풀이

STEP III 2010, 문제 3

순수수학 • 1의 거듭제곱근

STEP III 2010, 3번 문제

더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:

step.maths.org/questions/10-s3-q3

이 문제는 *Beyond STEP*의 6.1 절 **근이 모두 단위근인 다항식**에서 단계별 안내와 함께 자세히 다룬다: https://beyondstep.keithmcnulty.org/ko/ch06/cyclotomic.html

핵심 아이디어

1의 거듭제곱근(root of unity) a는 모두 단 하나의 **위수**(order)를 가진다. 위수란 $a^m = 1$을 만족하는 가장 작은 양의 정수 m이다. 1의 원시(primitive) n제곱근이라는 것은 위수가 정확히 n이라는 뜻일 뿐이다. 따라서 $C_n(x)$를 구하려면 1의 n제곱근 $e^{2\pi ik/n}$을 나열하고, 그보다 작은 거듭제곱에서 이미 1로 돌아오는 것들을 버린 뒤, 남은 것들에 대해 $(x-a)$를 모두 곱해 전개하면 된다. 각 수가 단 하나의 위수만 가진다는 사실은 마지막 소문항을 해결하는 열쇠이기도 하다.

풀이

이 풀이 전체에서 1의 n제곱근은 $k = 0, 1, \ldots, n-1$에 대한 ω^k이다. 여기서 $\omega = e^{2\pi i/n}$이고, $(\omega^k)^m = 1$은 n이 km을 나눌 때, 그리고 그때에만 성립한다. C_n은 최고차항의 계수가 1(monic)이고 중근(repeated root)이 없으며, 그 근은 정확히 1의 원시 n제곱근이므로

$$C_n(x) = \prod_{a\text{원시}} (x-a).$$

1의 4제곱근

1의 4제곱근은 $1, i, -1, -i$이다. 이때 $1^1 = 1$이고 $(-1)^2 = 1$이므로 이 둘은 원시근이 아니다. 그러나 $i^1 = i$, $i^2 = -1$, $i^3 = -i$로 어느 것도 1이 아니며, $-i$도 마찬가지이다(그 거듭제

곱은 앞의 것들의 켤레(conjugate)이다). 따라서 1의 원시 4제곱근은 i와 $-\mathrm{i}$이고

$$C_4(x) = (x-\mathrm{i})(x+\mathrm{i}) = x^2+1,$$

이므로 요구한 결과가 성립한다.

소문항 (i)

$n = 1$. 1의 1제곱근은 1뿐이고, $0 < m < 1$인 m은 존재하지 않으므로 1은 원시근이다: $C_1(x) = x-1$.

$n = 2$. 1의 제곱근은 ± 1이다. $1^1 = 1$이므로 1은 제외되고, 한편 $(-1)^1 \neq 1$이다. 따라서 $C_2(x) = x+1$이다.

$n = 3$**과** $n = 5$. n이 소수(prime)이면, $1 \le k \le n-1$인 근 ω^k가 $(\omega^k)^m = 1$을 만족하는 것은 $n \mid km$일 때뿐이다. 그런데 n은 소수이고 k를 나누지 않으므로, 이로부터 $n \mid m$이어야 한다. 따라서 1이 아닌 1의 n제곱근은 모두 원시근이다. 이들은 다음 다항식의 근이다.

$$\frac{x^n-1}{x-1} = x^{n-1}+x^{n-2}+\cdots+x+1,$$

이 다항식은 최고차항의 계수가 1이고 서로 다른 근을 가진다. 그러므로

$$C_3(x) = x^2+x+1, \qquad C_5(x) = x^4+x^3+x^2+x+1.$$

$n = 6$. $\omega = \mathrm{e}^{\pi\mathrm{i}/3}$이라 하면 거듭제곱 ω^k의 위수는 $6/\gcd(k,6)$이다. 따라서 $\omega^0 = 1$의 위수는 1, $\omega^3 = -1$의 위수는 2, ω^2, ω^4의 위수는 3이고, 위수가 6인 것은 ω와 $\omega^5 = \overline{\omega}$뿐이다. 이 둘의 합은 $2\cos\frac{\pi}{3} = 1$이고 곱은 $|\omega|^2 = 1$이므로

$$C_6(x) = x^2-x+1.$$

(검산으로, 1의 6제곱근은 모두 위수가 1, 2, 3, 6 중 하나이므로 $x^6-1 = C_1C_2C_3C_6$이고, 실제로 $(x-1)(x+1)(x^2+x+1)(x^2-x+1) = (x^3-1)(x^3+1) = x^6-1$이다.)

소문항 (ii)

$x^4+1 = 0$의 임의의 근을 a라 하자. 그러면 $a^4 = -1$이므로 $a^8 = 1$이다. a의 위수 d는 8을 나눈다($8 = qd+r$, $0 \le r < d$로 쓰면 $a^r = a^8(a^d)^{-q} = 1$이므로, d의 최소성에 의해 $r = 0$이다). 따라서 $d \in \{1,2,4,8\}$이다. d가 1, 2, 4 중 하나라면 $a^4 = 1$이 되어 $a^4 = -1$에 모순(contradiction)이다. 그러므로 x^4+1의 근은 모두 1의 원시 8제곱근이다.

역으로, $\omega = \mathrm{e}^{\pi\mathrm{i}/4}$일 때 ω^k의 위수가 8인 것은 정확히 k가 홀수일 때이므로(k가 짝수이면 $(\omega^k)^4 = 1$), 원시 8제곱근은 정확히 네 개, 즉 $\omega, \omega^3, \omega^5, \omega^7$이다. 사차식 x^4+1은 서로 다른 네 근(이들은 $\mathrm{e}^{(2j+1)\pi\mathrm{i}/4}$, $j = 0,1,2,3$이다)을 가지며 이들은 모두 원시 8제곱근이므로, 바로 이 네 개이다. 따라서 $C_8(x) = x^4+1$이다.

다른 n은 성립하지 않는다: C_n의 근은 모두 위수가 n이고, x^4+1의 근은 위수가 8이다. 따라서 답은 $n=8$이다.

소문항 (iii)

소문항 (i)에서 $n=3$과 $n=5$에 쓴 논증은 임의의 소수 p에 그대로 적용된다: 1을 제외한 1의 p제곱근은 모두 원시근이다. 그러므로

$$C_p(x) = \frac{x^p-1}{x-1} = x^{p-1}+x^{p-2}+\cdots+x+1.$$

($p=2$이면 $x+1$이 되어 소문항 (i)의 결과와 일치한다.)

소문항 (iv)

어떤 양의 정수 q, r, s에 대해 $C_q(x) \equiv C_r(x)C_s(x)$라고 가정하고 모순을 이끌어 내자.

먼저 C_s는 적어도 하나의 근을 가진다. $e^{2\pi i/s}$가 1의 원시 s제곱근이기 때문이다: $(e^{2\pi i/s})^m = e^{2\pi i m/s} = 1$은 $s \mid m$일 때만 성립한다. C_r도 마찬가지이다. 따라서 C_r과 C_s의 차수(degree)는 모두 1 이상이다.

C_r의 임의의 근 a를 택하자. 항등식(identity)에 의해 $C_q(a) = C_r(a)C_s(a) = 0$이므로, a는 1의 원시 q제곱근이면서 동시에 1의 원시 r제곱근이다.

> **생각해 보기** 하나의 수가 1의 원시 r제곱근이면서 1의 원시 q제곱근이고 $r \neq q$일 수 있을까?

그럴 수 없다. 예를 들어 $r<q$이면 $0<r<q$인데 $a^r=1$이므로, a가 원시 q제곱근이라는 데 모순이다. $q<r$이면 역할을 바꾸면 된다. 따라서 $r=q$이고, 같은 방법으로(C_s의 근을 이용하면) $s=q$이다.

그런데 그러면 항등식은 $C_q = C_q^2$가 된다. 차수를 비교하면 $\deg C_q = 2\deg C_q$이므로 $\deg C_q = 0$이 되어, C_q가 근을 가진다는 사실에 모순이다. (또는 C_q^2는 중근을 가지지만 C_q는 그렇지 않다는 점을 써도 된다.) 따라서 그러한 q, r, s는 존재하지 않는다.

검산

- C_n의 차수는 $1 \le k \le n$이고 $\gcd(k,n)=1$인 k의 개수이다: $n=1,\ldots,6$에 대해 차수는 $1,1,2,2,4,2$이고 $n=8$에 대해서는 4로, 모두 일치한다.
- 1의 n제곱근은 모두 n의 약수인 어떤 위수 d를 가지므로, x^n-1은 n의 약수 d 전체에 대한 C_d의 곱이다. $n=4$일 때: $(x-1)(x+1)(x^2+1) = x^4-1$; $n=8$일 때: $(x^4-1)(x^4+1) = x^8-1$.

- 수치적으로, $n \leq 40$에 대해 원시근 전체에 걸쳐 $(x-a)$를 곱해 전개하면 위의 모든 다항식이 그대로 나오고, x^4+1은 $n=8$일 때만 나오며, $q,r,s \leq 30$인 범위에서 항등식 $C_q = C_r C_s$는 찾을 수 없다.

흔한 실수

- 원시근에 1(또는 -1)을 포함하는 것: C_n은 x^n-1이 아니다.
- 소문항 (ii)에서 더 작은 위수를 배제하지 않고 x^4+1이 x^8-1을 나눈다는 것만 확인하는 것: 핵심은 $a^4 = -1 \neq 1$이라는 점이다.
- 소문항 (iv)에서 차수만으로 논증하는 것: $\deg C_q = \deg C_r + \deg C_s$는 실제로 일어날 수 있으므로(예: $4 = 2+2$), 모순을 주는 것은 차수가 아니라 근이다.

STEP 너머

C_n을 **원분다항식**(cyclotomic polynomial)이라 한다. 항등식 $x^n - 1 = \prod_{d|n} C_d(x)$는 이들의 계수가 항상 정수임을 보여 주며, 더 깊은 정리에 따르면 각 원분다항식은 유리수 위에서 기약(irreducible)이다. 원분다항식은 갈루아(Galois) 이론의 핵심이며, 어떤 정다각형을 자와 컴퍼스로 작도할 수 있는지에 대한 가우스(Gauss)의 발견에서도 중심적인 역할을 한다. Allenby의 *Rings, Fields and Groups*(환, 체, 군)는 이 대수학을 전개하며, Needham의 *Visual Complex Analysis*(시각적 복소해석학)는 1의 거듭제곱근에 대한 기하학적 그림을 제공한다.

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.