수론 1 정수의 기본개념과 응용

$\mathbb{N}$: 자연수의 집합
$\mathbb{Z}$: 정수의 집합
$\mathbb{Q}$: 유리수의 집합
$\mathbb{R}$: 실수의 집합
$X^+ = \{x \in X \mid x > 0\}$
$X^- = \{x \in X \mid x < 0\}$

· $\mathbb{N}$의 정렬성

$\mathbb{N} \supset S$ 인 어떤(∀) S 에서도 S는 $\emptyset$ 또는 최소원소가 존재한다.

· 수학적 귀납법의 원리

$S \subset \mathbb{N}$ 에서

$\begin{cases} ① \ 1 \in S \\ ② \ n \in S \Rightarrow n+1 \in S \end{cases}$ 이면

$\Longrightarrow \quad S = \mathbb{N}$

· 정리 $a, b \in \mathbb{N}$ 이면

$a = bq + r$, $q \geq 0$
$0 \leq r < b$

인 정수 q, r 이 있다

그리고 이 q, r은 유일하다.

pf.) $X = \{a - b\cdot 0,\ a - b\cdot 1,\ a - b\cdot 2, \cdots\}$

i) $0 \notin X$ 일때 $X^+ = S \Rightarrow a = a - b\cdot 0$ $S \neq \emptyset$

∴ $X^+ \subset \mathbb{N}$ 이므로 자연수집합의 정렬성에 의해 최소원소가 존재.

S의 가장작은 원소를 r 이라고 하자

$r > 0$

만약 $r \geq b$ 이면 $r - b \in X^+$ 이나 '최소'에 모순

∴ $0 < r < b$

$a - bq = r$

ii) $0 \in X$ 일때 $a = bq$꼴

i) ii) 에서 $a = bq + r$ 인 q, r 존재 $0 \leq r < b$

만일 $a = bq + r$

$a = bq' + r'$ $\quad r, r' \in [0, b)$

이때

$b(q - q') = r' - r$

$-b < r' - r < b$

$-b < b(q - q') < b$

∴ $q' = q$ ∴ $r = r'$

$q = q'$

(모든 문자는 정수로 하자)

- 기호의 정의

$a, b \in \mathbb{Z}$

만일 $b = ac$, $c \in \mathbb{Z}$ 이면

b는 a의 배수이며

a는 b의 약수라고 한다.

기호 : $a \mid b$

○ $n > 1$ 이 합성수 $\Longrightarrow$ $n = ab$ ($1 < a, b < n$) 꼴로 표시 가능하다

- $n \in \mathbb{N} \Rightarrow$ $n = 1$ 이거나
  $n =$ 소수 이거나
  $n =$ 합성수 $\Rightarrow n = ab$ .....
  ∴ ↳ 소수들의 유한 개의 곱으로 표시가능

○ 정리: 소수는 무한히 많다. (유클리드)

p.f) 소수가 유한개라 가정하자.

그것들을 $p_1, p_2, p_3, \cdots, p_n$ 라 하자.

이때 $A = p_1 p_2 p_3 \cdots p_n + 1$ 라 하면

A는 소수이거나 소수의 곱이다

i) 소수라면 : $A \neq p_1, p_2, \cdots, p_n$ 중 어느 것과도 같지 않으므로 모순

ii) 소수의 곱이라면

어떤 소수 p_j 로 나누어도 1이 남으므로 소수의 곱이 아니다 ⇒ 모순

∴ 소수는 무한개이다

Ex) $4k+3$ 꼴의 소수는 무한히 많다

p.f) $4k+3$ 꼴소수가 무한이 아니라 하자.

그것을 $p_1, p_2, \cdots, p_n$ 라 하자.

이때 $A = 4p_1 p_2 \cdots p_n - 1$ 라 하면

A는 소수 또는 합성수이다

i) 소수라면 : $A \neq p_j$ 인데 A가 $4k+3$ 꼴 $\rightarrow$ 모순

ii) 합성수라면

① A가 $4k+3$ 꼴 소인수를 가진다면

이것은 $p_1, p_2, \cdots, p_n$ 어느것도 아니므로 모순

② A가 $4k+3$ 꼴 소인수를 가지지 않는다면

A는 $4k+1$ 꼴 소인수만 가진다

그러면 A는 4로 나눠 나머지 1이 되므로 모순

∴ $4k+3$ 꼴 소수는 유한개가 아니다

· 정의 $n! = 1 \cdot 2 \cdot 3 \cdots n$, $0! = 1$
↑ factorial

· Ex) $150!+2$
$150!+3$
$150!+4$
$\vdots$
$150!+150$
} 합성수 (연속된 많은 수들이 합성수) → 소수들사이 gap은 얼마든지 커질수 있다.

○ $a, b \in \mathbb{Z}$ 에서
c가 a와 b의 공약수 $\Leftrightarrow$ $c|a$ .. $c|b$
$-|a|, -|b| \le c \le |a|, |b|$
만일 a,b 의 공약수가 ±1 뿐이면 a,b를 서로소라 한다.

○ $a, b \in \mathbb{Z} - \{0\}$ 에서
$X = \{ ax+by \mid x, y \in \mathbb{Z} \}$ 라 하자
$\begin{cases} 0 \in X \\ X^+ \neq \emptyset. \rightarrow X^+ \text{에는 최소원소 } g \text{가 있다.} \end{cases}$

* $\begin{cases} g = \gcd(a,b) \\ X = \{ x \mid x \text{는 } g \text{의 배수} \} \end{cases}$

p.f) 일단 X의 모든 원소는 $\gcd(a,b)$로 나누어짐이 명백하다.
즉 $X \subset \{ x \mid x \text{는 } \gcd(a,b) \text{의 배수} \}$ ..... ①
$\gcd(a,b) \in X$ 임을 보이면 된다 → (뒷페이지 유클리드호제법)
만일 그렇다면 $\gcd(a,b) = ax_0 + by_0$
$\gcd(a,b)$의 배수 $= (ax_0+by_0)k$
$= a(x_0k) + b(y_0k)$
$\therefore g = ax_0 + by_0$
a를 g로 나누어보면
$a = gq + r$
$r = a - gq = a(1-x_0q) + b(-y_0q)$ 이니
$r \in X$. 그런데 $0 \le r < g$ 에서
$r \neq 0$ 이면 $r \in X^+$ → g가 최소라는데 모순
$\therefore r = 0$
$\therefore a$는 g의 배수이다
마찬가지로 b는 g의 배수이다

◦ 유클리드의 호제법

$a, b \in \mathbb{N}$

$a = bq + r \qquad q, r \in \mathbb{Z}$

$\gcd(a,b) = \gcd(b,r)$

p.f) 만일 c가 a, b의 공약수라면
c는 b, r의 공약수.

또 c가 b, r의 공약수라면 · c는 a, b의 공약수.

∴ (a, b공약수 집합) = (b, r 공약수 집합)

$a = bq + r$

$b = rq_1 + r_1$

$r = r_1 q_2 + r_2$

$r_1 = r_2 q_3 + r_3$

$\vdots$

$r_{k-2} = r_{k-1} q_k + r_k$

$r_{k-1} = r_k q_{k+1} + 0$

$\gcd(a,b) = \gcd(b,r)$
$= \gcd(r, r_1)$
$= \cdots = \gcd(r_{k-1}, r_k) = r_k$

⟹ 거꾸로 올라가면 $\gcd(a,b) = ax + by$ 로 표현 가능하다

◦ $a = 7,\ b = 5$

$7 = 5 \cdot 1 + 2$

$5 = 2 \cdot 2 + 1$

$2 = 1 \cdot 2 + 0$

양변을 $\frac{\text{큰수}}{\text{작은수}}$로 나눈다 →

$\frac{7}{5} = 1 + \frac{2}{5}$

$= 1 + \frac{1}{\frac{5}{2}}$

$= 1 + \frac{1}{2 + \frac{1}{2}}$: 연분수

예) $\frac{56}{22} = 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{5}}}$

· p: 소수 $p \mid ab \Longrightarrow p \mid a$ or $p \mid b$

p.f) 만일 $p \nmid a$ 라면

$\gcd(p, a) = 1 = ax + py$

$b = (ab)x + p(by)$

$p \mid ab$, $p \mid p$ 이므로 ∴ $p \mid b$

· 소인수분해의 유일성

$p_1 p_2 p_3 \cdots p_m = q_1 q_2 \cdots q_n$ (p_i, q_i : 소수들) 라면

$p_1 \mid (q_1 q_2 \cdots q_n)$

∴ $p_1 \mid q_1$ 이거나 $p_1 \mid q_2 q_3 \cdots q_n$

$\vdots$

$p_i \mid q_j$ 꼴 ⟹ $p_i = q_j$ ∴ 소인수분해를 하면 나타나는 소수는 유일.

· 합동 (Gauss)

(기호) $a \equiv b \pmod n \iff n \mid (a-b)$

그래서 (동치조건)
- $a \equiv a \pmod n$
- $a \equiv b \pmod n \iff b \equiv a \pmod n$
- $a \equiv b \pmod n,\ b \equiv c \pmod n \implies a \equiv c \pmod n$

$a \equiv b \pmod n$, $c \equiv d \pmod n$ $\implies$ $a \pm c \equiv b \pm d \pmod n$, $ac \equiv bd \pmod n$

· 잉여계 (mod n) :

ex) (mod 5)에서 $\{0,1,2,3,4\}$

$\{-2,-1,0,1,2\}$

EX) $a^2+b^2-8c=6$ 의 정수해가 없다

sol.) (mod 8)로 보면 $a^2+b^2 \equiv 6 \pmod 8$

그런데 어떤 정수를 제곱하면 (mod 8)로 0,1,4만 나온다.

(mod 8)

b^2 \ a^2	0	1	4
0	0	1	4
1	1	2	5
4	4	5	0

∴ 6과 합동일 수 없다

· $ac \equiv ab \pmod n \not\Rightarrow b \equiv c \pmod n$

반례) $3 \cdot 2 \equiv 3 \cdot 4 \pmod 6$

$\not\Rightarrow 2 \not\equiv 4 \pmod 6$

◦ 일차합동식과 일차부정방정식

· (실제로 같다) <
- 일차합동식 : $ax \equiv c \pmod b$
- 일차부정방정식 : $ax+by=c$

$(a,b,c$: 상수)

근을 가진다 $\iff \gcd(a,b) \mid c$

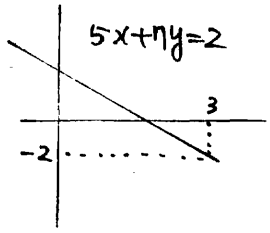
ex) $15x+21y=6$

$5x+7y=2$

호제법에서 $\gcd(5,7)=1=5x_0+7y_0$

$2=5(2x_0)+7(2y_0)$

$2=5(2x_0+7t)+7(2y_0-5t)$

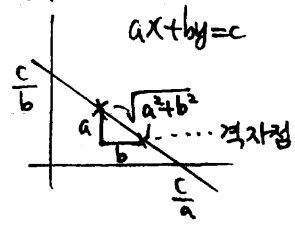


$x_0=3,\ y_0=-2$

∴ $2=5(6+7t)+7(-4-5t)$

$\begin{cases} x=6+7t \\ y=-4-5t \end{cases}$

· 양의 정수해 존재정리



◦ 중국인의 나머지 정리

ex) $\begin{cases} x\equiv 1 \pmod 5 \\ x\equiv 3 \pmod 7 \end{cases} \Rightarrow x=31,\ 31+5\cdot 7,\ 31+5\cdot 7\cdot k\ \cdots$

$\Rightarrow x\equiv 31 \pmod{35}$

역의 $x\equiv 31 \pmod{35}$ 이라면 $\Rightarrow \begin{cases} x\equiv 1 \pmod 5 \\ x\equiv 3 \pmod 7 \end{cases}$ 이고

·중국인의 나머지정리

$x\equiv a_1 \pmod{n_1}$

$\vdots$

$x\equiv a_k \pmod{n_k}$

이고 $\gcd(n_i, n_j)=1$ $(i\neq j)$

$\Longrightarrow$ 이 연립합동식을 풀 수 있다

ex) $\begin{cases} x\equiv 1 \pmod 5 \\ x\equiv 3 \pmod 7 \\ x\equiv 4 \pmod{11} \end{cases}$

·해가 없는 예 (서로소가 아님)

$\begin{cases} x\equiv 1 \pmod 6 \\ x\equiv 2 \pmod 4 \end{cases} \Rightarrow \begin{cases} x\equiv 1 \pmod 3 \\ x\equiv 2 \pmod 3 \end{cases}$

∴해가 없다

sol.) $\begin{cases} x\equiv 1 \pmod 5 \\ x\equiv 0 \pmod 7 \\ x\equiv 0 \pmod{11} \end{cases}$ 인 x는?

$x=77k\equiv 1 \pmod 5$ $\quad k=3$

$\therefore \begin{cases} 77\cdot 3\equiv 1 \pmod 5 \\ 77\cdot 3\equiv 0 \pmod 7 \\ 77\cdot 3\equiv 0 \pmod{11} \end{cases}$

마찬가지로 $\begin{cases} 55\cdot 6\equiv 0 \pmod 5 \\ 55\cdot 6\equiv 1 \pmod 7 \\ 55\cdot 6\equiv 0 \pmod{11} \end{cases}$

$\begin{cases} 35\cdot 6\equiv 0 \pmod 5 \\ 35\cdot 6\equiv 0 \pmod 7 \\ 35\cdot 6\equiv 1 \pmod{11} \end{cases}$

∴ 하나의 해 $x=(77\cdot 3)+3(55\cdot 6)+4(35\times 6)$

다른해는 모든 $x\equiv(77\cdot 3)+3\cdot(55\cdot 6)+4(35\cdot 6) \pmod{5\cdot 7\cdot 11}$

- $ax \equiv 1 \pmod n \iff ax+ny=1$
  $\gcd(a,n)=1$ 때 해가 존재. (동치)

ex) $2x \equiv 1 \pmod 6$: 해가 없다.
$5x \equiv 1 \pmod 6$ 해 $x \equiv -1 \pmod 6$

그런데 n이 소수일때 즉 $n=p$ 일때
$ax \equiv 1 \pmod p$
$p \nmid a$ 이면 (즉 $a \not\equiv 0 \pmod p$)
항상 해가 존재.

ex) $x^2-1 \equiv 0 \pmod{15}$: $xy \equiv 0 \pmod p$ 라면 $x \equiv 0$ or $y \equiv 0 \pmod p$
$\Rightarrow x \equiv \pm 1, \pm 4 \pmod{15}$
(15 합성수) 차수보다 근이 많다

ex) $x^2-1 \equiv 0 \pmod p$
$(x-1)(x+1) \equiv 0 \pmod p$
$x \equiv \pm 1 \pmod p$

- 윌슨의 정리
p : 소수
$(p-1)! \equiv -1 \pmod p$
혹은 $(p-2)! \equiv 1 \pmod p$

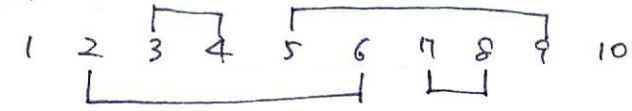
$1! \equiv -1 \pmod 2$
예) $2! \equiv -1 \pmod 3$
$3! \equiv X$ (4는 소수 X)
$4! \equiv 24 \equiv -1 \pmod 5$

증명) i) $p=2$인 경우 명백
ii) p가 홀수인 소수인 경우
$\{ 1, 2, 3, \cdots, p-2, p-1 \}$: 모두 p와 서로소
1 ↓ 곱셈의 결과와 무관
둘씩 쌍을 지어 곱하면 1

∵ $ax \equiv 1 \pmod p$ 에서 항상 해가 있다
이때 $a \equiv x$ 인 경우는 위 ex처럼 $a \equiv 1, p-1 \pmod p$ 인 경우뿐이다

$\therefore (p-1)! \equiv p-1 \equiv -1 \pmod p$

예) $p=11$



ex) $x^2 \equiv -1 \pmod{p=17}$ $x \equiv \pm 4 \pmod{17}$

이제 $p=4k+1$ 꼴이라고 하자. ($2k$: 짝수개)

$(p-1)! \equiv 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \frac{p+3}{2} \cdots (p-1) \equiv (-1) \pmod p$
$\equiv 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p-1}{2} \cdot \frac{p-3}{2} \cdots (1) \equiv (-1) \pmod p$
$\equiv \left[\left(\frac{p-1}{2} \right)! \right]^2 \equiv -1 \pmod p$

$\frac{p+1}{2} \equiv -\frac{p-1}{2}$
$\frac{p+3}{2} \equiv -\frac{p-3}{2}$
⋮ } $2k$개
$\times$) $p-1 \equiv -1$

$\frac{p+1}{2} \cdot \frac{p+3}{2} \cdots (p-1) \equiv \left(\frac{p-1}{2} \right)!$

$\therefore \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod p$

$p: 4k+1$ 꼴 소수

ex) $\left[\left(\frac{17-1}{2}\right)!\right]^2 \equiv -1 \pmod{17}$

$\left[\left(\frac{5-1}{2}\right)!\right]^2 \equiv (2!)^2 \equiv -1 \pmod 5$

◦ 페르마의 정리

p: 소수

$\gcd(a,p)=1$ 이면 $\quad a^{p-1} \equiv 1 \pmod p$

ex) $3^2 \equiv 2 \pmod 7$

$3^4 \equiv 4 \pmod 7$

$3^6 \equiv 8 \equiv 1 \pmod 7$

(증명) $f: \{1,2,3,\cdots,p-1\} \longrightarrow \{1,2,\cdots,p-1\}$

$\vee$

$x \longrightarrow (ax$ 와 합동인 수$)$

$y \longrightarrow (ay$ 와 합동인 수$)$

$ax \equiv ay \pmod p$ 라면

$ac \equiv 1 \pmod p$ 인 c가 존재하므로

$acx \equiv acy \pmod p$

$x \equiv y \pmod p \quad \therefore x=y$

즉 f는 단사함수 이다.

특히 전단사함수 (일대일대응) 이 된다.

($\because$ 역원소수 = 공역원소수)

$1\cdot 2\cdot 3\cdots(p-1) \equiv (a\cdot 1)(a\cdot 2)\cdots(a\cdot(p-1)) \pmod p$

$(p-1)! \equiv a^{p-1}(p-1)! \pmod p$

$1 \equiv a^{p-1} \pmod p$

◦ 오일러의 정리

$\gcd(a,n)=1. \quad a^{\phi(n)} \equiv 1 \pmod n$

(증명) $f: \{x \mid 0 \le x \le n-1, (x,n)=1\} \longrightarrow \{x \mid 0 \le x \le n-1, (x,n)=1\}$

에서 원소의 개수는 $\phi(n)$ 이다

페르마의 정리 증명처럼 하면

$a^{\phi(n)} \equiv 1 \pmod n$

ex) $3^{1993} \equiv 3^{6\times 330+13} \pmod 7$
$\equiv 3^{6\times 2+1} \pmod 7$ $\because 3^6 \equiv 1 \pmod 7$
$\equiv 3 \pmod 7$

Ex① ((4444^4444의 자리수의 합)의 자리수의 합)의 자리수의 합 ?

Hint: 자리수의 합 ↳ (mod 9)

(정의) p가 소수이면 적당한 a가 있어서
$\{0, a, a^2, a^3, \cdots, a^{p-1}\}$ 이 잉여계이다.
이런 a를 '원시근'이라고 한다.

ex) mod 7에서 원시근은 3, 5
나머지는 원시근이 아니다.

• p: 소수 (a,p)=1 인 때
$ax \equiv b \pmod p$
$a^{p-1}x \equiv a^{p-2}b \pmod p$ ↙ Fermat의 정리
$x \equiv a^{p-2}b \pmod p$

◦ p: 소수 (a,p)=1 일 때
$a^{p-1} \equiv 1 \pmod p$ 이므로
$a, a^2, a^3, \cdots, a^r, \cdots$ 에는 1과 합동인 수가 존재한다. (mod p)
그중 제일 작은 수를 a^r 라 하면
r을 'a의 위수' (mod p) 라 부른다.

(정리) 위수는 항상 p-1의 약수이다 (mod p)
(증명) r = (p-1) = r·q + 나머지
$a^{\text{나머지}} \equiv a^{p-1-rq} \pmod p$
$\equiv a^{p-1}\cdot(a^r)^{-q} \pmod p$
$\equiv 1 \pmod p$
그런데 위수는 최소인 것이라 하였으니
나머지가 0이 아니라면 최소라는 것에 모순!
∴ 나머지 = 0
즉 $r \mid (p-1)$

· 순환소수

$\frac{1}{9} = 0.1111\cdots = 0.\dot{1}$

$$\frac{1}{10-1} = \frac{1}{10}\left(\frac{1}{1-\frac{1}{10}}\right)$$

$$= \frac{1}{10}\left(1+\frac{1}{10}+\frac{1}{10^2}+\cdots\right)$$

$$= \frac{1}{10}+\frac{1}{10^2}+\frac{1}{10^3}+\cdots$$

$$= 0.1111\cdots$$

· $\frac{1}{23}$ 을 순환소수로 표현

배라는 것 : $10^x - 1 \equiv$ (23의 배수)

$10^x \equiv 1 \pmod{23}$

그중 최소인것을 찾으려니까, x는 10의 위수

$\therefore x \mid 22$

$x = 1, 2, 11, 22$ 중 하나

계산해보면 $x = 22$

$$\therefore \frac{1}{23} = \frac{k}{23k}$$

$$= \frac{k}{10^{22}-1}$$

$$= \frac{k}{10^{22}}\left(\frac{1}{1-\frac{1}{10^{22}}}\right)$$

$$= \frac{k}{10^{22}}+\frac{k}{10^{44}}+\frac{k}{10^{66}}+\cdots$$

주기 : 22 (10 의 위수 (mod 23))

$0.\underbrace{\overline{a_1 a_2 \cdots a_{22}}}_{k}$

(10진법)

· 순환소수의 주기 (mod 분모) 에서 10의 위수

· 분모에 2, 5 의 소인수가 있다면 10의 위수가 존재하지 않으므로 순환되지 않는다.

· 2차합동식 $ax^2+bx+c \equiv 0 \pmod{n}$

$4a^2x^2+4abx+4ac \equiv 0 \pmod{n}$

$(2ax+b)^2+4ac-b^2 \equiv 0 \pmod{n}$

$t^2 \equiv b^2-4ac \pmod{n}$

결국 $x^2 \equiv a \pmod m$ 으로 귀착된다.

만일 $m = p_1 p_2 \cdots p_k$ 라면 ($p_1, p_2, \cdots, p_k$ 는 서로다른 소수의 곱)

$$\begin{cases} x^2 \equiv a \pmod{p_1} \\ \vdots \\ x^2 \equiv a \pmod{p_k} \end{cases}$$

여기서는 $x^2 \equiv a \pmod p$ 을 구할수 있으면 해를 구할수있다.

g : 원시근 이라 하자 (p가 소수이니 반드시 존재)

$a \equiv g^i \pmod p$ 인 i가 존재.

그러면 $x^2 \equiv g^i \pmod p$

이때 i가 짝수여야 해가 있다

즉 해가있다 $\iff$ i가 짝수

그런데 i가 짝수이면

$g^{p-1} \equiv g^{2\cdot\frac{p-1}{2}} \equiv 1 \pmod p$ 니까

$a = g^i$

$(g^i)^{\frac{p-1}{2}} \equiv 1 \pmod p$ ($\because i$: 짝수)

$\therefore i$가 짝수 $\iff a^{\frac{p-1}{2}} \equiv 1 \pmod p$ ($\because$ 판정법)

$a = g^i$

$x^2 \equiv a \pmod p$ a가 p가 근이 있다면

$a^{\frac{p-1}{2}} \equiv 1 \pmod p$

$p = 4k+3$ 꼴이라면

$$\left(a^{\frac{p+1}{4}}\right)^2 \equiv a^{\frac{p+1}{2}} \equiv a^{\frac{p-1}{2}+1} \equiv a \pmod p$$

ex) $p = 23$ $a = 7$

이때

$$\left(7^{\frac{24}{4}}\right)^2 \equiv 7 \pmod{23}$$

즉 7^6은 $X^2 \equiv 7 \pmod{23}$의 근이다.

Hint : 원순의 정리 사용

ex② $p = 4k+1$ 꼴일때 $x^2 \equiv a \pmod p$ 의 근을 구해보라

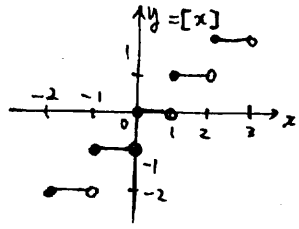
morning glory

정수론적 함수
(산술함수)

- 가우스 함수 $x \in \mathbb{R}$. 일때

x를 넘지 않는 최대의 정수값을 $[x]$로 표현한다.

$[2.1]=2 \quad [\pi]=3 \quad [-4.2]=-5$



$m \in \mathbb{Z}$일때 $\Leftrightarrow [m]=m$

○성질 (1) $[x] \le x < [x]+1$

(2) $m \in \mathbb{Z}$ 이면

$[m+x] = m+[x]$

(증명) $x=[x]+u \quad , \quad 0 \le u < 1$ 라 두자. (성질 (1)에 의해)

$m+x = m+[x]+u$

$\underbrace{m+[x]}_{\text{정수}} \le m+x < m+[x]+1$

$\therefore [m+x] = m+[x]$ (by 정의)

(3) $[x]+[y] \le [x+y] \le [x]+[y]+1$

(증명) $x = [x]+u, \quad 0 \le u < 1$

$y = [y]+v, \quad 0 \le v < 1$

$x+y = [x]+[y]+u+v$

$[x+y]$

$= [[x]+[y]+u+v]$

$= [x]+[y]+[u+v]$ (성질 (2))

$[u+v]=0$ or 1 이므로

$[x]+[y] \le [x+y] \le [x]+[y]+1$

(4) $[x][y] \le [xy] \quad , \quad x, y \ge 0$

(증명) $x=[x]+u \quad , \quad 0 \le u < 1$

$y=[y]+v \quad , \quad 0 \le v < 1$

$xy = [x][y]+v[x]+u[y]+uv$

$[xy] = [[x][y]+v[x]+u[y]+uv]$

$= [x][y] + [v[x]+u[y]+uv]$

$\ge [x][y]$

(5) $[x]+[-x] = \begin{cases} 0 & (x \in \mathbb{Z}) \\ -1 & (x \notin \mathbb{Z}) \end{cases}$

(증명) i) $x \in \mathbb{Z}$인 경우 $[x]=x, \ [-x]=-x$ 이므로 성립

ii) $x \notin \mathbb{Z}$인 경우 $x=[x]+u \quad , \quad 0<u<1$ 로 두자

$-x = -[x]+(-u)$

$-x = -[x]-1+(1-u)$

$$[-x] = [-[x]+(-1)+(1-u)]$$
$$= -[x]-1+[1-u] \qquad 0<1-u<1$$
$$= -[x]-1$$
$$\therefore [x]+[-x]=-1. \qquad x\notin\mathbb{Z}$$

(6) $x\in\mathbb{R}$, $m\in\mathbb{Z}^+$ 일때

$$\left[\frac{[x]}{m}\right]=\left[\frac{x}{m}\right]$$

(증명) $[x]=qm+r \qquad 0\le r\le m-1$ 로 두자

$$x=[x]+u \qquad 0\le u<1$$
$$= qm+r+u$$
$$\frac{x}{m} = q+\frac{r}{m}+\frac{u}{m}$$

정수 ↑

$$\begin{cases} 0\le\frac{r}{m}<1-\frac{1}{m} \\ 0\le\frac{u}{m}<\frac{1}{m} \end{cases}$$
$$0\le\frac{r}{m}+\frac{u}{m}<1$$
$$\therefore \left[\frac{x}{m}\right]=q=\left[\frac{[x]}{m}\right]$$

(7) $m,n>0$ 정수 일때

$\left[\frac{m}{n}\right]$ 은 m을 n으로 나눌때 몫.

ie. $m=qn+r \qquad 0\le r\le n-1$

$$m=\left[\frac{m}{n}\right]n+r$$

④ $1,2,3,\cdots,m$ 까지 수중 n의 배수의 갯수.

(8) $-[-x]=x$보다 작지 않은 최소의 정수

(9) $[x+\frac{1}{2}]=x$에서 가장 가까운 정수값. 거리가 같은경우 더 작은 쪽.

(10) $-[-x+\frac{1}{2}]=x$에서 가장 가까운 정수값. 거리가 같은경우 더 큰 쪽.

드뽈리낙 (정리) (de Polignac 의 공식)

n이 자연수일때 $n!$의 소인수 p의 지수는

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\cdots = \sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right]$$

(사실상 유한개의 합이다.)

pf 1) n에 대한 수학적 귀납법사용

$n=1$: 당연히 성립

$n=k$ 일때 성립한다면

$$(k+1)! = (k+1)\,k!$$
$$\left[\frac{k}{p}\right]+\left[\frac{k}{p^2}\right]+\cdots+\cdots$$
$$\vdots$$

pf 2) $n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdots n$

이 중 우리는 소수 p의 지수만 생각하므로

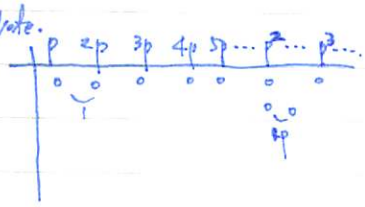
$p \cdot 2p \cdot 3p \cdots \left[\frac{n}{p}\right]p$ 개수 : $\left[\frac{n}{p}\right]$

$1 \cdot 2 \cdot 3 \cdots \left[\frac{n}{p}\right]$ 에서 p의 배수 개수 : $\left[\frac{\left[\frac{n}{p}\right]}{p}\right]$

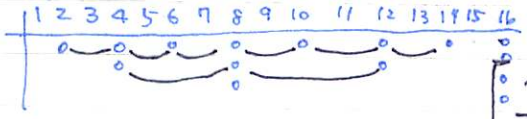
또 p^2을 지우면

$\left[\frac{\left[\frac{n}{p}\right]}{p}\right]!$ 에서 곱중 p의 배수 개수: $\left[\frac{\left[\frac{\left[\frac{n}{p}\right]}{p}\right]}{p}\right]$

Note.



예 $p=2$



$$\left[\frac{n}{p}\right] - \left[\frac{\left[\frac{n}{p}\right]}{p}\right] + \left[\frac{\left[\frac{\left[\frac{n}{p}\right]}{p}\right]}{p}\right] + \cdots$$

$$= \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

p : 소수

$p^\alpha \| a$

$\Leftrightarrow p^\alpha | a$ and $p^{\alpha+1} \nmid a$

EX) $n, k \in \mathbb{Z}$ 일때

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$$ 가 정수임을 보여라.

sol.) 임의의 소수 p에 대해 분자의 p의 지수가 분모의 p의 지수 보다 크거나 같음을 보이자.

분자: $\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$

분모: $\left[\frac{k}{p}\right] + \left[\frac{k}{p^2}\right] + \left[\frac{k}{p^3}\right] + \cdots$

$+ \left[\frac{n-k}{p}\right] + \left[\frac{n-k}{p^2}\right] + \left[\frac{n-k}{p^3}\right] + \cdots$

$[x+y] \geq [x]+[y]$

∴ 분자 의 p의 지수 $\geq$ 분모의 p의 지수

EX) 다항계수 $\frac{n!}{r_1!\,r_2! \cdots r_\ell!}$ (단 $r_1+r_2+\cdots+r_\ell = n$) 은 항상 정수이다.

여기서 $n, r_1, r_2, \cdots, r_\ell$은 정수.

EX , $1000!$ 에서 7의 지수는?

sol, $\left[\frac{1000}{7}\right] + \left[\frac{1000}{7^2}\right] + \left[\frac{1000}{7^3}\right] + \cdots$

$\left[\frac{1000}{7}\right] = 142$

$\left[\frac{1000}{7^2}\right] = \left[\frac{142}{7}\right] = 20$

$\left[\frac{1000}{7^3}\right] = \left[\frac{20}{7}\right] = 2$

∴ $142+20+2$

$= 164$ 개

EX) $a, b \in \mathbb{N}$ 이면

$\dfrac{(ab)!}{(a!)^b\, b!}$ 은 정수임을 보여라.

sol, p가 소수일때

분자의 p의 지수는

$$\left[\frac{ab}{p}\right]+\left[\frac{ab}{p^2}\right]+\left[\frac{ab}{p^3}\right]+\left[\frac{ab}{p^4}\right]+\cdots=\sum_{i=1}^{\infty}\left[\frac{ab}{p^i}\right]$$

분모의 p의 지수는

$$b\left(\left[\frac{a}{p}\right]+\left[\frac{a}{p^2}\right]+\cdots\right)+\left[\frac{b}{p}\right]+\left[\frac{b}{p^2}\right]+\cdots$$

$$=b\sum_{i=1}^{\infty}\left[\frac{a}{p^i}\right]+\sum_{i=1}^{\infty}\left[\frac{b}{p^i}\right]$$

우리가 보일것은 다음을 보이면 충분하다.

$$\left[\frac{ab}{p^i}\right]\geq b\left[\frac{a}{p^i}\right]+\left[\frac{b}{p^i}\right] \quad \cdots ①$$

이를 $i=1$일때 $a=\left[\frac{a}{p}\right]p+r \qquad 0\leq r\leq p-1$

$b=\left[\frac{b}{p}\right]p+s \qquad 0\leq s\leq p-1$

$$ab=\left[\frac{a}{p}\right]\left[\frac{b}{p}\right]p^2+\left[\frac{a}{p}\right]ps+\left[\frac{b}{p}\right]pr+rs$$

$$\frac{ab}{p}=\left[\frac{a}{p}\right]\left[\frac{b}{p}\right]p+\left[\frac{a}{p}\right]s+\left[\frac{b}{p}\right]r+\frac{rs}{p}$$

$$\left[\frac{ab}{p}\right]=\left[\frac{a}{p}\right]\left[\frac{b}{p}\right]p+\left[\frac{a}{p}\right]s+\left[\frac{b}{p}\right]r+\left[\frac{rs}{p}\right]$$

$$=b\left[\frac{a}{p}\right]+\left[\frac{b}{p}\right]r+\left[\frac{rs}{p}\right]$$

(대결) 만약 $p\nmid a$ 일때 $r\neq 0$ $\geq b\left[\frac{a}{p}\right]+\left[\frac{b}{p}\right]$

반약 $p\mid a$ 즉 $r=0$ 이라면 ? $\longrightarrow$?

$i=1$일때 성립한다면 다 된 것이다.

$$\left[\frac{1}{p}\left[\frac{ab}{p}\right]\right]\geq\left[\frac{1}{p}\left(b\left[\frac{a}{p}\right]+\left[\frac{b}{p}\right]\right)\right]$$

$$\left[\frac{ab}{p^2}\right]\geq b\left[\frac{a}{p^2}\right]+\left[\frac{b}{p^2}\right]$$

마찬가지로 하면 ①이 성립.

EX 1. $n>0$, 정수이면
$\frac{(2n)!}{(n!)^2}$ 은 정수이다.

EX 2. $(a,b)=1$ 이고 $a+b=n+1$ 이면
$\frac{n!}{a!b!}$ 은 자연수이다.

EX 3. n이 자연수이면 $\sum_{j=1}^{\infty}\left[\frac{n}{2^j}+\frac{1}{2}\right]=n$

EX 4. $x>0$ 인 실수이면
$[x]+[x+\frac{1}{n}]+[x+\frac{2}{n}]+\cdots+[x+\frac{n-1}{n}]=[nx]$

EX 5. n 자연수이면
$\frac{(2n-2)!}{n!(n-1)!}$ 은 정수이다

○ n이 자연수일때

① $d(n)$ = n의 양의 약수의 개수 $=\left|\{x \mid x는\ n의\ 약수,\ x\in\mathbb{N}\}\right|=\sum_{\substack{d\mid n\\ d>0}}1$

$d(6)=2\times2=4$

$d(3)=2$ $\qquad$ $d(p)=2$

$n=p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\cdots p_k^{\alpha_k}$ 로 소인수분해 되면

$d(n)=(\alpha_1+1)(\alpha_2+1)(\alpha_3+1)\cdots(\alpha_k+1)$

$=\prod_{p^{\alpha}\| n}(\alpha+1)$

② $\sigma(n)$ = n의 양의 약수의 합

$\sigma(6)=12$, $\sigma(p)=p+1$ $\quad(p$: 소수)

$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ 로 소인수분해되면

$\sigma(n)=(1+p_1+p_1^2+\cdots+p_1^{\alpha_1})(1+p_2+\cdots+p_2^{\alpha_2})\cdots(1+p_k+p_k^2+\cdots+p_k^{\alpha_k})$

$=\prod_{p^{\alpha}\| n}(1+p+p^2+\cdots+p^{\alpha})=\prod_{p^{\alpha}\| n}\frac{p^{\alpha+1}-1}{p-1}$

③ $\varphi(n)$ = 1부터 n까지 자연수중에서 n과 서로 소인 것들의 개수

$\varphi(6)=2$ ($\because$ 1, 5)

$\varphi(10)=4$ ($\because$ 1, 3, 7, 9)

$\varphi(p)=p-1$

$\varphi(p^2)=p^2-p$ ($\because$ p : $1p, 2p, 3p, \cdots, pp$)

$\therefore$ $\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}$

($1\sim p^\alpha$까지 p의 배수는 $1\cdot p, 2\cdot p, \cdots, p^{\alpha-1}p$ 즉 $p^{\alpha-1}$개)

• f가 자연수에서 정의될 때

$(m,n)=1$ 이면 $f(mn)=f(m)f(n)$을 만족할때

multiplicative function f를 승법적인 산술함수라 한다.

예) $f(n)=1$, $f(n)=n$

$d(n)$, $\sigma(n)$

φ는 승법적인 함수. 정리★. $(m,n)=1$ 일때 $\varphi(mn)=\varphi(m)\varphi(n)$

(증명) $A=\{\, mr+ns \mid 1\le r\le n,\ (r,n)=1,\quad 1\le s\le m,\ (s,m)=1 \,\}$

$|A|=\varphi(m)\varphi(n)$

$\because$ $mr+ns,\ mr'+ns' \in A$

$mr+ns=mr'+ns'$ 라 하자.

$m(r-r')=n(s'-s)$

$(\bmod n)$ $r\equiv r' \pmod n$ $\therefore r=r'$

$(\bmod m)$ $s\equiv s' \pmod n$ $\therefore s=s'$

$\therefore$ 원소는 중복되는 것이 없다

A가 mod mn의 기약 잉여계이다

A의 원소들이 m, n과 서로소이고 modulo mn으로 봐을 때 서로 다르다

$\because$ ① $(mr+ns, mn)=1$

$\Leftrightarrow$ $(mr+ns, m)=1$ and $(mr+ns, n)=1$

$\Leftarrow$ $(ns, m)=1$ and $(mr, n)=1$

$\Leftrightarrow$ $(s, m)=1$ and $(r, n)=1$.

② 만약 $mr+ns \equiv mr'+ns' \pmod{mn}$ 라면

($mr+ns,\ mr'+ns' \in A$)

$mr+ns\equiv mr'+ns' \pmod m$

$ns\equiv ns' \pmod m$ $s\equiv s' \pmod m$ $\therefore s=s'$

$mr+ns\equiv mr'+ns' \pmod n$

$mr\equiv mr' \pmod n$ $r\equiv r' \pmod n$ $\therefore r=r'$

$\therefore$ $s=s'$, $r=r'$

$\therefore$ $\varphi(mn)=\varphi(m)\varphi(n)$

morning glory

◦ f가 승법적이고 $n=\prod_{p^\alpha \| n} p^\alpha$ 이면

$$f(n)=f\left(\prod_{p^\alpha \| n} p^\alpha\right)$$

$$=\prod_{p^\alpha \| n} f(p^\alpha)$$

특히 f가 φ일때 $n=\prod_{p^\alpha \| n} p^\alpha$ 이면

$$\varphi(n)=\prod_{p^\alpha \| n} \varphi(p^\alpha)$$

$$=\prod_{p^\alpha \| n} p^\alpha\left(1-\frac{1}{p}\right)$$

$$= n \prod_{p \| n}\left(1-\frac{1}{p}\right)$$

◦ f가 승법적이면 $F(n)=\sum_{d|n} f(d)$ 도 승법적이다

(증명) $(m,n)=1$ 라 가정하자.

$$F(mn)=\sum_{d|mn} f(d)$$

$(m,n)=1$ 이므로 mn의 약수 $d=d_1d_2$ 로 쓸수 있다 단, $d_1|m,\ d_2|n \Rightarrow (d_1,d_2)=1$

$$=\sum_{\substack{d_1|m\\ d_2|n}} f(d_1d_2)$$

$$=\sum_{\substack{d_1|m\\ d_2|n}} f(d_1)f(d_2) = \sum_{d_1|m}\sum_{d_2|n} f(d_1)f(d_2)$$

$$=\left(\sum_{d_1|m} f(d_1)\right)\left(\sum_{d_2|m} f(d_2)\right)= F(m)F(n)$$

◦ f, g가 승법적이면 $F(n)=\sum_{d|n} f(d)\,g\left(\frac{n}{d}\right)$ 도 승법적이다.

(증명) $(m,n)=1$ 일때

$$F(mn)=\sum_{d|mn} f(d)g\left(\frac{mn}{d}\right)$$

$$=\sum_{d_1|m}\sum_{d_2|n} f(d_1d_2)\,g\left(\frac{m}{d_1}\cdot\frac{n}{d_2}\right)$$

$$=\sum_{d_1|m}\sum_{d_2|n} f(d_1)\,g\left(\frac{m}{d_1}\right)\,f(d_2)\,g\left(\frac{n}{d_2}\right)$$

$$=\sum_{d_1|m} f(d_1)\,g\left(\frac{m}{d_1}\right)\cdot\sum_{d_2|n} f(d_2)\,g\left(\frac{n}{d_2}\right)$$

$$= F(m)\,F(n)$$

○ 뫼비우스 (Möbius) 함수

$$\mu(n) = \begin{cases} (-1)^k & : n\text{이 서로 다른 } k\text{개의 소수의 곱일때} \\ 0 & : \text{소수의 제곱인수가 들어있을 때.} \\ 1 & : n=1 \end{cases}$$

m, n을 소인수분해해서 간단히 보일수있다 ← μ : 승법적 함수

· 뫼비우스의 역공식

f가 산술함수이고

$g(n)=\sum_{d|n} f(d)$ 로 정의한다.

그러면 $f(n)=\sum_{d|n} \mu(d)\, g\left(\frac{n}{d}\right)$

그 역도 성립한다.

(증명) $\sum_{d|n} \mu(d)\, g\left(\frac{n}{d}\right)$

$= \sum_{d|n} \mu(d) \sum_{k|\frac{n}{d}} f(k)$

$= \sum_{d|n} \sum_{k|\frac{n}{d}} f(k)\mu(d)$ ← $kd=l$로 치환 $l|n$

$= \sum_{k|n} \sum_{d|\frac{n}{k}} f(k)\mu(d)$

$= \left(\sum_{k|n} \left[f(k) \sum_{d|\frac{n}{k}} \mu(d) \right]\right)$

$= f(n)$. ∵ 윗의 예를보면 $\frac{n}{k}=1$ 일때만 $\sum_{d|\frac{n}{k}} \mu(d)=1$ 이기 때문.

· f, g가 승법적이면

$f(n)=g(n) \iff f(p^\alpha)=g(p^\alpha)$ p : prime

f승법적 ⇒ $f(1)=1$.

예) · $f(l)=\sum_{d|l} \mu(d)$

$f(p^\alpha)=\sum_{d|p^\alpha} \mu(d)$

$= \mu(1)+\mu(p)+\mu(p^2)+\cdots+\mu(p^\alpha)$

$= 1-1 = 0$

$g(l)=\begin{cases} 1 & : l=1 \\ 0 & : l\neq 1 \end{cases}$ (승법적인 함수)

$g(p^\alpha)=0$

$\therefore f(p^\alpha)=g(p^\alpha) \iff f(n)=g(n)$

morning glory

Ex) $\sum_{k|n} d(k)^3 = \left(\sum_{k|n} d(k) \right)^2$

p.f) $F(n) = \sum_{k|n} d(k)^3$

$G(n) = \left(\sum_{k|n} d(k) \right)^2$ 라 두자.

예제 F, G : 승법적인 함수이다.

소수 p 에 대해

$$F(p^\alpha) = \sum_{k|p^\alpha} d(k)^3 = d(1)^3 + d(p)^3 + d(p^2)^3 + \cdots + d(p^\alpha)^3$$
$$= 1 + 2^3 + 3^3 + 4^3 + \cdots + (\alpha+1)^3$$
$$= \left\{ \frac{(\alpha+1)(\alpha+2)}{2} \right\}^2$$

$$G(p^\alpha) = \left(\sum_{k|p^\alpha} d(k) \right)^2$$
$$= \left\{ d(1) + d(p) + d(p^2) + \cdots + d(p^\alpha) \right\}^2$$
$$= \left\{ 1 + 2 + 3 + \cdots + (\alpha+1) \right\}^2$$
$$= \left\{ \frac{(\alpha+1)(\alpha+2)}{2} \right\}^2$$

$\therefore F(p^\alpha) = G(p^\alpha)$

$\therefore F(n) = G(n)$ ($\because$ 승법적인 함수이므로) $=$

트윈트 13번) Ex①) $\sum_{\substack{a=1 \\ (a,n)=1}}^{n} (a-1, n) = d(n)\varphi(n)$

p.f) $F(n) = \sum_{\substack{a=1 \\ (a,n)=1}}^{n} (a-1, n)$

$(m,n)=1$ 라 하자.

$$F(mn) = \sum_{\substack{a=1 \\ (a,mn)=1}}^{mn} (a-1, mn)$$

$a = km + ln$ $\quad 1 \le k \le n$ $\quad (k,n)=1$

$\quad 1 \le l \le m$ $\quad (l,m)=1$

$$\left.\begin{array}{l} (a,mn)=1 \iff (km+ln, mn)=1 \\ \iff (km+ln, m)=1 \text{ and } (km+ln, n)=1 \\ \iff (l,m)=1 \text{ and } (k,n)=1 \end{array}\right\} \text{라 두면}$$

$(a-1, mn) = (km+ln-1, mn)$ 이다.

$$F(mn) = \sum_{\substack{a=1 \\ (a,mn)=1}}^{mn} (a-1, mn)$$
$$= \sum_{\substack{k=1 \\ (k,n)=1}}^{n} \sum_{\substack{l=1 \\ (l,m)=1}}^{m} (kn+ln-1, m) \cdot (km+ln-1, n)$$
$$= \sum_{\substack{k=1 \\ (k,n)=1}}^{n} (kn-1, m) \sum_{\substack{l=1 \\ (l,m)=1}}^{m} (ln-1, m)$$

m과 n의 각각의 기약잉여계 원소에 대한 작업(summation)으로 총합은 다음과 같다

$$= \sum_{\substack{k=1 \\ (k,n)=1}}^{n} (k-1, n) \sum_{\substack{l=1 \\ (l,m)=1}}^{m} (l-1, m)$$

$$= F(n)\,F(m)$$

∴ 좌변은 승법적 함수.

EX ② $\quad \dfrac{n}{\varphi(n)} = \sum_{d|n} \dfrac{\mu^2(d)}{\varphi(d)}$

※ 승법적 함수라고 밝힌 후 p^α에서 증명 → 해결

sol 1) 좌우변 모두 가 승법적인 함수 → $n = p^\alpha$ 대입후 계산

sol 2) $\sum_{d|n} \dfrac{\mu^2(d)}{\varphi(d)} = 1 + \sum_{\substack{p_i|n \\ p_i \neq p_j}} \dfrac{\mu^2(p_1 p_2 \cdots p_\ell)}{\varphi(p_1 p_2 \cdots p_\ell)}$

※ 합(Σ)을 곱($\prod_{p\cdots}$)으로 변형 → 해결

$$= 1 + \sum \frac{1}{\varphi(p_1)\varphi(p_2)\cdots\varphi(p_\ell)}$$

$$= \prod_{p|n} \left(1 + \frac{1}{\varphi(p)}\right)$$

$$= \prod_{p|n} \left(\frac{p-1+1}{p-1}\right)$$

우변: $\quad = \prod_{p|n} \dfrac{p}{p-1}$

좌변 $\quad \dfrac{n}{\varphi(n)} = \dfrac{n}{n\prod_{p|n}(1-\frac{1}{p})} = \prod_{p|n} \dfrac{p}{p-1}$

※ $1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots$

합(Σ) → 곱(Π)

$$= \prod_{p} \left(1 + \frac{1}{p^2} + \frac{1}{p^4} + \cdots\right)$$

EX ③ $\quad \sum_{k=1}^{n} d(k) = \sum_{k=1}^{n} \left[\frac{n}{k}\right]$

sol 1) $\sum_{k=1}^{n} d(k) = \sum_{k=1}^{n} \sum_{d|k} 1 = \sum_{d=1}^{n} \sum_{\substack{d|k \\ 1\le k\le n}} 1 = \sum_{d=1}^{n} \left[\frac{n}{d}\right]$

sol 2) 식이 필요없이 명백하다.

1~n까지 어떤 수의 약수의 개수

= 1~n 까지 수를 약수로 갖는 1~n까지 수의 개수

= 1~n 까지 수의 배수의 개수 (1~n범위)

morning glory

· n이 완전수 $\iff$ $\sigma(n)=2n$

$\iff$ n을 제외한 약수의 합이 n과 같은 수

예) 6 : $1+2+3=6$.

28 : $1+2+4+7+14=28$

· $n=2^{a-1}(2^a-1)$, 2^a-1 : 소수 이면 n은 완전수이다.

($\because$) $\sigma(2^{a-1}(2^a-1))$

$=\sigma(2^{a-1})\,\sigma(2^a-1)$

$=(2^{a-1}+2^{a-2}+\cdots+1)\cdot(2^a-1+1)$

$=2^a\left(\frac{2^a-1}{2-1}\right)$

$=2\cdot(2^{a-1})(2^a-1)$

$=2n$

그런데 n이 짝수이면서 완전수

$\iff$ $n=2^{a-1}(2^a-1)$ $\quad 2^a-1$: 소수

(증명) $n=2^k m$ $\quad 2\nmid m$, $k\geq 1$

$\sigma(n)=\sigma(2^k)\,\sigma(m)$

$=\frac{2^{k+1}-1}{2-1}\cdot\sigma(m)$

$=(2^{k+1}-1)\cdot\sigma(m)=2n=2^{k+1}m$

$\therefore \sigma(m)=\frac{2^{k+1}m}{2^{k+1}-1}$

$(2^{k+1}-1)\mid m$ 이므로 $m=(2^{k+1}-1)p$ 라두자. p : 정수

$\sigma(m)=2^{k+1}p$

$\sigma((2^{k+1}-1)p)=2^{k+1}p$

$\sigma(m)\geq m+1$
(등호는 m이 소수)

morning glory

· 연분수 (Continued Fractions)

1. 유한 연분수 (finite continued fraction)

e.g. $1+\cfrac{1}{2+\cfrac{1}{3+\frac{1}{4}}} = \langle 1,2,3,4\rangle = \langle 1,2,3+\frac{1}{4}\rangle$

정의 $r_0, r_1, r_2, \cdots r_n \in \mathbb{R}$

$r_1, r_2, \cdots r_n > 0$

$r_0+\cfrac{1}{r_1+\cfrac{1}{r_2+\cdots\cfrac{1}{r_{n-1}+\frac{1}{r_n}}}}$: 유한 연분수.

if $r_i \in \mathbb{Z}$ 이면 유한 단순연분수

표시: $\langle r_0, r_1, r_2, \cdots, r_n\rangle$

정리 (1) $\langle r_0, r_1, \cdots, r_{n-1}, r_n\rangle = \langle r_0, r_1, \cdots, r_{n-2}, r_{n-1}+\frac{1}{r_n}\rangle$

(2) $\langle r_0, r_1, \cdots, r_n\rangle = r_0+\cfrac{1}{\langle r_1, r_2, \cdots, r_n\rangle}$

(3) 유한 단순연분수는 유리수이다.

(4) 임의의 유리수는 유한 단순 연분수로 표시할 수 있다.

(증명) (4) r : 임의의 유리수

$r=\frac{m_0}{m_1}$ $(m_0, m_1 \in \mathbb{Z},\ m_1>0)$ $(m_0, m_1)=1$.

$m_0 = r_0 m_1 + m_2 \quad (0<m_2<m_1)$

$m_1 = r_1 m_2 + m_3 \quad (0<m_3<m_2)$

$\vdots$

$m_n = r_n m_{n+1}. \quad (n \geq 0)$

여기서 당연히 $r_1, r_2, \cdots > 0$

$$r=\frac{m_0}{m_1}=\frac{r_0 m_1+m_2}{m_1}$$

$$= r_0+\frac{1}{\frac{m_1}{m_2}}$$

$$= r_0+\cfrac{1}{r_1+\frac{1}{\frac{m_2}{m_3}}}$$

$$= \cdots\cdots = r_0+\cfrac{1}{r_1+\cfrac{1}{r_2+\cdots\cdots+\frac{1}{r_n}}}$$

$$= \langle r_0, r_1, \cdots, r_n\rangle$$

e.g. $\frac{14}{17}$

$= 0 + \frac{1}{\frac{17}{14}} = 0 + \frac{1}{1+\frac{3}{14}}$

$= 0 + \frac{1}{1+\frac{1}{4+\frac{2}{3}}}$

$= 0 + \frac{1}{1+\frac{1}{4+\frac{1}{1+\frac{1}{2}}}} = \langle 0, 1, 4, 1, 2 \rangle$

2. 무한 연분수 (infinite continued fraction)

$a_0, a_1, \cdots, a_n, \cdots \in \mathbb{Z}$

$a_1, a_2, \cdots > 0$

h_i, k_i를 다음과 같이 정의한다.

$h_{-2}=0$, $h_{-1}=1$ $\quad h_i = a_i h_{i-1} + h_{i-2}$

$k_{-2}=1$, $k_{-1}=0$ $\quad k_i = a_i k_{i-1} + k_{i-2}$

	-2	-1	a_0	a_1	a_2
h_i	0	1	a_0+0	$a_0a_1+a_0$	$a_0a_1a_2+a_0a_2+a_0a_1+a_0$
k_i	1	0	1	a_1+0	a_1a_2+1

정리, (1) $1 = k_0 \le k_1 < k_2 < \cdots$

(2) $\langle a_0, a_1, a_2, \cdots, a_{n-1}, x \rangle = \frac{x h_{n-1} + h_{n-2}}{x k_{n-1} + k_{n-2}}$

(3) $r_n = \langle a_0, \cdots, a_{n-1}, a_n \rangle$ 라 하면 $r_n = \frac{h_n}{k_n}$

(증명) (1) $k_0 = a_0 k_{-1} + k_{-2} = 1$

$k_1 = a_1 k_0 + k_{-1} = a_1 \ge 1 = k_0$

$\vdots$

$k_i > k_{i-1} \ge k_{i-2}$ 라 가정하자. $(i>1)$

$k_{i+1} = a_{i+1} k_i + k_{i-1} > a_{i+1} k_i \ge k_i$

(2) $n=0$ 일때 좌변 $\langle x \rangle = x$

우변 $\frac{x h_{n-1} + h_{n-2}}{x k_{n-1} + k_{n-2}} = x$

$\therefore$ L.H.S = R.H.S

(n일때) $\frac{x h_{n-1} + h_{n-2}}{x k_{n-1} + k_{n-2}} = \langle a_0, a_1, \cdots, a_{n-1}, x \rangle$ 라 가정하자

$$\begin{aligned}
&\langle a_0, a_1, \cdots, a_{n-1}, a_n, x\rangle \\
&= \langle a_0, a_1, \cdots, a_{n-1}, a_n + \tfrac{1}{x}\rangle \\
&= \frac{(a_n+\frac{1}{x})h_{n-1} + h_{n-2}}{(a_n+\frac{1}{x})k_{n-1} + k_{n-2}} \\
&= \frac{(a_n h_{n-1} + h_{n-2})x + h_{n-1}}{(a_n k_{n-1} + k_{n-2})x + k_{n-1}} \\
&= \frac{x h_n + h_{n-1}}{x k_n + k_{n-1}}
\end{aligned}$$

(3) (2)에서 x 대신 a_n을 대입하자.

$$\langle a_0, a_1, \cdots, a_n\rangle = \frac{a_n h_{n-1} + h_{n-2}}{a_n k_{n-1} + k_{n-2}} = \frac{h_n}{k_n}$$

e.g.)

		2	1	1	3	4
h_i	0	1	2	3	5	18	77
k_i	1	0	1	1	2	7	30

(2×0+1, 4×7+2)

$\therefore \langle 2,1,1,3,4\rangle = \frac{77}{30}$

정리. (1) $h_i k_{i-1} - h_{i-1} k_i = (-1)^{i-1}$

특히 $(h_i, k_i) = 1$ $\therefore$ $\frac{h_i}{k_i}$는 기약분수

(2) $h_i k_{i-2} - h_{i-2} k_i = (-1)^i a_i$

증명 (1) induction을 사용.

STEP 1) $i=-1$. $h_{-1}k_{-2} - h_{-2}k_{-1} = 1\cdot 1 - 0\cdot 0 = 1 = (-1)^{-2} = 1$

$\therefore$ 성립.

STEP 2) n일 때 성립을 가정

즉 $h_i k_{i-1} - h_{i-1} k_i = (-1)^{i-1}$ 라 가정하면

$$\begin{aligned}
&h_{i+1} k_i - h_i k_{i+1} \\
&= (a_{i+1} h_i + h_{i-1}) k_i - h_i (a_{i+1} k_i + k_{i-1}) \\
&= -(h_i k_{i-1} - h_{i-1} k_i) \\
&= -1 \cdot (-1)^{i-1} \\
&= (-1)^i
\end{aligned}$$

$\therefore$ 즉 성립

(2) $h_i k_{i-2} - h_{i-2} k_i$

$$\begin{aligned}
&= (a_i h_{i-1} + h_{i-2}) k_{i-2} - h_{i-2}(a_i k_{i-1} + k_{i-2}) \\
&= a_i (h_{i-1} k_{i-2} - h_{i-2} k_{i-1}) \\
&= a_i (-1)^{i-2} \quad \text{(정리 (1).)} \\
&= (-1)^i a_i
\end{aligned}$$

서로소인 이유

$(a,b) = 1 \iff ax_0 + by_0 = 1$인 $x_0, y_0 \in \mathbb{Z}$가 존재

$\therefore$

$h_i(k_{i-2}) + k_i(-h_{i-1}) = (-1)^{i-1}$

에서 $(h_i, k_i) = 1$

정리. $r_n = \langle a_0, \cdots, a_n \rangle \quad a_i \in \mathbb{Z}.$

$a_1, a_2, \cdots, a_n, \cdots > 0$

$\Rightarrow$ (1) $r_0 < r_2 < r_4 < \cdots < r_5 < r_3 < r_1$

(2) $\lim_{n\to\infty} r_n$ 값이 존재. $(r_{2n} < r < r_{2n+1})$

(증명) (1) $r_n = \frac{h_n}{k_n} \qquad r_{n-1} = \frac{h_{n-1}}{k_{n-1}}$

$$r_n - r_{n-1} = \frac{h_n}{k_n} - \frac{h_{n-1}}{k_{n-1}} = \frac{(-1)^{n-1}}{k_n k_{n-1}}$$

$$r_n - r_{n-2} = \frac{h_n}{k_n} - \frac{h_{n-2}}{k_{n-2}} = \frac{a_n (-1)^n}{k_n k_{n-2}}$$

n이 짝수일때 $+$

$\therefore r_0 < r_2 < \cdots$

n이 홀수일때

$r_1 > r_3 > \cdots$

그런데 $r_{홀} > r_{짝}$ (홀짝: 인접한수)

$\therefore r_0 < r_2 < \cdots < r_3 < r_1$

(2) (1)에 의해 존재한다.

(3) $n \to \infty$ 일때 즉 $r = \lim_{n\to\infty} r_n$ 로 두면

r은 무리수이다.

$|r_n - r|$

$r_n < r < r_{n+1}$ 라면

$|r_{n+1} - r_n|$

(증명) $|r_{n+1} - r_n| = \left|\frac{(-1)^n}{k_n k_{n+1}}\right| = \frac{1}{k_n k_{n+1}}$

$0 < |r - r_n| < |r_{n+1} - r_n|$

$0 < \left|r - \frac{h_n}{k_n}\right| < \left|\frac{1}{k_{n+1} k_n}\right|$

$0 < |rk_n - h_n| < \frac{1}{k_{n+1}}$

이제 r을 유리수라 가정하자.

$r = \frac{a}{b}$ (a, b는 서로소인 정수)

$0 < \left|\frac{a}{b}k_n - h_n\right| < \frac{1}{k_{n+1}}$

$0 < |ak_n - bh_n| < \frac{b}{k_{n+1}}$, $\forall n \in \mathbb{N}$.

그런데 $k_0 \le k_1 < k_2 < \cdots < k_n < \cdots$ 이므로

또한 k_i는 정수이므로

어떤 n이 존재하여 $k_{n+1} > b$

$\therefore 0 < \underbrace{|ak_n - bh_n|}_{\text{정수}} < \frac{b}{k_{n+1}} < 1$

$\therefore$ 모순 즉, 무리수이다.

morning glory

e.g. $1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cdots}}} = \langle 1,1,1,\cdots\rangle = \langle \overline{1}\rangle = k$ 라 두자

정리에 의해 수렴한다.

k 대신 $\sum$ 로 쓴다

$k = 1+\frac{1}{k}$ $\quad k^2-k-1=0$ $\quad k=\frac{1\pm\sqrt{5}}{2}$

$(\because \langle\overline{1}\rangle = \langle 1,\overline{1}\rangle = 1+\frac{1}{\langle\overline{1}\rangle} = 1+\frac{1}{k}\rangle$

$k > \langle 1\rangle$ $\quad \therefore k=\frac{1+\sqrt{5}}{2}$

e.g. $\sqrt{3} = \langle a_0, a_1, a_2, \cdots\rangle$

$a_0 = [\sqrt{3}] = 1$

$a_1 = \left[\frac{1}{\sqrt{3}-1}\right] = \left[\frac{\sqrt{3}+1}{2}\right] = 1$

$a_2 = \left[\frac{1}{\frac{\sqrt{3}+1}{2}-1}\right] = \left[\frac{2}{\sqrt{3}-1}\right] = \left[\sqrt{3}+1\right] = 2$

$a_3 = \left[\frac{1}{\sqrt{3}+1-2}\right] = \left[\frac{\sqrt{3}+1}{2}\right] = a_1 = 1.$

$a_4 = a_2 = 2.$

$a_5 = a_3 = a_1 = 1$

$\vdots$

$\sqrt{3} = \langle 1,1,2,1,2,1,2,\cdots\rangle$

$= \langle 1,\overline{1,2}\rangle$

$\langle 1,\overline{1,2}\rangle$ → 순환부터

3. 순환(무한) 단순) 연분수

2차무리수 : 어떤 정수계수 이차방정식의 근이 되는 무리수

정리 1. 순환 연분수는 2차무리수이다

정리 2. 역으로 2차무리수는 순환 연분수이다.

정의 $\langle b_0, b_1, \cdots, b_\ell, \overline{a_1, a_2, \cdots, a_r}\rangle$: 순환 무한(단순) 연분수

$b_i, a_i \in \mathbb{Z}$

$b_1, b_2, \cdots, b_\ell, a_1, a_2, \cdots, a_r > 0$

$\langle \overline{a_1, a_2, \cdots, a_r}\rangle$ 순순환 단순 연분수

정리 1의 증명: $x = \langle \overline{a_1, a_2, \cdots, a_r}\rangle$ 라 하자.

$x = \langle a_1, a_2, \cdots, a_r, \overline{a_1, a_2, \cdots, a_r}\rangle$

$x = \langle \overline{a_1, a_2, \cdots, a_r}\rangle = \langle a_1, a_2, \cdots, a_r, \overline{a_1, \cdots, a_r}\rangle$

$= \langle a_1, a_2, \cdots, a_r, x\rangle$

$= \frac{\alpha x+\alpha'}{\beta x+\beta'}$ (단 $\alpha,\beta,\alpha',\beta' \in \mathbb{Z}$. $\beta \neq 0$)

$\rightarrow p$

$x(\beta x+\beta') = \alpha x+\alpha'$

① $\cdots$ $\beta x^2+(\beta'-\alpha)x-\alpha'=0$ ※

무한연분수이므로 무리수 $\Rightarrow$ ∴ x는 이차무리수.

이제 일반적으로

$y=\langle b_0, b_1, b_2, \cdots, b_l, \overline{a_1, \cdots, a_n}\rangle$

$=\langle b_0, b_1, b_2, \cdots, b_l, x\rangle$

$=\dfrac{\alpha'' x+\alpha'''}{\beta'' x+\beta'''}$ $(\text{단 } \alpha'', \alpha''', \beta'', \beta''' \in \mathbb{Z})$

$(\beta'' y-\alpha'')x = \alpha'''-\beta''' y$

$x=\dfrac{-\beta''' y+\alpha'''}{\beta'' y+(-\alpha'')}$

이것은 ①식에 대입하면 분모^{2}을 곱하면 정수계수 2차방정식이 된다 ∴ 2차무리수

정리 2의 증명

x는 이차무리수 이므로

$x=\dfrac{a+\sqrt{b}}{c}$ $a, b, c \in \mathbb{Z}$, $c\neq 0$, $b>0$, b는 완전제곱수가 아님

$ax^2+bx+c=0 \Rightarrow x=\dfrac{-b\pm\sqrt{b^2-4ac}}{2a}$

다음과 같이 x_n, a_n을 귀납적으로 정의하자:

$x_0=x$, $a_0=[x]$

$x_1=\dfrac{1}{x_1-a_0}$, $a_1=[x_1]$

$\vdots$

$x_{n+1}=\dfrac{1}{x_n-a_n}$, $a_{n+1}=[x_{n+1}]$

x_i 각각은 무리수이므로 x_i는 0이 아니다

그러면 $x=\langle a_0, a_1, \cdots, a_{n+1}, \cdots\rangle$

우리는 x가 순환함을 보이려 한다.

$m_0=a|c|$, $q_0=c|c|$, $d=c^2b$ 라 하자.

$x=\dfrac{a+\sqrt{b}}{c}=\dfrac{a|c|+\sqrt{bc^2}}{c|c|}=\dfrac{m_0+\sqrt{d}}{q_0}$ $(q_0\neq 0)$

$d-m_0^2=c^2b-(a|c|)^2=c^2(b-a^2)$

$q_0 \mid (d-m_0^2)$

아래와 같이 m_n, q_n을 정의하자.

$m_n=a_{n-1}q_{n-1}-m_{n-1}$

$q_n=\dfrac{d-m_n^2}{q_{n-1}}$

STEP (1) $m_n, q_n \in \mathbb{Z}$, $q_n\neq 0$, $q_n \mid (d-m_n^2)$

$n=0$: 자명.

morning glory

n일때 성립가정. $n+1$ 일때는

$$m_{n+1} = a_n q_n - m_n \quad : m_{n+1} \in \mathbb{Z}.$$

$$q_{n+1} = \frac{d - m_{n+1}^2}{q_n}$$

$$= \frac{d - (a_n q_n - m_n)^2}{q_n}$$

$$= \frac{d - (a_n^2 q_n^2 - 2 m_n a_n q_n + m_n^2)}{q_n}$$

$$= \underbrace{\frac{d - m_n^2}{q_n}} - a_n^2 q_n + 2 m_n a_n \quad \therefore q_{n+1} \in \mathbb{Z}.$$

↳ 가정에 의해 정수

d는 완전제곱수가 아니므로 $d \neq m_{n+1}^2$

$$\therefore \quad q_{n+1} \neq 0.$$

$$q_n q_{n+1} = d - m_{n+1}^2$$

이므로 $\quad q_{n+1} \mid (d - m_{n+1}^2)$

STEP(2) $\quad x_n = \dfrac{m_n + \sqrt{d}}{q_n}$ 임을 보이자

$n=0$: 자명.

n일때 성립한다고 가정하고 $n+1$ 일때는 ?

$$x_{n+1} = \frac{1}{x_n - a_n}$$

$$= \frac{1}{\frac{m_n + \sqrt{d}}{q_n} - a_n}$$

$$= \frac{q_n}{m_n + \sqrt{d} - a_n q_n}$$

$$= \frac{q_n}{\sqrt{d} - m_{n+1}}$$

$$= \frac{q_n (\sqrt{d} + m_{n+1})}{d - m_{n+1}^2}$$

$$= \frac{m_{n+1} + \sqrt{d}}{q_{n+1}}$$

STEP(3) $\quad x = \langle a_0, a_1, \cdots \rangle$: 순환 연분수.

x : 무리수

$\bar{x}$: 켤레무리수(?)

$x + \bar{x}$: x의 norm.

$x\bar{x}$: x의 trace

$x \in \mathbb{Q} \iff x = \bar{x}$

$\overline{\left(\frac{x}{y}\right)} = \frac{\bar{x}}{\bar{y}}$

$$x = x_0 = \langle a_0, a_1, \cdots, a_{n-1}, x_n \rangle$$

$$= \frac{x_n h_{n-1} + h_{n-2}}{x_n k_{n-1} + k_{n-2}}$$

$$\bar{x} = \frac{\bar{x_n} h_{n-1} + h_{n-2}}{\bar{x_n} k_{n-1} + k_{n-2}}.$$

$$(\bar{x} k_{n-1} - h_{n-1})\bar{x_n} = (-k_{n-2}\bar{x} + h_{n-2})$$

$$\overline{x_n} = \frac{\cdot\,\overline{x}(-k_{n-2}) + h_{n-2}}{\overline{x}k_{n-1} - h_{n-1}} = -\frac{\overline{x}(k_{n-2}) - h_{n-2}}{\overline{x}\,k_{n-1} - h_{n-1}}$$

$$= -\frac{k_{n-2}}{k_{n-1}} \cdot \frac{\overline{x} - \frac{h_{n-2}}{k_{n-2}}}{\overline{x} - \frac{h_{n-1}}{k_{n-1}}}$$

$$M_n = \frac{\overline{x} - \frac{h_{n-2}}{k_{n-2}}}{\overline{x} - \frac{h_{n-1}}{k_{n-1}}}$$

x는 무리수이므로 $\qquad x \neq \overline{x}$

한편 $\quad x = \lim_{n\to\infty} \frac{h_n}{k_n} = \lim_{n\to\infty} \frac{h_{n-1}}{k_{n-1}} = \lim_{n\to\infty} \frac{h_{n-2}}{k_{n-2}}$

$$\lim_{n\to\infty} M_n = \lim_{n\to\infty} \frac{\overline{x} - \frac{h_{n-2}}{k_{n-2}}}{\overline{x} - \frac{h_{n-1}}{k_{n-1}}} = \frac{x-x}{\overline{x}-x} = 1$$

$\therefore$ 충분히 큰 N이 존재하여 $n \geq N$인 모든 n에 대하여

$M_n > 0$ 이다.

$\therefore \overline{x_n} < 0 \qquad (\because n \geq N)$

한편 $\forall n \in \mathbb{N}, \quad x_n > 0$

모든 $n \geq N$에 대하여

$$\overline{x_n} < 0, \quad x_n > 0$$

$$0 < x_n - \overline{x} = \frac{m_n + \sqrt{d}}{q_n} - \frac{m_n - \sqrt{d}}{q_n} = \frac{2\sqrt{d}}{q_n}$$

$\therefore \quad q_n > 0 \qquad (q_n \in \mathbb{Z})$

$$0 < q_n \leq q_n q_{n+1} = d - m_{n+1}^2 \leq d$$

$$m_n^2 < m_n^2 + q_{n-1} q_n = d$$

$$-\sqrt{d} < m_n < \sqrt{d}$$

$$0 < q_n \leq d$$

m_n, q_n은 정수이므로

m_n, q_n이 취할 수 있는 가짓수 (m_n, q_n)은 유한개

$\therefore$ 비둘기집 원리에 의해서

$(m_{l+r}, q_{l+r}) = (m_l, q_l)$ 인 $l, r > 0$ 이 존재

이때 $\quad x_{l+r} = x_l \quad \therefore a_{l+r} = a_l$

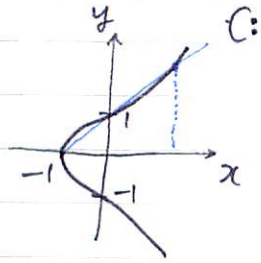
즉 $x = \langle a_0, a_1, \cdots, a_l, \cdots \rangle$

$= \langle a_0, a_1, \cdots, a_{l-1}, \overline{a_l, a_{l+1}, \cdots, a_{l+r-1}} \rangle$ (증명끝)

(STEP 2)

$x_n = \frac{m_n + \sqrt{d}}{q_n}$

morning glory



$C: y^2 = x^3+1$

정수해, 유리수해 ?

방법 1. ⊛ $P_1(x_1,y_1)$ $P_2(x_2,y_2)$ P_1P_2 : C상의 점

$x_i, y_i \in \mathbb{Q}$.

$P_3(x_3,y_3)$ 를 직선 P_1P_2와 C가 만나는 점이라 하면

$x_3, y_3 \in \mathbb{Q}$.

$\because$ $\lambda = (P_1P_2 \text{ 기울기}) = \frac{y_1-y_2}{x_1-x_2} \in \mathbb{Q}$.

$\mu = \lambda x_1 - y_1 \in \mathbb{Q}$.

직선 P_1P_2: $y = \lambda x+\mu$

이것과 C를 연립하면

$(\lambda x+\mu)^2 = x^3+1$

$x^3 - \lambda^2 x^2 - 2\lambda\mu x + 1 - \mu^2 = 0$

이것의 근중 2개는 x_1, x_2 나머지 하나를 x_3라 하면

$x_1+x_2+x_3 = \lambda^2$

$x_3 = \lambda^2 - x_1 - x_2$: 유리수.

$y_3 = \lambda x_3 + \mu$: 유리수.

이문제 경우 $(-1,0)$. $(0,1)$ 을 알고 있다.

이 두점 있는 선: $y = x+1$

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

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

$(x+1)(x^2-2x) = 0$

$(x+1)x(x-2) = 0$ $\therefore x = 2,\ y = 3$

$(2,3)$ 은 C의 유리수해이다 (특히 정수해)

(일반화) ※ $C: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ $(a_i \in \mathbb{Z})$

요약: 두 유리점을 알면 다른 유리점을 구할 수도 있다.

$P_1(x_1,y_1)$, $P_2(x_2,y_2)$: 유리점

$P_3 = (x_3,y_3)$: 직선 P_1P_2와 곡선 C가 만나는 다른 점

$\Longrightarrow$ P_3 : 유리점이 됨.

「직선을 P_1에서의 접선으로 잡으면 1점의 유리점만 알아도 구할수있다. 이것은 근이 x_1, x_1, x_3 가 되기 때문이다. ……」

(증명) $\overline{P_1P_2}$: $y = \lambda x+\mu$ 라 하면

$\lambda = \frac{y_1-y_2}{x_1-x_2} \in \mathbb{Q}$. $\mu = y_1 - \lambda x_1 \in \mathbb{Q}$.

이것은 C에 대해 λ.

$(\lambda x+\mu)^2 + a_1x(\lambda x+\mu) + a_3(\lambda x+\mu) = x^3 + a_2x^2 + a_4x + a_6$

근이 x_1, x_2, x_3 이다.

물론 x_3가 정수가 아니어야 한다. 그런데 정수일 수 없다

$x_1+x_2+x_3 = \lambda^2+a_1\lambda-a_2$

$x_3 = \lambda^2+a_1\lambda-a_2-x_1-x_2 \in \mathbb{Q}$.

$y_3 \in \mathbb{Q}$.

예) $y^2 = x^3+17$

$x=0$: $\times$

$x=1$: $\times$

몇개점찾는 것은 노가다. $x=-1$: $y=\pm 4$.

$(-1,4)$ 에서 접선을 그어보자.

미분: $2yy' = 3x^2$ $\quad y' = \frac{3x^2}{2y}$

접선의 기울기 : $\frac{3}{8}$

$\therefore$ 접선 : $y = \frac{3}{8}x+\frac{3}{8}+4$

$= \frac{3}{8}x+\frac{35}{8}$

이것을 원식에 대입

$\frac{1}{64}(3x+35)^2 = x^3+17$

$9x^2+210x+1225 = 64x^3+1088$

$64x^3-9x^2-210x-137=0$

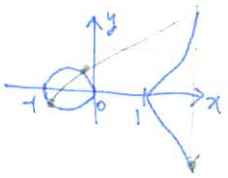
접선과 곡선의 교점중 $x=-1$ 은 알고있다. → 분명히 인수분해 된다

다른 점을 α라 하면

$-2+\alpha = \left(\frac{3}{8}\right)^2$ $\quad \therefore \alpha = 2+\frac{9}{64} = \frac{137}{64}$

유리점개수: 무한

다른 유리점 $\left(\frac{137}{64}, \frac{3}{8}\cdot\frac{137}{64}+\frac{35}{8}\right)$



예, $C: y^2 = x^3-x$

C위의 유리점의 갯수 : 3

예 $y^2 = x^3$

$y=\lambda x$를 그어보면

$\lambda^2x^2 = x^3$

$x^2(x-\lambda^2)=0$ $\quad$ 근 $x=0$ (중근) λ^2

접선과 곡선사이 교점 (λ^2, λ^3) ← 유리수점.

$\forall \lambda \in \mathbb{Q}$에 대해 $y=\lambda x$와 $y^2=x^3$과의 교점은 유리점이다.

예, $y^2 = x^2(x+1)$

morning glory

$y=\lambda x$

$\lambda^2 x^2 = x^2(x+1)$

$x^2(x+1-\lambda^2)=0$

$x=\lambda^2-1$.

유리점 $(\lambda^2-1,\ \lambda^3-\lambda)$ $\lambda\in\mathbb{Q}$.

$y^2=x^3+ax^2+bx+c$ * $y^2=x^3+ax^2+bx+c$. $(a,b,c\in\mathbb{Z})$

: 타원곡선

(elliptic curve

3중근가질때 : cusp

2중근 : node

(1) $x^3+ax^2+bx+c=0$ 이 3중근 $\alpha\in\mathbb{Q}$를 가질때

$y^2=(x-\alpha)^3$

$y=\lambda(x-\alpha)$와 이것과 교점은 $x=\alpha+\lambda^2$; 모두 유리수점

(2) 이중근인 경우

$y^2=(x-\alpha)^2(x-\beta)$

$y=\lambda(x-\alpha)$ 로 두면

$\lambda^2=x-\beta$ $x=\beta+\lambda^2$

유리점 $(\beta+\lambda^2,\ \lambda(\beta-\alpha+\lambda^2))$

(3) 근이 다 다른 경우

$y^2=(x-\alpha)(x-\beta)(x-\gamma)$

$=x^3+ax^2+bx+c$

$=\left(x+\frac{a}{3}\right)^3+a'\left(x+\frac{a}{3}\right)+a''$

일반적일지 않고 x^2항을 없앨수 있다.

판별식 : $(\alpha-\beta)^2$

. 2차식 $D=(\alpha-\beta)^2$

$x^2+bx+c=0$ $=(\alpha+\beta)^2-4\alpha\beta$

에서 $=b^2-4c$

$b,c\in\mathbb{R}$

$D>0$: $\alpha\neq\beta$. 실수

$D=0$: $\alpha=\beta$. 실수.

$D<0$: $\alpha\neq\beta$. 허수.

$\alpha=\bar{\beta}$

. 3차식 . $x^3+ax+b=0$

의 근 α,β,γ

$D=(\alpha-\beta)^2(\beta-\gamma)^2(\gamma-\alpha)^2$

$D=0$: 중근, 3중근

$D\neq0$: 세근이 서로 다름.

morning glory

방정식, 다항식

Ex 1. (1968 IMO) $x_1, x_2, \cdots, x_n$: 미지수 a, b, c : 실수 $a \neq 0$

$$\begin{cases} ax_1^2 + bx_1 + c = x_2 \\ ax_2^2 + bx_2 + c = x_3 \\ \vdots \\ ax_{n-1}^2 + bx_{n-1} + c = x_n \\ ax_n^2 + bx_n + c = x_1 \end{cases}$$

$D = (b-1)^2 - 4ac$ 라 할때

i) $D < 0$ ⇒ 실근이 없다

ii) $D = 0$ ⇒ 실근이 하나

iii) $D > 0$ ⇒ 실근이 둘이상

일을 보여라.

(풀이) $i = 1, 2, \cdots, n$, $x_{n+1} = x_1$.

$$ax_i^2 + bx_i + c = x_{i+1}$$

$$ax_i^2 + (b-1)x_i + c = x_{i+1} - x_i$$

$y = Ax^2 + Bx + C$ 에서 $D = B^2 - 4AC < 0$ 인 경우 $A(Ax^2 + Bx + C) > 0$ $\forall x$

(i) $D < 0$ 인 경우

$$0 < a\left(ax_i^2 + (b-1)x_i + c\right) = a(x_{i+1} - x_i)$$

$$\therefore ax_i < ax_{i+1}$$

$$ax_1 < ax_2 < ax_3 < \cdots < ax_n < ax_1 \quad : \text{모순}$$

$\therefore x_i$ 가 실수가 아님 (i.e. 실근이 없다)

(ii) $D = 0$ 인 경우

$$ax_i^2 + (b-1)x_i + c$$

$$= a\left(x_i + \frac{b-1}{2a}\right)^2 = x_{i+1} - x_i$$

$$a^2\left(x_i + \frac{b-1}{2a}\right)^2 = a(x_{i+1} - x_i) \geq 0$$

$$ax_1 \leq ax_2 \leq \cdots \leq ax_n \leq ax_1$$

즉 모두 등호가 성립해야 한다

$$\therefore x_1 = x_2 = \cdots = x_n$$

(iii) $D > 0$ 인 경우

$$ax_i^2 + (b-1)x_i + c = x_{i+1} - x_i$$

$at^2 + (b-1)t + c = 0$ 의 두 실근을 α, β 라 하자. $(\alpha \neq \beta)$

$x_1 = x_2 = \cdots = x_n = \alpha$

or

$x_1 = x_2 = \cdots = x_n = \beta$ 가 성립한다 (위식의 근이다)

즉 적어도 2근이 존재한다.

Ex 1-1. $\begin{cases} (x_1-1)(x_1-2)=x_2-x_1 \\ (x_2-1)(x_2-2)=x_1-x_2 \end{cases}$ 을 풀어라

(정근) 해가 2개

Ex 1-2. $\begin{cases} (x_1-1)(x_1-4)=x_2-x_1 \\ (x_2-1)(x_2-4)=x_1-x_2 \end{cases}$ 을 풀어보라.

실근이 4개.

Ex 2. (1984 U.S.M.O)

$x^4-18x^3+kx^2+200x-1984=0$

의 4개의 근중 2개의 곱이 -32일때 $k=?$

(풀이 I) 근이 $\alpha, \beta, \gamma, \delta$ 라 하자.

근과 계수사이의 관계에 의해

$\alpha\beta\gamma\delta = -1984$ ···①

$\alpha\beta\gamma+\alpha\beta\delta+\alpha\gamma\delta+\beta\gamma\delta=-200$ ···②

$\alpha+\beta+\gamma+\delta=-18$ ···③

$\alpha\beta+\alpha\gamma+\alpha\delta+\beta\gamma+\beta\delta+\gamma\delta=k$ ···④

이렇게 해서 $\alpha\beta=-32$ 로 두고 풀면 된다.

(풀이 II) 근중 2개의 곱이 -32 이므로 다른 2개의 곱은 $\frac{-1984}{-32}=62$ 이다

$\therefore x^4-18x^3+kx^2+200x-1984$

$=(x^2+px-32)(x^2+qx+62)$

3차항: $-18=p+q$ ···①

2차항: $k=62+pq-32=30+pq$ ···②

1차항: $200=62p-32q$ ···③

③': $100=31p-16q$

③'+16×① $-188=47p$ $\quad p=-4$

$q=-14$.

$\therefore k=30+4\times14=86$

Ex 3. (1983. U.S.M.O)

$2a^2<5b$ 일때 (단, a, b, c, d, e 는 실수)

$x^5+ax^4+bx^3+cx^2+dx+e=0$

는 적어도 하나의 허근을 갖는다

(풀이) 근이 $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$ 라 하고 모두 실수라 하자.

morning glory

근과 계수사이의 관계에 의해

$$-a = \alpha_1+\alpha_2+\alpha_3+\alpha_4+\alpha_5 = \sum \alpha_i$$

$$b = \alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_1\alpha_4+\alpha_1\alpha_5+\alpha_2\alpha_3+\alpha_2\alpha_4+\alpha_2\alpha_5+\alpha_3\alpha_4+\alpha_3\alpha_5+\alpha_4\alpha_5 = \sum \alpha_i\alpha_j$$

$$\therefore\ a = -\sum \alpha_i$$

$$b = \sum \alpha_i\alpha_j$$

$$2a^2-5b$$

$$= 2\left(\sum_{i=1}^{5}\alpha_i\right)^2 - 5\left(\sum \alpha_i\alpha_j\right)$$

여기서 $\sum$ 는 $\sum_{1\le i<j\le 5}$ 이다

$$= 2\sum_{i=1}^{5}\alpha_i^2 + 4\sum \alpha_i\alpha_j - 5\sum \alpha_i\alpha_j$$

$$= 2\sum_{i=1}^{5}\alpha_i^2 - \sum \alpha_i\alpha_j$$

$$= \frac{1}{2}\sum (\alpha_i-\alpha_j)^2 \ge 0$$ 이므로 $2a^2 \le 5b$ 에 모순

$\therefore$ 적어도 1개의 허근이 존재한다.

Ex 4. (1993 IMO) $a, b \in \mathbb{R}$

$x^4+ax^3+bx^2+ax+1=0$ 이 최소한 하나의 실근을 갖게 하는 a, b 중 a^2+b^2 의 최소값을 구하라

(풀이) $\left(x^2+\frac{1}{x^2}\right)+a\left(x+\frac{1}{x}\right)+b=0$

$x+\frac{1}{x}=y$ 라 두면 $x\in\mathbb{R}$ 일때, $y\le -2$ 또는 $y\ge 2$.

$y^2+ay+b-2=0 \quad \cdots ①$

즉 ①이 최소한 $y\le -2$, $y\ge 2$ 에서 실근을 적어도 하나 가져야 한다.

(i) $-\frac{a}{2}>0$ 인 경우 : 대칭축이 y축 오른쪽에 있다.

원하는 실근이 존재할 조건은 $y=2$일때 0 이하여야 한다.

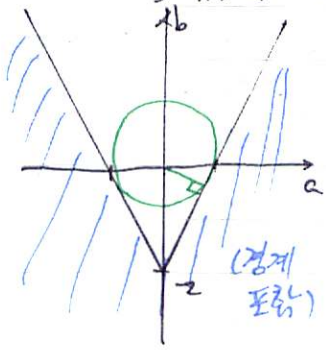
$$4+2a+b-2\le 0$$

(ii) $-\frac{a}{2}\le 0$ 인 경우

마찬가지로 $y=-2$일때 0 이하여야 한다

$$4-2a+b-2<0$$

i) ii) 의 그래프를 그리자



직선식은

$2a+b+2=0$

$2a-b-2=0$

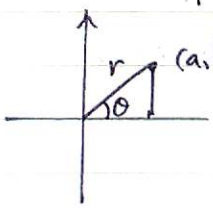
이때 구하는 영역은 왼쪽 그래프의 타원색부분과 같다.

a^2+b^2의 최소값은 직선의 방정식과 원점과 거리의 제곱이 되므로

a^2+b^2 최소는 $\left(\frac{|2\cdot 0+0+2|}{\sqrt{2^2+1^2}}\right)^2 = \frac{4}{5}$

◦ 복소수 $z=a+bi \Leftrightarrow$ 복소평면 $(a,b) \Leftrightarrow$ vector (a,b)

$P(a,b)$ 라 하고 원점이 O 일때



$OP=r \quad (r\geq 0)$ 라고 하고

OP와 x축 양의 방향이 이루는 각 θ라 두면

$a=r\cos\theta,\ b=r\sin\theta$

$\therefore z=r(\cos\theta+i\sin\theta)=re^{i\theta}$

이때 $r=|z|$

$e^{i\theta}=\cos\theta+i\sin\theta$ 〈정의〉

De Moivre 정리

$z^n=r^n(\cos\theta+i\sin\theta)^n$

$=r^n(\cos n\theta+i\sin n\theta) \qquad n\in\mathbb{Z}$

i.e. $(e^{i\theta})^n=e^{in\theta}$

$w=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$ 일때 $w^n=1$

$x^n=1$ 의 근은 $\underbrace{1, w, w^2, \cdots, w^{n-1}}_{n\text{개}}$ 그 합은 0

Ex 5. $\cos\frac{2\pi}{n}$ 을 근으로 갖는 가장 차수가 낮은 유리수계수의 다항식은?

(풀이) $w=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$

$1+w+w^2+w^3+w^4+w^5+w^6=0$

$w^6=w^{-1}$

$w^5=w^{-2}$

$w^4=w^{-3}$

$w+w^6=w+w^{-1}=2\cos\frac{2\pi}{n}$

$w^2+w^5=w^2+w^{-2}=(w+w^{-1})^2-2=\left(2\cos\frac{2\pi}{n}\right)^2-2$

$w^3+w^4=w^3+w^{-3}=(w+w^{-1})^3-3(w+w^{-1})=\left(2\cos\frac{2\pi}{n}\right)^3-3\left(2\cos\frac{2}{n}\pi\right)$

$\cos\frac{2\pi}{n}=x$ 라 두면

$1+2x+4x^2-2+8x^3-6x=0$

$8x^3+4x^2-4x-1=0$: $\cos\frac{2\pi}{n}$ 을 근으로 가짐

$\pm\frac{(1\text{의 약수})}{(8\text{의 약수})}$ 을 대입해보고, 유리근존재 여부를 가린다

그러나 $8x^3+4x^2-4x-1=0$ 은 유리근을 갖지 못한다

$\therefore 8x^3+4x^2-4x-1=0$ 이 찾는 방정식이다

Ex 6. $\cos\frac{\pi}{n}-\cos\frac{2\pi}{n}+\cos\frac{3\pi}{n}=\frac{1}{2}$ 임을 보여라

(1963 IMO)

(풀이) $w=\cos\frac{\pi}{n}+i\sin\frac{\pi}{n}$, $w^n=-1$

morning glory

$$w-w^2+w^3-w^4+w^5-w^6 = \frac{w(1-w^6)}{1-(-w)} = \frac{w-w^7}{1+w} = \frac{w+1}{w+1} = 1$$

실수부만 비교하면

$$\cos\frac{\pi}{7} - \cos\frac{2}{7}\pi + \cos\frac{3}{7}\pi - \cos\frac{4\pi}{7} + \cos\frac{5}{7}\pi - \cos\frac{6}{7}\pi = 1$$

$$-\cos\frac{6}{7}\pi = \cos\frac{\pi}{7}$$

$$\cos\frac{5}{7}\pi = -\cos\frac{2}{7}\pi$$

$$-\cos\frac{4}{7}\pi = \cos\frac{3}{7}\pi$$

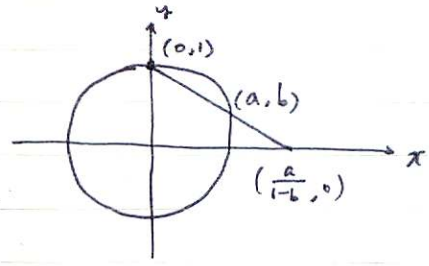
$$\therefore \quad 2\left(\cos\frac{\pi}{7} - \cos\frac{2}{7}\pi + \cos\frac{3}{7}\pi\right) = 1$$

$$\cos\frac{\pi}{7} - \cos\frac{2}{7}\pi + \cos\frac{3}{7}\pi = \frac{1}{2}$$

조밀하다 : 어떤 작은 구간을 잡아도 (유리점)가 존재

정리. 단위원상에 유리수를 좌표를 갖는 점은 조밀하다

(증명) 단위원 : T



$$f : T - \{(0,1)\} \longrightarrow \mathbb{R}$$

$$(a,b) \longrightarrow \frac{a}{1-b}$$

역함수를 g라 하면

$$\begin{cases} \frac{a}{1-b} = t \\ a^2+b^2 = 1 \end{cases}$$

$$(1-b)^2t^2 + b^2 = 1$$

$$b^2(1+t^2) + t^2 - 1 - 2t^2b = 0$$

$$b^2(1+t^2) - 2t^2b + t^2 - 1 = 0$$

$$(b-1)\left((t^2+1)b - (t^2-1)\right) = 0$$

$b \neq 1$, $\therefore \quad b = \frac{t^2-1}{t^2+1}$

$$a = (1-b)t = \frac{2t}{t^2+1}$$

$$\therefore g(t) = \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}\right)$$

f에 의해 단위원상의 유리수점중 $(0,1)$은 제외한 것과, x축 위 유리수점이 일대일 대응된다. x축위 유리수점은 조밀하다.

따라서 단위원상에 있는 유리수점은 조밀하다.

Ex 7. (1975 IMO)

단위원에 임의의 두점의 거리가 모두 유리수인 1975개의 점이 있는가?

풀이) $w = \cos\theta + i\sin\theta$, $0 < \theta < \frac{2\pi}{1975}$ 을 생각하자.

$w, w^2, \cdots, w^{1975}$ 를 생각하자.

$$|w^i - w^j|$$

$$= |w^i(1 - w^{j-i})|$$

$$= |1 - w^{i-j}|$$

$= |1-w^n|$ let $n=j-i$.

$= |1-\cos n\theta - i\sin n\theta|$

$= |2\sin^2\frac{n}{2}\theta - i\,2\sin\frac{n}{2}\theta\cos\frac{n}{2}\theta|$

$= |2\sin\frac{n}{2}\theta|\,|\sin\frac{n}{2}\theta - i\cos\frac{n}{2}\theta|$

$= 2|\sin\frac{n}{2}\theta|$

$\alpha = \cos\frac{\theta}{2} + i\sin\frac{\theta}{2}$ 가 유리수좌표를 갖는다면

$\alpha^2, \alpha^3, \cdots, \alpha^n, \cdots$ 모두 유리수좌표를 갖는다.

$\therefore$ $\cos\frac{\theta}{2}$, $\sin\frac{\theta}{2}$가 유리수이면

$\cos\frac{n\theta}{2}$, $\sin\frac{n\theta}{2}$가 유리수가 된다.

$0<\theta<\frac{2\pi}{1995}$ 되는 범위중

θ를 $\cos\frac{\theta}{2}$, $\sin\frac{\theta}{2}$가 유리수되게 잡으면 (유리수점은 조밀) ↓ 앞페이지 참조.

$w, w^2, \cdots, w^{1995}$ 는 임의의 두점사이 거리가 유리수.

※ α를 근으로 갖는 다항식 중에서 차수가 최소인것 $= h(x)$

$f(x)$가 α를 근으로 갖는다면

$f(x)=h(x)g(x)$ 게 된다.

이것을 다항식을
① 정수계수
② 유리수계수
③ 실수계수 ④ 복소수계수
로 제한해서 생각해야 한다

(증명) $f(x)=h(x)g(x)+r(x)$

degree $r <$ degree h

$x=\alpha$. $f(\alpha)=h(\alpha)g(\alpha)+r(\alpha)$

$r(\alpha)=0$

$h(x)$가 차수가 최소이니 $r(x)=0$

$\therefore f(x)=h(x)g(x)$

일반적으로
유리수, 실수일때는
$f(x)$를 임의의 유리수(혹은 실수)계수
다항식으로 나눠도 몫과 나머지는 마찬가지이다. (단 1회만)

※ $f(x)$의 계수가 정수일때

$f(x)$를 $x-k$로 나누면 $k\in\mathbb{Z}$

나머지 : 정수

몫 : 정수계수

Ex 8. (1963. IMO)

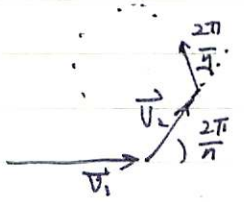
내각이 모두 같은 n각형에서 이웃한 변들의 길이가 부등식

$a_1 \geq a_2 \geq \cdots \geq a_n$

을 만족하면 $a_1 = a_2 = \cdots = a_n$

(풀이) $w=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$

morning glory



$\vec{v_1}+\vec{v_2}+\cdots+\vec{v_n}=0$

복소수로 생각

$a_1+a_2\omega+a_3\omega^2+\cdots+a_n\omega^{n-1}=0 \quad \cdots ①'$

실수부 $a_1+a_2\cos\frac{2\pi}{n}+a_3\cos\frac{4\pi}{n}+\cdots+a_n\cos\frac{2(n-1)}{n}\pi=0 \quad \cdots ①$

허수부 $a_2\sin\frac{2}{n}\pi+a_3\sin\frac{4\pi}{n}+\cdots+a_n\sin\frac{2(n-1)}{n}\pi=0 \quad \cdots ②$

허수부를 생각하였음

②에서

$(a_2-a_n)\sin\frac{2\pi}{n}+(a_3-a_{n-1})\sin\frac{4\pi}{n}+\cdots+\cdots=0$

0. 양수 모든항 0. 양수 모든항

합이 0이려면

$a_2=a_n, \quad a_3=a_{n-1} \cdots$

즉 $a_2=a_3=a_4=\cdots=a_n$

①'에서 $a_1+a_2(\omega+\omega^2+\cdots+\omega^{n-1})=0$

$a_1+a_2(0-1)=0$

$a_1-a_2=0 \quad \therefore a_1=a_2$

$\therefore a_1=a_2=a_3=\cdots=a_n$

Ex 9. (1974 IMO)

$P(x)=x$ 라면 $P(x)$: 정수계수를 갖는 다항식

$n(P)=2$ ($\because x^2-1=0$, $x=\pm1$) $P(x)^2-1=0$ 의 정수해의 개수를 $n(P)$ ← 중근은 1개로 센다.

$n(P)\leq \deg P+2$

$\deg P$: $P(x)$의 차수

(풀이) $\deg P=d$

$P(x)+1=0, \quad P(x)-1=0$

$P(x)+1=0$ 의 정수해를 $k_1, k_2, \cdots, k_r$ 라 두면

단 $k_1<k_2<\cdots<k_r$

$P(x)+1=(x-k_1)(x-k_2)\cdots(x-k_r)Q(x) \quad \cdots ⑧$

↳ 정수계수 다항식.

$P(x)-1=0$ 의 한 정수해를 l 라 하자.

$x=l$을 ⑧에 대입하면

$2=(l-k_1)(l-k_2)\cdots(l-k_r)Q(l)$

(위에서 $r=1, 2$ 일때는 $P(x)+1=0$ 의 정수해 : 2개 이하

즉 $r\geq3$을 가정. $P(x)-1=0$ 의 정수해 : d개 이하 이나 명백)

$l-k_1, l-k_2, \cdots, l-k_r$은 서로 다른 정수이고 $Q(l)$도 정수이며,

곱해서 2이므로, 또한 $l-k_1>l-k_2>l-k_3>\cdots>l-k_r$

그런데 곱해서 2이므로 $2\times 1\times -1\times(-1)$

$1\times(-1)\times(-2)\times(1)$

$\uparrow\ \uparrow\ \uparrow$

$l-k_1\quad l-k_2\quad l-k_3$

인 경우 뿐이다. 즉 $r=3$

즉 $l=k_1+2=1+k_2=-1+k_3$

또는

$l=k_1+1=k_2-1=k_3-2$

즉 $P(x)-l=0$ 의 해는 많아야 2개

즉 $n(P)\le 5\le \deg P+2$ $(\because \deg P\ge 3)$

$(r\ge 3$을 가정했었음)

$\therefore n(P)\le \deg P+2$

Ex 10. (1911년 U.S.M.O)

$P(x)$: 정수계수

$a_1, a_2, \cdots, a_n$: 서로다른 정수 $(n\ge 3)$

$P(a_1)=a_2,\ P(a_2)=a_3,\ \cdots\ P(a_{n-1})=a_n\quad P(a_n)=a_1$

인 P가 없다

(풀이) $P(x)-P(a_i)=(x-a_i)Q_i(x)$ $(\because x=a_i$ 하면 나머지가 0)

$x=a_{i+1}$ ↳정수계수

$P(a_{i+1})-P(a_i)=(a_{i+1}-a_i)Q_i(a_{i+1})$

$a_{i+2}-a_{i+1}=(a_{i+1}-a_i)Q_i(a_{i+1})$

변변곱하면 $\prod_{i=1}^{n} Q_i(a_{i+1})=1.$

$\therefore Q_i(a_{i+1})=1$ or -1

if $Q_i(a_{i+1})=-1.$

$a_{i+2}-a_{i+1}=-(a_{i+1}-a_i)$

$a_{i+2}=a_i$ 이므로 모순

$\therefore Q_i(a_{i+1})=1$

$\therefore a_{i+2}-a_{i+1}=a_{i+1}-a_i$

$a_1-a_2=a_2-a_3=\cdots=a_{n-1}-a_n=a_n-a_1=k$

$a_1=a_2+k$ 변변 더하면 $k=0$

$a_2=a_3+k$ $\therefore a_1=a_2=\cdots=a_n$

$\vdots$

$a_n=a_1+k$ 즉 만족하는 P가 없다

• $P(x,y)$ $\quad P(x,y)=3x^2+6xy^3$: 차수 4

동차식 : 차수가 모두 같은 항으로만 구성된 다항식

ex) $x^3+y^3+x^2y+xy^2$

임의의 다항식은 동차식의 합으로 표현할 수 있다.

• P가 동차식, 차수 n

$\Leftrightarrow P(tx,ty)=t^n P(x,y) \quad \forall t$

$\because (\Leftarrow) P=P_0+P_1+\cdots+P_d$

P_i 각각은 i차의 동차식

$P(tx,ty)$

$= P_0(x,y)+tP_1(x,y)+t^2P_2(x,y)+\cdots+t^dP_d(x,y)$

• (a,b)가 $P(x,y)=0$ 의 근이면 단 P는 동차식

$P(x,y)$가 $(bx-ay)$로 나누어 떨어진다.

(∵)

$P(x,y)=a_0x^ny^0+a_1x^{n-1}y^1+\cdots+a_nx^0y^n$

$=y^n\left(a_0\left(\frac{x}{y}\right)^n+a_1\left(\frac{x}{y}\right)^{n-1}+\cdots+a_n\right)$

$t=\frac{x}{y}$ 라 하자

if $b=0$ 라면

$P(a,0)=0$. $\quad a_0=0$.

$P(x,y)=yQ(x)$ 에서 ay로 나누어진

$b\neq 0$ $\quad t=\frac{x}{y}$ 라 두면

$a_0t^n+a_1t^{n-1}+\cdots+a_n=\left(t-\frac{a}{b}\right)Q(x)$

$\therefore P(x,y)=y^n\left(\frac{bx-ay}{by}\right)Q(x)$

$=\frac{1}{b}y^{n-1}Q(x)\cdot(bx-ay)$

즉 $bx-ay$로 나누어 떨어진다.

Ex 11. (1995 IMO)

다음 조건을 만족하는 두변수의 다항식 P를 모두 찾아라.

(i) $P(tx,ty)=t^nP(x,y) \quad \forall t,x,y\in\mathbb{R}$

(ii) $P(a+b,c)+P(b+c,a)+P(c+a,b)=0 \quad \forall a,b,c\in\mathbb{R}$

(iii) $P(1,0)=1$.

(풀이) $\quad a+b=1,\ c=-1 \quad b=1-a$

$P(1,-1)+P(1-a-1,a)+P(-1+a,1-a)=0$

$P(1,-1) + (-a)^n P(1,-1) + (a-1)^n P(1,-1) = 0$

$\{1 + (-a)^n + (a-1)^n\} P(1,-1) = 0 \quad \forall a \in \mathbb{R}$

if $n \geq 2$, $1 + (-a)^n + (a-1)^n$ 이 항상 0일 수 없으므로 (근이 많아야 n개)

$P(+1,-1) = 0$

먼저 $a=b=c=1$ 이면

$P(2,1) = 0$

$\therefore P(x,y)$는 $(x-2y)$를 인수로 가진다.

$n=1$ 이라면 P의 차수가 1인 동차식.

$\therefore P(x,y) = k(x-2y)$

$P(1,0) = k = 1 \quad \therefore P(x,y) = x-2y$

이때 $P(a+b,c) + P(b+c,a) + P(c+a,b)$

$= a+b-2c + b+c-2a + c+a-2b$

$= 0$

$\therefore \quad n=1 \; ; \; P(x,y) = x-2y$

$n \geq 2$인 경우만 보자

P는 $x+y$라는 인수를 가진다

$P(x,y) = (x+y)\,Q(x,y)$

$Q(tx,ty) = \frac{P(tx,ty)}{t(x+y)} = t^{n-1} Q(x,y)$ ····· ①

$\therefore Q$는 $n-1$차 동차식.

$Q(1,0) = P(1,0) = 1$ ····· ③

$Q(a+b,c) + Q(b+c,a) + Q(c+a,b)$ ····· ④

$= \frac{P(a+b,c) + P(b+c,a) + P(c+a,b)}{a+b+c} \quad (a+b+c \neq 0)$

$= 0$

다항식은 연속이므로, $a+b+c=0$일때도 ④가 성립.

$a+b+c=0$ 일때, $a^b c$ 고정

$b \leftarrow b+\varepsilon$ 을 대입한후

$\varepsilon \to 0$ 하면, 이것이 연속인

ε의 함수이니, $\varepsilon=0$ 일때도 그값이 0.

①, ③, ④에 의해

$Q(x,y)$도 문제의 3개 성질을 만족한다.

Q에 대해 이런식으로 계속하면

$P(x,y) = (x+y)^{n-1}(x-2y) \quad (n \geq 2)$

역으로 이것은 실제로 문제의 성질을 갖는다.

$\therefore$ 구하는 해는

$$\begin{cases} P(x,y) = (x+y)^{n-1}(x-2y) & n \geq 2 \\ P(x,y) = x-2y & n=1 \end{cases}$$

morning glory