풀이

STEP I 1992, 문제 5

순수수학 • 다항식의 중복 인수

> **STEP I 1992, 5번 문제**
>
> 더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:
>
> step.maths.org/questions/92-s1-q5

이 문제는 *Beyond STEP*의 9.7 절 **같은 거듭제곱의 합**에서 단계별 안내와 함께 자세히 다룬다: https://beyondstep.keithmcnulty.org/ko/ch09/equal-power-sums.html

핵심 아이디어

다항식(polynomial)이 중복된 인수(factor) $(1-x)^m$을 가지면, 이를 미분하고 x를 곱해도 인수 $(1-x)^{m-1}$이 남는다. 따라서 1은 이 다항식의 근(root)일 뿐 아니라, 이렇게 이어지는 다음 몇 개의 다항식의 근이기도 하다. 이 다항식들 각각에 계수(coefficient)를 이용하여 $x=1$을 대입하면 $\sum k^r c_k$ 꼴의 합이 나온다. 모든 계수가 ± 1이면, 이 합들은 각각 두 정수 집합의 r제곱의 합이 같다는 것을 말해 준다.

풀이

인수 $(1-x)^3$

제곱의 차 공식(difference of two squares)을 두 번 쓰면

$$1-x^2=(1-x)(1+x), \qquad 1-x^4=(1-x^2)(1+x^2)=(1-x)(1+x)(1+x^2),$$

이므로

$$\mathrm{p}_0(x)=(1-x)^3(1+x)^2(1+x^2),$$

이다. 따라서 요구한 대로 $(1-x)^3$은 $\mathrm{p}_0(x)$의 인수이다.

$\mathrm{p}_0'(1)=0$과 $\mathrm{p}_1'(1)=0$

작은 사실 하나를 증명하고 이를 반복해서 사용한다.

보조정리(*lemma*). $m \geq 1$이고 q가 다항식일 때 $\mathrm{p}(x) = (1-x)^m \mathrm{q}(x)$이면, $\mathrm{p}'(x)$는, 따라서 $x\mathrm{p}'(x)$도, 인수 $(1-x)^{m-1}$을 가진다.

증명(*proof*). 곱의 미분법(product rule)에 의해

$$\mathrm{p}'(x) = -m(1-x)^{m-1}\mathrm{q}(x) + (1-x)^m \mathrm{q}'(x) = (1-x)^{m-1}\big[(1-x)\mathrm{q}'(x) - m\,\mathrm{q}(x)\big],$$

이고, 대괄호 안은 다항식이다. x를 곱해도 이 인수는 없어지지 않는다. □

$m = 3$으로 이를 적용하면 $\mathrm{p}_0'(x)$는 인수 $(1-x)^2$을 가지므로 $\mathrm{p}_0'(1) = 0$이다. 또 $\mathrm{p}_1(x) = x\mathrm{p}_0'(x)$도 인수 $(1-x)^2$을 가진다. $m = 2$로 보조정리를 한 번 더 적용하면 $\mathrm{p}_1'(x)$는 인수 $1-x$를 가지므로 $\mathrm{p}_1'(1) = 0$이다.

? **생각해 보기** 세 괄호의 곱을 그냥 미분하고 $x = 1$을 대입하면 안 될까?

그렇게 할 수도 있지만, 문제는 인수를 이용해 논증하라고 요구하고 있으며, 일반화되는 것도 인수를 이용한 논증이다. 중복도(multiplicity)가 m인 근은 $m-1$번 미분해도 살아남으며, 마지막 소문항에서 필요한 것이 바로 이 사실이다.

두 항등식

전개하면

$$(1-x)(1-x^2) = 1 - x - x^2 + x^3,$$

이고, 이어서

$$\mathrm{p}_0(x) = 1 - x - x^2 + x^3 - x^4 + x^5 + x^6 - x^7.$$

이다. 따라서 $c_0 = c_3 = c_5 = c_6 = 1$이고 $c_1 = c_2 = c_4 = c_7 = -1$이다.

이제

$$\mathrm{p}_0'(x) = \sum_{k=1}^{7} k\,c_k x^{k-1}, \qquad \mathrm{p}_1(x) = \sum_{k=0}^{7} k\,c_k x^k, \qquad \mathrm{p}_1'(x) = \sum_{k=1}^{7} k^2 c_k x^{k-1}.$$

이다. $x = 1$을 대입하고 $\mathrm{p}_0'(1) = 0$을 이용하면

$$-1 - 2 + 3 - 4 + 5 + 6 - 7 = 0, \quad \text{즉} \quad 1 + 2 + 4 + 7 = 3 + 5 + 6.$$

이고, $\mathrm{p}_1'(1) = 0$을 이용하면

$$-1^2 - 2^2 + 3^2 - 4^2 + 5^2 + 6^2 - 7^2 = 0, \quad \text{즉} \quad 1^2 + 2^2 + 4^2 + 7^2 = 3^2 + 5^2 + 6^2.$$

이다. (양변은 각각 14이고, 제곱의 경우에는 70이다.) c_0항은 0 또는 0^2이 곱해지므로 아무 기여도 하지 않는다.

마지막 소문항

한 단계 더 나아가자.

$$\mathrm{P}_0(x) = (1-x)(1-x^2)(1-x^4)(1-x^8) = \mathrm{p}_0(x)(1-x^8).$$

이라 하자. $1-x^8 = (1-x)(1+x)(1+x^2)(1+x^4)$이므로 $\mathrm{P}_0(x)$는 인수 $(1-x)^4$을 가진다. $j = 0, 1, 2$에 대하여 $\mathrm{P}_{j+1}(x) = x\mathrm{P}_j'(x)$로 정의한다. 보조정리에 의해 P_1, P_2, P_3은 각각 인수 $(1-x)^3$, $(1-x)^2$, $(1-x)$를 가지므로

$$\mathrm{P}_1(1) = \mathrm{P}_2(1) = \mathrm{P}_3(1) = 0.$$

이다.

$\mathrm{P}_0(x) = \sum_{k=0}^{15} d_k x^k$로 쓰자. $x\frac{\mathrm{d}}{\mathrm{d}x}$를 한 번 적용할 때마다 x^k의 계수에 k가 곱해지므로 $\mathrm{P}_r(x) = \sum_{k=0}^{15} k^r d_k x^k$이고,

$$\sum_{k=1}^{15} k^r d_k = 0 \qquad \text{단, } r = 1, 2, 3.$$

이다.

d_k를 구하기 위해 $\mathrm{p}_0(x)$에 $1-x^8$을 곱한다. 그러면

$$\mathrm{P}_0(x) = \mathrm{p}_0(x) - x^8\mathrm{p}_0(x).$$

이다. 둘째 항은 p_0의 부호를 반대로 한 $x^8, \ldots, x^{15}$의 항들을 준다. 겹치는 항이 없으므로 모든 d_k는 ± 1이다.

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
d_k	+	−	−	+	−	+	+	−	−	+	+	−	+	−	−	+

(사실 $d_k = (-1)^{s(k)}$이며, 여기서 $s(k)$는 k의 이진 전개(binary expansion)에 나타나는 1의 개수이다. x^k는 k의 이진 자릿수에 대응하는 괄호들에서 $-x^{2^i}$를 골라서 생기기 때문이다.)

$k = 0$을 제외하면, $k \in \{1, 2, 4, 7, 8, 11, 13, 14\}$(여덟 개의 수)에 대해서는 계수 $d_k = -1$이고, $k \in \{3, 5, 6, 9, 10, 12, 15\}$(일곱 개의 수)에 대해서는 $d_k = +1$이다. 이 둘을 합치면 정확히 $1, 2, \ldots, 15$가 된다. 따라서

$$(a_1, \ldots, a_8) = (1, 2, 4, 7, 8, 11, 13, 14), \qquad (a_9, \ldots, a_{15}) = (3, 5, 6, 9, 10, 12, 15).$$

로 잡자. 그러면 $\sum k^r d_k = 0$은 정확히

$$a_1^r + \cdots + a_8^r = a_9^r + \cdots + a_{15}^r \qquad (r = 1, 2, 3),$$

를 뜻하며, 이것이 보여야 할 내용이다.

생각해 보기 왜 한쪽에는 여덟 개, 다른 쪽에는 일곱 개의 수가 오도록 나뉠까?

$+1$ 쪽에는 $k = 0$도 들어 있는데, 이것은 $r \geq 1$일 때 $0^r = 0$을 기여하므로 빼도 된다. 그래서 양쪽의 항의 개수가 같을 필요가 없다. ($r = 0$이면 항등식에 0이 필요하며, 이때는 $8 = 8$이 된다.)

검산

직접 계산하면, 합은 $r = 1$일 때 $60 = 60$, $r = 2$일 때 $620 = 620$, $r = 3$일 때 $7200 = 7200$이다. 컴퓨터로 P_0를 전개하여 그 부호들과 근 $x = 1$의 중복도가 4임을 확인하였고, 세 등식을 모두 검증하였다. $r = 4$일 때는 등식이 성립하지 않는데(근의 중복도가 4뿐이므로), 이는 논증이 빈틈없이 정확하다는 좋은 신호이다.

흔한 실수

- $k = 0$항을 잊어버려서 양쪽의 크기가 같아야 한다고 생각하는 것.
- $\mathrm{p}_0''(1) = 0$만으로 $\mathrm{p}_1'(1) = 0$이라고 결론짓는 것. $\mathrm{p}_1' = \mathrm{p}_0' + x\mathrm{p}_0''$이므로 $\mathrm{p}_0'(1) = 0$과 $\mathrm{p}_0''(1) = 0$이 모두 필요하다.

STEP 너머

이것은 Prouhet–Tarry–Escott 문제이다. $\{0, 1, \ldots, 2^n - 1\}$을 이진 자릿수 합의 홀짝성(parity)에 따라 나누면(투에-모스 수열(Thue–Morse sequence)), $r < n$인 모든 r에 대하여 r제곱의 합이 같은 두 집합을 얻는다. 그 뒤에 있는 도구, 즉 중복도가 m인 근은 처음 $m - 1$개의 도함수의 근이기도 하다는 사실은 임의의 체(field) 위의 다항식 대수에서 핵심적이다. 다항식과 그 근의 대수에 대해서는 Allenby, *Rings, Fields and Groups*(환, 체, 군)를 참고하라. 더 일반적인 정수론에 대해서는 Davenport, *The Higher Arithmetic*(고등 산술)을 참고하라.

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.