VANISHING SUMS OF ROOTS OF UNITY

DONGRYUL KIM

양의 정수 n이 존재하여 $x^n = 1$이 되는 x를 root of unity(한글로는 1의 거듭제곱근)이라 부른다. 방정식 $x^n = 1$의 근들은

$$1, e^{2\pi i/n}, e^{4\pi i/n}, \ldots, e^{2(n-1)\pi i/n}$$

이므로 $\zeta_n = e^{2\pi i/n}$이라 하면 $1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$이 근이 될 것이다. 이 수들이 가지는 대수적인 성질들 덕분에 1의 거듭제곱근은 정수론이나 조합에서 자주 사용된다.

1. Algebraic properties

정리 1.1. *양의 정수 n과 복소수 $\zeta = \zeta_n$에 대해 다음이 성립한다.*

$$1 + \zeta^m + \zeta^{2m} + \cdots + \zeta^{(n-1)m} = \begin{cases} n & \text{if } n \mid m, \\ 0 & \text{if } n \nmid m. \end{cases}$$

Proof. 만약 $\zeta^m \neq 1$이라면

$$1 + \zeta^m + \cdots + \zeta^{(n-1)m} = \frac{\zeta^{mn} - 1}{\zeta^m - 1} = \frac{1^m - 1}{\zeta^m - 1} = 0$$

이다. 한편 $\zeta^m = 1$이면

$$1 + \zeta^m + \cdots + \zeta^{(n-1)m} = 1 + 1 + \cdots + 1 = n$$

이다. □

소수 p가 주어졌을 때, 원시근 중 하나를 g라 하면 $g^n \equiv 1 \pmod{p}$인 최소의 n은 $p-1$이다. 따라서 $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$에서 g는 ζ_{p-1}과 같이 행동한다.

연습문제 1.2. 소수 p에 대해

$$1^m + 2^m + \cdots + (p-1)^m$$

을 mod$p$로 계산하여라.

정리 1.3. *소수 p와 $\zeta = \zeta_p$에 대해, 유리수 $a_0, \ldots, a_{n-1}$이*

$$a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{p-1}\zeta^{p-1} = 0$$

을 만족시킬 필요충분조건이 $a_0 = a_1 = \cdots = a_{p-1}$인 것이다.

Date: July 29, 2016.

Proof. 우선 $1+\zeta+\zeta^2+\cdots+\zeta^{p-1}=0$이므로 $a_0=\cdots=a_{p-1}$이면 $a_0+a_1\zeta+\cdots+a_{p-1}\zeta^{p-1}=0$이 될 것이다.

반대로 $a_0+a_1\zeta+\cdots+a_{p-1}\zeta^{p-1}=0$이 성립한다고 가정하자. 이것은 ζ가 다항식 $a_0+a_1X+\cdots+a_{p-1}X^{p-1}$의 근이라는 것과 동치이다. 복소수 ζ를 근으로 갖는 유리계수 다항식들 중 차수가 최소인 다항식 $f_{\min}(X)$를 생각하자. 다른 임의의 $g(\zeta)=0$인 유리계수 다항식 $g(X)$에 대해, f와 g의 최대공약수 $\gcd(f,g)$를 생각하자.[1] 그러면 $a(X)f(X)+b(X)g(X)=\gcd(f,g)(X)$인 유리계수 다항식 a,b가 존재하므로 $\gcd(f,g)$도 ζ를 근으로 갖는다. 다항식 f의 최소성에 의해 $\gcd(f,g)=cf$인 상수 c가 존재해야한다. 따라서 f는 g를 다항식으로서 나누어야만 한다.

이제 $g(X)=X^{p-1}+X^{p-2}+\cdots+1$을 생각하자.

$$g(X+1)=\frac{(X+1)^p-1}{(X+1)-1}=\sum_{i=0}^{p-1}\binom{p}{i+1}X^i$$

이므로 Eisenstein's criterion에 의해 $g(X)$는 기약다항식이다. 위에서 $g(\zeta)=0$이므로 f는 g를 나누어야 한다. 하지만 g는 기약이므로 $f=cg$인 상수 c가 존재해야 한다. 같은 논리를 $h(X)=a_0+a_1X+\cdots+a_{p-1}X^{p-1}$에 적용해보자. 그러면 마찬가지로 f는 h도 나누어야 한다. 두 다항식의 차수 모두 $\deg h=p-1$이고 $\deg f=\deg g=p-1$이므로 $h=c_1g$인 상수 c_1이 존재해야 한다. 따라서 $a_0=a_1=\cdots=a_{p-1}$이다. □

연습문제 1.4 (Fourier inversion formula for finite cyclic groups)**.** 양의 정수 n과 복소수 $\zeta=\zeta_n$가 주어져 있다. 각각의 $0\le k<n$에 대해

$$\hat{a}_k=a_0+a_1\zeta^k+a_2\zeta^{2k}+\cdots+a_{n-1}\zeta^{(n-1)k}$$

을 정의하자. 이때

$$a_k=\frac{1}{n}(\hat{a}_0+\hat{a}_1\zeta^{-k}+\hat{a}_2\zeta^{-2k}+\cdots+\hat{a}_{n-1}\zeta^{-(n-1)k})$$

임을 증명하여라.

연습문제 1.5. 수열 $\{a_i\}_{0\le i<n}$과 $\{b_i\}_{0\le i<n}$에 대해 위와 같이 $\{\hat{a}_i\}$와 $\{\hat{b}_i\}$를 정의하자. 새로운 수열

$$c_i=\sum_{\alpha+\beta\equiv i\,(\mathrm{mod}\ n)}a_\alpha b_\beta$$

와 임의의 $0\le i<n$에 대해 $\hat{c}_i=\hat{a}_i\hat{b}_i$임을 증명하여라.

연습문제 1.6 (Putnam 2015 A3)**.** 다음의 값을 계산하여라:

$$\prod_{a=1}^{2015}\prod_{b=1}^{2015}(1+e^{2\pi iab/2015})$$

[1] 다항식 f와 g의 최대공약수는 f와 g를 동시에 나누며 차수가 최대인 다항식으로 정의된다.

2. Problems

1의 거듭제곱근들을 더했을 때 합이 사라진다는 성질을 이용하면 생성함수에서 특정한 차수를 가지는 항만 뽑아내는 일을 쉽게 할 수 있다.

정리 2.1. *다항식 $p(x) = a_0 + a_1x + \cdots + a_dx^d$가 주어져 있다. 이때*

$$\sum_{0\le i\le d/n} a_{ni}x^{ni} = \frac{1}{n}(p(x) + p(\zeta_n x) + \cdots + p(\zeta_n^{n-1}x))$$

이다.

Proof. 우변을 전개해보면 자명하다. □

이러한 성질을 잘 활용한 대표적인 예시로 디리클레의 정리가 있다. 모든 과정을 엄밀하게 증명하기는 어려우므로, 그 개요만 간단히 살펴보자. 증명을 간단히 하기 위해 $pk + a$꼴의 소수들만 생각할 것이다.

정리 2.2 (Dirichlet)**.** *임의의 소수 p와 p와 서로소인 a에 대해, $pk + a$꼴의 소수가 무한히 많다.*

Proof. 우선 모든 양의 정수는 소수들의 곱으로 유일하게 표현되므로

$$\prod_{q\neq p}\frac{1}{1-q^{-1}} = \prod_{q\neq p}\Big(1+\frac{1}{q}+\frac{1}{q^2}+\cdots\Big) = \sum_{p\nmid n}\frac{1}{n} = \infty$$

이다.

이제 p의 원시근 g를 고정시키자. p와 서로소인 임의의 정수 n에 대해, $g^i \equiv n \pmod p$인 i가 $\bmod p-1$로 유일하게 존재할 것이다. 그 i를 $\log n$으로 표기하자. 그러면 $g^{\log n} \equiv n \pmod p$이고 $\log n + \log m = \log nm$일 것이다.

$\zeta = \zeta_{p-1}$에 대해, $\log n$이 $\bmod p-1$로 잘 정의되었으므로 $\zeta^{\log n}$도 복소수로서 잘 정의된다. 위와 마찬가지로,

$$\prod_{q\neq p}\frac{1}{1-\zeta^{k\log q}q^{-1}} = \prod_{q\neq p}\Big(1+\frac{\zeta^{k\log q}}{q}+\frac{\zeta^{k\log q^2}}{q^2}+\cdots\Big) = \sum_{p\nmid n}\frac{\zeta^{k\log n}}{n}$$

이다. 여기서 $k \not\equiv 0 \pmod{p-1}$라면 우변에는 단위분수들이 무작위적인 방향으로 더해지므로 0이 아닌 상수로 수렴할 것이다.[2] 그려면 양 변에 (진짜)log를 취해

$$\Big|-\sum_{q\neq p}\log\Big(1-\frac{\zeta^{k\log q}}{q}\Big)\Big| < \infty$$

를 얻는다. x가 작을 때 $\log(1+x)\approx x$이므로

$$\Big|\sum_{q\neq p}\frac{\zeta^{k\log q}}{q}\Big| < \infty$$

[2]수렴한다는 것은 Abel sum을 이용하면 엄밀하게 만들 수 있지만, 수렴하는 값이 0이 아니라는 것을 증명하는 것이 까다롭다.

라고도 할 수 있을 것이다. 반면에 $p-1 \mid k$이면

$$\sum_{q \neq p} \frac{1}{q} = \infty$$

이다.

여기서 $q \equiv a \pmod{p-1}$인 소수들만 뽑아내기 위해서 각 식에 $\zeta^{-k \log a}$를 곱해준 뒤 더하자. 그려면

$$\begin{aligned}\sum_{q \equiv a \,(\mathrm{mod}\ p)} \frac{1}{q} &= \frac{1}{p-1} \sum_{k=0}^{p-2} \zeta^{-k \log a} \sum_{q \neq p} \frac{\zeta^{k \log q}}{q} \\ &= \frac{1}{p-1}(\infty + \zeta^{-\log a} c_1 + \zeta^{-2 \log a} c_2 + \cdots + \zeta^{-(p-2) \log a} c_{p-2}) = \infty\end{aligned}$$

이 된다. 따라서 $q \equiv a \pmod{p}$인 소수 q는 무한히 많아야 한다. □

굳이 알고 있어야 할 정리는 아니지만, 이러한 아이디어들이 문제들에서 종종 사용되는 경우가 있으니 눈여겨볼만 하다. 이제 실제로 올림피아드에 출제되는 문제들을 풀어보자.

연습문제 2.3. 임의의 양의 정수 n에 대해

(a) $\binom{2n}{0} + \binom{2n}{2} + \binom{2n}{4} + \cdots + \binom{2n}{2n}$의 값을 구하여라.

(b) $\binom{3n+1}{2} + \binom{3n+1}{5} + \binom{3n+1}{8} + \cdots + \binom{3n+1}{3n-1}$의 값을 구하여라.

연습문제 2.4. 양의 정수 a, b, n에 대해, $a \times b$ 크기의 직사각형이 $1 \times n$ 크기의 직사각형들로 분할될 수 있다고 한다. 이때 $n \mid a$이거나 $n \mid b$임을 증명하여라.

연습문제 2.5 (USAMO 1976 5)**.** 다항식 P, Q, R, S가

$$P(x^5) + xQ(x^5) + x^2 R(x^5) = (x^4 + x^3 + x^2 + x + 1) S(x)$$

을 만족시킨다고 할 때, $x-1$이 $P(x)$를 나눔을 증명하여라.

연습문제 2.6 (Leningrad 1991)**.** 유한수열 $\{a_1, \ldots, a_n\}$에 대해, 모든 $1 \leq k \leq p$에 대해

$$s(k,p) = a_k + a_{k+p} + a_{k+2p} + \ldots$$

의 값이 같다면, 수열 $\{a_i\}$를 *p-balanced*라 하자. 만약 길이 50이 수열이 $3, 5, 7, 11, 13, 17$-balanced라면, 모든 항이 0이어야 함을 증명하여라.

연습문제 2.7 (IMO Shortlist 2002 N5)**.** 양의 정수 $m, n \geq 2$와 m^{n-1}의 배수가 아닌 정수 $a_1, \ldots, a_n$이 있다. 이때 모두 0은 아니며 $|e_i| < m$인 정수 $e_1, \ldots, e_n$이 존재하여 $e_1 a_1 + e_2 a_2 + \cdots + e_n a_n$이 m^n의 배수가 됨을 증명하여라.

연습문제 2.8 (IMO Shortlist 2007 C3)**.** 양의 정수들 $1, 2, \ldots, n$이 빨강 또는 파랑으로 색칠되어 있다. 수들 x, y, z가 같은 색으로 이루어져 있으며 $n \mid x + y + z$인 순서쌍 (x, y, z)의 개수가 2007이라고 할 때, 가능한 n의 값을 모두 구하여라.

연습문제 2.9 (Kömal B.4401)**.** 소수 $p = 3n + 1$에 대해 $1^3, 2^3, \ldots, n^3$을 p로 나눈 나머지들이 모두 다를 수 있는가?

연습문제 2.10 (Vietnam TST 2008 6)**.** 집합 $M = \{1, 2, \ldots, n\}$의 각 원소는 빨강, 노랑, 파랑 중 하나로 색칠되어 있다. 두 집합

$$S_1 = \{(x, y, z) \in M^3 : x, y, z\text{는 서로 같은 색으로 칠해져 있으며 } n \mid x + y + z\}$$
$$S_2 = \{(x, y, z) \in M^3 : x, y, z\text{는 서로 다른 색으로 칠해져 있으며 } n \mid x + y + z\}$$

을 정의하자. 이때 $2|S_1| \geq |S_2|$임을 증명하여라.

연습문제 2.11 (IMO 1995 6)**.** 홀수인 소수 p에 대해, 집합 $\{1, 2, \ldots, 2p\}$의 부분집합들 중 원소의 개수가 p이고 원소의 합이 p의 배수인 것의 개수를 구하여라.

연습문제 2.12 (IMO Shortlist 1999 C7)**.** 소수 $p > 3$이 있다. 공집합이 아닌 임의의 부분집합 $T \subset \{0, 1, \ldots, p-1\}$에 대해,

$$E(T) = \{(x_1, \ldots, x_{p-1}) : x_1, \ldots, x_{p-1} \in T,\ p \mid x_1 + 2x_2 + \cdots + (p-1)x_{p-1}\}$$

을 정의하자. 이때, $|E(\{0, 1, 2\})| \leq |E(\{0, 1, 3\})|$이며 등호가 성립할 필요충분조건은 $p = 5$임을 증명하여라.

연습문제 2.13 (Miklós Schweitzer 1991 2)**.** 단위원 위에 n개의 점이 놓여있어 그 위의 임의의 점에서 n개의 점들까지의 거리의 곱이 항상 2 이하라 한다. 이때 n개의 점들은 정n각형을 이루어야 함을 증명하여라.

연습문제 2.14 (Saint-Petersburg 2003)**.** 소수 p, 정수 $n \geq p$와 $a_1, \ldots, a_n$이 있다. 각각의 $0 \leq k \leq n$에 대해, $\{1, \ldots, n\}$의 크기 k 부분집합들 $\{s_1, \ldots, s_k\}$ 중 $p \mid a_{s_1} + \cdots + a_{s_k}$인 것들의 개수라 하자. 이때

$$p \mid f_0 - f_1 + f_2 - f_3 + \cdots + (-1)^n f_n$$

임을 증명하여라. (여기서 $f_0 = 1$이다.)

연습문제 2.15 (Chevalley-Warning theorem)**.** 양의 정수 n와 $x_1, \ldots, x_n$을 변수로 가지는 정수계수 다항식 $f_1, \ldots, f_m$이 있다. 만약 $\deg f_1 + \cdots + \deg f_m < n$이라면,[3]

$$\begin{cases} f_1(x_1, \ldots, x_n) \equiv 0 \pmod{p} \\ \quad \vdots \\ f_m(x_1, \ldots, x_n) \equiv 0 \pmod{p} \end{cases}$$

를 동시에 만족시키는 $(x_1, \ldots, x_n) \in \{0, \ldots, p-1\}^n$의 개수가 p의 배수임을 증명하여라.

[3]여기서 deg는 항들 중 차수의 합의 최댓값으로 정의된다. 예를 들어 $\deg(x_1 + x_2^3 + x_1^2 x_3^2) = 4$이다.

연습문제 2.16 (Zhang, 1989)**.** 정수 $a_1, \ldots, a_n$과 양의 정수 $d_1, \ldots, d_n$이 있다. 임의의 x에 대해 $x \equiv a_i \pmod{d_i}$인 i가 존재한다고 할 때, 어떤 $1 \leq i_1 < \cdots < i_k \leq n$가 존재하여 $1/d_{i_1} + \cdots + 1/d_{i_k}$가 정수가 됨을 증명하여라.

연습문제 2.17 (IMO Shortlist 2012 N8)**.** 임의의 소수 $p > 100$과 정수 r에 대해, p가 $a^2 + b^5 - r$을 나누게 되는 정수 a와 b가 존재함을 증명하여라.