풀이

STEP II 1997, 문제 4

순수수학 • 나머지 정리

> **STEP II 1997, 4번 문제**
>
> 더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:
>
> step.maths.org/questions/97-s2-q4

핵심 아이디어

차수(degree)가 d인 다항식으로 나누면 나머지(remainder)의 차수는 d보다 작고, 항등식(identity) 피제수 $=$ 제수 $\times$ 몫 $+$ 나머지는 **모든** x에 대해 성립한다. 따라서 제수를 0으로 만드는 x의 값을 대입하면 몫(quotient)이 사라지고 나머지만 남는다. 이 문제의 모든 내용은 이 한 가지 요령을 세 번 쓰는 것이다.

풀이

나머지 정리

$\mathrm{p}(x)$를 일차 다항식 $x-a$로 나누면 몫 $\mathrm{s}(x)$와 차수가 1보다 작은 나머지 R가 생기므로, R는 상수이다.

$$\mathrm{p}(x) = (x-a)\,\mathrm{s}(x) + R \qquad \text{모든} x.$$

이것은 x에 대한 항등식이므로 $x=a$를 대입할 수 있다. 우변의 첫째 항은 $0\cdot \mathrm{s}(a)=0$이 되어 $\mathrm{p}(a)=R$만 남는다. 따라서 나머지는 $\mathrm{p}(a)$이고, 이것이 보이려던 것이다.

소문항 (i)

나머지 정리(remainder theorem)에 의해 주어진 나머지들은 다음을 뜻한다.

$$\mathrm{p}(1)=3, \qquad \mathrm{p}(2)=1, \qquad \mathrm{p}(3)=5.$$

$\mathrm{p}(x)=(x-1)(x-2)(x-3)\mathrm{q}(x)+\mathrm{r}(x)$에 $x=1,2,3$을 대입하면 매번 첫째 항이 없어지므로

$$\mathrm{r}(1)=3, \qquad \mathrm{r}(2)=1, \qquad \mathrm{r}(3)=5.$$

생각해 보기 우리는 $\mathrm{q}(x)$에 대해 아무것도 모른다. 이것이 문제가 될까?

그렇지 않다. $x = 1, 2, 3$에서 인수 $(x-1)(x-2)(x-3)$이 0이므로 q가 무엇이든 아무런 기여도 하지 않는다. r는 계수가 많아야 세 개이므로 세 개의 값으로 완전히 결정된다.

차수가 2 이하인 다항식을 다음과 같이 쓰면 편리하다.

$$\mathrm{r}(x) = A(x-1)(x-2) + B(x-1) + C,$$

이렇게 쓰면 대입할 때마다 항이 하나씩 사라지기 때문이다.

$$\begin{aligned} x = 1: &\quad C = 3, \\ x = 2: &\quad B + C = 1 \;\Rightarrow\; B = -2, \\ x = 3: &\quad 2A + 2B + C = 5 \;\Rightarrow\; 2A - 4 + 3 = 5 \;\Rightarrow\; A = 3. \end{aligned}$$

따라서

$$\mathrm{r}(x) = 3(x-1)(x-2) - 2(x-1) + 3 = 3x^2 - 11x + 11.$$

확인하면 $\mathrm{r}(1) = 3 - 11 + 11 = 3$, $\mathrm{r}(2) = 12 - 22 + 11 = 1$, $\mathrm{r}(3) = 27 - 33 + 11 = 5$이다.

소문항 (ii)

(문제에서 한 곳에 $\mathrm{P}_n(x)$라고 쓰여 있는데, 이는 같은 다항식 $\mathrm{P}(x)$를 뜻한다.) 나머지 정리에 의해 다음이 필요하다.

$$\mathrm{P}(a) = a \qquad \text{단, } a = 0, 1, \ldots, n.$$

다항식 x는 이미 이 조건을 만족하지만 차수가 맞지 않는다. 그래서 대신 $\mathrm{D}(x) = \mathrm{P}(x) - x$를 살펴보자. $a = 0, 1, \ldots, n$에 대해 $\mathrm{D}(a) = 0$이어야 하므로, 인수 정리(factor theorem, 나머지가 0인 경우의 나머지 정리)에 의해 $x, x-1, \ldots, x-n$ 각각이 $\mathrm{D}(x)$를 나누어떨어지게 한다. 이 $n+1$개의 일차 인수는 서로 다르므로 그 곱이 $\mathrm{D}(x)$를 나누고, 그 곱의 차수는 $n+1$이다.

생각해 보기 어떻게 하면 $\mathrm{P}(x)$의 차수가 정확히 $n+1$이 되게 할 수 있을까?

$\mathrm{D}(x)$를 바로 그 곱으로 잡으면 된다(원한다면 0이 아닌 상수를 곱해도 된다). $n+1 \geq 2$이므로 x를 더해도 최고차항(leading term) x^{n+1}이 상쇄되지 않는다. 따라서

$$\mathrm{P}(x) = x + x(x-1)(x-2)\cdots(x-n)$$

은 차수가 $n+1$이고, $0 \leq a \leq n$인 각 정수 a에 대해 $\mathrm{P}(a) = a + 0 = a$이다. 이것이 요구된 종류의 다항식이다.

사실 이 논증으로 그러한 다항식을 모두 찾을 수 있다. P의 차수가 $n+1$이고 주어진 나머지를 가진다면, $\mathrm{D}(x) = \mathrm{P}(x) - x$는 차수가 $n+1$ 이하이고 차수 $n+1$인 곱으로 나누어떨어지므로 어떤 상수 k에 대해 $\mathrm{D}(x) = k\,x(x-1)\cdots(x-n)$이며, 차수가 $n+1$이 되려면 $k \neq 0$이어야 한다. 일반적인 답은 다음과 같다.

$$\mathrm{P}(x) = x + k\,x(x-1)(x-2)\cdots(x-n), \qquad k \neq 0.$$

검산

- $n = 1$이면 $\mathrm{P}(x) = x + x(x-1) = x^2$이다. x로 나누면 나머지가 0이고 $x-1$로 나누면 나머지가 1이므로 조건에 맞는다.
- (i)에서 아무 q, 예컨대 $\mathrm{q}(x) = x$를 잡아 p를 만들고 조립제법(synthetic division)으로 $x-1, x-2, x-3$으로 나누면 나머지가 $3, 1, 5$로 나온다.
- 컴퓨터로 무작위 다항식 1000개에 대해 나머지 정리를, 무작위로 고른 q 100개에 대해 소문항 (i)을, $k = 1, -3, 7$일 때 $n = 1, \ldots, 11$에 대해 소문항 (ii)를 확인했으며, 모든 나머지가 정확히 일치했다.

흔한 실수

- 소문항 (ii)에서 다항식 $\mathrm{P}(x) = x$ 자체도 조건을 만족하지만 차수가 $n+1$이 아니라 1이라는 점을 잊는 것. 차수를 맞춰 주는 것은 곱으로 된 항이다.
- $ax^2 + bx + c$의 계수에 대한 세 개의 연립방정식(simultaneous equations)을 푸는 것도 괜찮지만 더 느리다. 중첩된 형태 $A(x-1)(x-2) + B(x-1) + C$를 쓰면 소거 과정을 피할 수 있다.

STEP 너머

소문항 (i)은 다항식 보간(polynomial interpolation)의 한 예이다. x값이 서로 다른 임의의 m개의 점을 지나는, 차수가 m보다 작은 다항식은 정확히 하나 존재하며, 우리가 사용한 중첩된 형태는 그 다항식의 뉴턴(Newton) 형식이다. 같은 논리를 환(ring)의 언어로 표현하면 다항식에 대한 중국인의 나머지 정리(Chinese remainder theorem)가 된다. 즉 $x-1$, $x-2$, $x-3$을 법으로 하는 다항식을 아는 것은 이들의 곱을 법으로 하는 다항식을 아는 것과 같다. Allenby의 *Rings, Fields and Groups*(환, 체, 군)에서 다항식환과 이 정리를 다룬다.

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.