 216 = 9 \times 24$이다. $n = 2$일 때 정확히 24가 나오므로, 모든 $n^5 - n^3$을 나누는 수 중 24보다 큰 것은 없다. 즉 24가 가장 좋은 값이다.
- 소문항 (ii): $n = 1, 2, 3$이면 각각 3, 15, 63이다.
- 소문항 (iii): $n = 4$이면 $63 = 7 \times 9$이고, $n = 7$이면 $342 = 38 \times 9$이며, 이는 $k = 1$, $k = 2$일 때의 $9k(3k^2 + 3k + 1)$과 일치한다.

세 결과 모두 5000 미만의 모든 n에 대하여(소문항 (ii)는 $n < 2000$에 대하여) 컴퓨터로 확인하였고, $n^5 - n^3$ 값들의 최대공약수가 정확히 24임도 확인하였다.

흔한 실수

- "$(n-1)n(n+1)$은 6으로 나누어떨어지고, n^2은 ..."라고 논증하다가 인수 8이 어디서 나오는지 놓치는 것. 짝수인 경우에는 n만이 아니라 n^3이 필요하다.
- 4로 나누어떨어지고 6으로 나누어떨어진다는 것에서 24로 나누어떨어진다고 결론짓는 것. 인수들은 서로소여야 한다.
- 소문항 (iii)에서 "$n - 1$이 3으로 나누어떨어지므로 $n^3 - 1 = (n-1)(\dots)$은 3으로 나누어떨어진다"에서 멈추는 것. 이렇게 하면 3을 하나만 얻는다.

STEP 너머

세 소문항은 모두 사실 합동식에 관한 명제이다. m을 법으로 하는 정수들은 환(ring)을 이루며, 소문항 (iii)은 $n \equiv 1 \pmod 3$이면 $n^3 \equiv 1 \pmod 9$라는 뜻이다. 이는 **지수 올리기**(*lifting the exponent*)라 불리는 일반적인 현상의 첫 단계이다. $p \mid n - 1$이면 $p^{j+1} \mid n^{p^j} - 1$이다. 페르마(Fermat)의 소정리(little theorem)($n^p \equiv n \pmod p$)로 소문항 (i)도 설명할 수 있는데, 이 정리에서 곧바로 $3 \mid n^3 - n$을 얻기 때문이다. Davenport의 *The Higher Arithmetic*(고등 정수론)은 이러한 아이디어에 대한 아름다운 입문서이다.

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.