제1판

중등임용 전공수학 대비

윤양동 임용수학

I

윤양동 편저

정수론
선형대수
조합론
확률통계

Mathematics

박문각 임용 동영상강의 www.pmg.co.kr

박문각

차 례

Contents

PART 4 조합 및 그래프

PART 5 확률 및 통계

윤양동

임용수학

Mathematics

PART

1

정수론

Chapter

01 합동방정식의 해법

01 합동식의 정의와 성질

1. 합동식

(1) 합동식의 뜻

법 n에 관한 합동식 $a \equiv b \pmod{n}$은 $n \mid a-b$와 동치이다. 즉,

a, b는 n으로 나눈 나머지가 같다는 뜻이다.

[합동식의 정의] $\quad a \equiv b \pmod{n} \leftrightarrow n \mid a-b$

이때, n이 m의 약수일 때 $n \mid m$라 표기한다. 즉, m은 n의 배수이다.

약수-배수에 관한 몇 가지 성질을 살펴보자. (단, 모든 문자는 정수이다.)

① $m \mid n$, $n \mid m$ 이면 $n = \pm m$

② $k \mid n$, $n \mid m$ 이면 $k \mid m$

③ $n \mid m_1$, $n \mid m_2$ 이면 $n \mid am_1 + bm_2$

④ $n \mid m$ 일 필요충분조건은 $kn \mid km$ (단, $k \neq 0$)

⑤ $\gcd(n, k) = 1$ 일 때, $n \mid m$ 일 필요충분조건은 $n \mid km$ (Euclid lemma)

⑥ p가 소수(prime)일 필요충분조건은 $p \mid nm \rightarrow p \mid n$ 또는 $p \mid m$
(단, $p \neq 0, \pm 1$)

위의 성질들 중에서 ③, ④, ⑤, ⑥을 합동식으로 바꿔 표현해보자.

③ $m_1 \equiv 0 \pmod{n}$, $m_2 \equiv 0 \pmod{n}$ 이면
$am_1 + bm_2 \equiv 0 \pmod{n}$

합동식을 조작하는 기본적인 기능을 모아놓은 것이다.

④ $a \equiv b \pmod{n} \leftrightarrow ka \equiv kb \pmod{kn}$ (단, $k \neq 0$)

⑤ $\gcd(n, k) = 1$ 일 때,
$a \equiv b \pmod{n} \leftrightarrow ka \equiv kb \pmod{n}$ (Euclid lemma)

⑥ p가 소수일 때,
$nm \equiv 0 \pmod{p} \leftrightarrow n \equiv 0 \pmod{p}$ 또는 $m \equiv 0 \pmod{p}$

(2) 최대공약수와 최소공배수의 성질

합동식을 처리하기 위해 알아야 할 정수에 관한 성질로서 최대공약수 (greatest common divisor)와 최소공배수(least common multiple)의 성질이 있다. 정수에 관한 최대공약수(gcd)와 최소공배수(lcm)는 약수/배수의 관계에 의하여 정의하며, 최대공약수는 양의 정수로 정의한다.

두 정수 a, b의 최대공약수는 $\gcd(a, b)$ 또는 간단히 (a, b)로 표기하고, 최소공배수는 $\mathrm{lcm}(a, b)$ 또는 간단히 $[a, b]$로 표기한다.

최대공약수와 최소공배수의 몇 가지 성질을 살펴보자.

① 양의 정수 a에 대하여 $\gcd(a, 0) = a$, $\gcd(a, 1) = 1$

② $\gcd(a, b) = \gcd(b, a)$

③ $\gcd(a, b) = \gcd(a, b+ka)$

④ $\gcd(a, b) = 1 \leftrightarrow as + bt = 1$ 인 정수 s, t가 존재한다.

⑤ $\gcd(a, b) = d \rightarrow as + bt = d$ 인 정수 s, t가 존재한다. (역은 성립하지 않는다.)

⑥ $\gcd(ka, kb) = k \cdot \gcd(a, b)$

⑦ $\gcd(a, b) = 1$이면 $\gcd(ab, n) = \gcd(a, n)\gcd(b, n)$

⑧ $\gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c))$

연산의 결합법칙과 유사하다.

⑨ $ab = \mathrm{lcm}(a, b) \cdot \gcd(a, b)$

⑩ $n \mid a$, $n \mid b \leftrightarrow n \mid \gcd(a, b)$

⑪ $a \mid m$, $b \mid m \leftrightarrow \mathrm{lcm}(a, b) \mid m$

⑫ $\gcd(\mathrm{lcm}(a, b), c) = \mathrm{lcm}(\gcd(a, c), \gcd(b, c))$

⑬ $\mathrm{lcm}(\gcd(a, b), c) = \gcd(\mathrm{lcm}(a, c), \mathrm{lcm}(b, c))$

⑭ $2 \le q$, $1 \le n, m$일 때, $n \mid m \leftrightarrow q^n - 1 \mid q^m - 1$

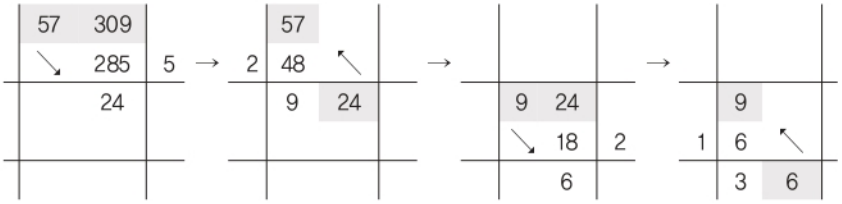
⑮ $2 \le q$, $1 \le n, m$일 때, $\gcd(q^n - 1, q^m - 1) = q^{\gcd(n, m)} - 1$

위의 성질 중에서 ①, ②, ③은 유클리드 알고리즘의 원리이며, ④, ⑤의 정수 s, t를 구하는 방법을 제시한다. 유클리드 알고리즘이란 나눗셈을 반복하는 절차를 말한다. 57과 309의 최대공약수 3을 구하는 유클리드 알고리즘 과정을 따라가면 아래와 같다.

$\gcd(57, 309) = \gcd(57, 24) = \gcd(9, 24) = \gcd(9, 6) = \gcd(3, 6)$

$= \gcd(3, 0) = 3$

위의 과정을 정리하면 아래의 절차를 얻는다. $a = 57$, $n = 309$라 두고 반복하면 다음과 같다.



유클리드 알고리즘을 두 번 사용하는 절차는 자주 사용하게 된다.

	57	309			a	n	
2	48	285	5	→ 2	$2n-10a$	$5a$	5
	9	24			$11a-2n$	$n-5a$	
1	6	18	2	1	$5n-27a$	$22a-4n$	2
	3	6			$38a-7n$	$5n-27a$	

오른쪽의 마지막 식이 $38a-7n = 38\times 57 - 7\times 309 = 3$이므로 성질 ⑤의 s, t를 알 수 있다.

(3) 유클리드 알고리즘과 연분수(continued fraction)

정수a_0 와 양의 정수 a_k $(k \geq 1)$를 사용하여 $a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$ 와 같이 실수를 표현하는 것을 연분수(continued fraction)라 하고 간단히 $[a_0 ; a_1 , a_2 , a_3 , \cdots]$으로 표기한다.

연분수의 수열 a_k가 유한수열이면 유한 연분수(finite continued fraction)라 하며, 모든 유한 연분수는 유리수이고, 모든 유리수는 유클리드 알고리즘을 써서 유한 연분수로 나타낼 수 있다. 예를 들어, 유리수 $\frac{25}{11}$ 를 연분수로 나타내기 위해 11, 25에 유클리드 알고리즘을 적용하면

②	11	25	①
3	9	22	2
④	2	3	③
2	2	2	1
	0	1	

$$\frac{25}{11} = 2+\frac{1}{11/3} \rightarrow \frac{11}{3} = 3+\frac{1}{3/2} \rightarrow \frac{3}{2} = 1+\frac{1}{2}$$

$$\frac{25}{11} = 2+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{2}}} = [2;3,1,2]$$

무한 연분수의 사례도 살펴보자.

무한연분수 $x = [1;1,1,1,\cdots]$라 하면 $x-1 = [0;1,1,1,\cdots]$,

$\frac{1}{x-1} = [1;1,1,1,\cdots] = x$이므로 $x^2-x-1=0$을 만족한다.

따라서 $x = \frac{1+\sqrt{5}}{2}$ 이다.

무리수 $\sqrt{2}$ 의 연분수를 구해보면 $\sqrt{2}-1 = \frac{1}{\sqrt{2}+1}$, $\sqrt{2}+1 = 2+\frac{1}{\sqrt{2}+1}$ 이므로 $\sqrt{2}+1 = [2;2,2,2,\cdots]$. 따라서 $\sqrt{2} = [1;2,2,2,\cdots]$이다.

2. 합동식에 관한 정리

(1) 오일러(Euler) 정리와 페르마(Fermat) 정리

[오일러 정리] $\gcd(a,n)=1 \leftrightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$

$\varphi(n)$는 오일러 φ-함수이며, $\varphi(n)$= n과 서로 소인 n 이하의 자연수 개수

n이 소수 p인 경우 다음과 같이 정리할 수 있다.

① 페르마 정리: $\gcd(a,p)=1 \leftrightarrow a^{p-1} \equiv 1 \pmod{p}$

이때 소수 p인 경우 $a^p \equiv a \pmod{p}$가 성립하므로 다음 성질이 있다.

② 따름 정리: 소수 p에 대하여 $(a+b)^p \equiv a^p + b^p \pmod{p}$

(2) 윌슨(Wilson) 정리

[윌슨(Wilson) 정리] $p \geq 2$일 때, p는 소수(prime number)
$\leftrightarrow (p-1)! \equiv -1 \pmod{p}$

특히, $3 \leq p$인 소수이면 $\left\{\left(\frac{p-1}{2}\right)!\right\}^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$도 성립한다.

예제 1 $2 \leq q$, $1 \leq n, m$일 때, $m \mid n \leftrightarrow q^m-1 \mid q^n-1$임을 보이시오.

풀이 ($\rightarrow$) $m \mid n$이라 하면 $n=mk$라 쓸 수 있으며

$q^n-1 = q^{mk}-1 = (q^m-1)\{(q^m)^{k-1}+(q^m)^{k-2}+\cdots+q^m+1\}$

이므로 $q^m-1 \mid q^n-1$

($\leftarrow$ 대우증명) $m \nmid n$이라 하면 $n=mk+r$(단, $1 \leq r < m$)라 쓸 수 있으며

$q^{mk+r}-1 = q^{mk+r}-1 = q^{mk+r}-q^r+q^r-1$

$= (q^m-1)q^r\{(q^m)^{k-1}+(q^m)^{k-2}+\cdots+q^m+1\}+q^r-1$

(단, $1 \leq q-1 \leq q^r-1 < q^m-1$)이므로 $q^m-1 \nmid q^n-1$

따라서 자연수 $q \geq 2$에 대하여 $m \mid n$ 일 필요충분조건은 $q^m-1 \mid q^n-1$ 이다.

2024 고객선호브랜드지수 1위
교육서비스 부문

2023 고객선호브랜드지수 1위
교육서비스 부문

2022 한국 브랜드 만족지수 1위
교육(교육서비스)부문 1위

2021 대한민국 소비자 선호도 1위
교육부문 1위 선정

2020 한국 산업의 1등
브랜드 대상 수상

2019 한국 우수브랜드평가대상
교육브랜드 부문 수상

2018 대한민국 교육산업 대상
교육서비스 부문 수상

브랜드스탁 BSTI
브랜드 가치평가 1위

박문각 www.pmg.co.kr

교재관련 문의 02 - 6466- 7202
학원관련 문의 02 -816 -2030
온라인강의 문의 02 - 6466 - 7201

윤양동
임용수학

I

정수론 선형대수 조합론 확률통계

Mathematics

14410
9 791172 624903
정가 20,000원
ISBN 979-11-7262-490-3
ISBN 979-11-7262-489-7(SET)