

2015학년도 전공수학 중등교원임용시험 대비

정현민 전공수학

정수론 기출분석

정 현 민 편저



PMG
박문각교육

박문각임용고시학원

(구) 노량진행정고시학원 www.ngosi.co.kr 02) 816-2030

1. 서론

유한 귀납법의 기본원리

양의 정수들로 이루어진 집합 S 가 다음 두 가지 성질을 만족한다고 하자.

- (i) 정수 1은 S 에 속한다.
 - (ii) 정수 k 가 S 에 속하면, $k+1$ 또한 S 에 속한다.
- 그러면 S 는 모든 양의 정수를 가진다.

2. 정수의 나눗셈정리

- (1) $a, b (b \neq 0)$ 가 정수이면 $a = qb + r$, $0 \leq r < |b|$ 을 만족하는 유일한 정수 q, r 이 존재한다.

$a|b, a \nmid b$

$c \in \mathbb{Z}$ 가 존재하여 $b = ac$ 를 만족할 때 b 는 $a (a \neq 0) \in \mathbb{Z}$ 로 나누어진다고 표현하고 $a|b$ 로 쓴다.
 b 가 a 로 나누어지지 않는 경우 $a \nmid b$ 로 쓴다.

- (1) 정수 a, b, c 에 대해 다음이 성립한다.
- (i) $a|0, 1|a, a|a$
 - (ii) $a|1 \Leftrightarrow a = \pm 1$
 - (iii) $a|b, c|d \Rightarrow ac|bd$
 - (iv) $a|b, b|c \Rightarrow a|c$
 - (v) $a|b, b|a \Leftrightarrow a = \pm b$
 - (vi) $a|b, b \neq 0 \Rightarrow |a| \leq |b|$
 - (vii) $a|b, a|c \Rightarrow \forall x, y \in \mathbb{Z}, a|(bx + cy)$

최대공약수 $\gcd(a, b)$

a, b 를 적어도 둘 중 하나는 0이 아닌 정수라 하자.
 a, b 의 최대공약수는 $\gcd(a, b)$ 로 쓰고 다음을 만족하는 양의 정수 d 이다.

- (i) $d|a, d|b$
- (ii) $c|a, c|b \Rightarrow c|d$

a, b 를 적어도 둘 중 하나는 0이 아닌 정수라 하자.

- (1) $\gcd(a, b) = ax + by$ 를 만족하는 x, y 가 존재한다.
 (2) 집합 $T = \{ax + by | x, y \text{는 정수}\}$ 는 정확히 정수 $d = \gcd(a, b)$ 의 배수로 이루어진 집합이다.

서로 소

둘 중 하나는 0이 아닌 정수 a, b 에 대해 $\gcd(a, b) = 1$ 인 경우 서로 소라 한다.

- (1) a, b 를 둘 중 하나는 0이 아닌 정수라 하자.
 $\gcd(a, b) = 1 \Leftrightarrow 1 = ax + by$ 를 만족하는 x, y 가 존재
 (2) $\gcd(a, b) = d \Rightarrow \gcd(a/d, b/d) = 1$
 (3) $a|c, b|c, \gcd(a, b) = 1 \Rightarrow ab|c$
 (4) 유클리드 보조정리: $a|bc, \gcd(a, b) = 1 \Rightarrow a|c$
 (5) $a = qb + r \Rightarrow \gcd(a, b) = \gcd(b, r)$
 (6) $k (\neq 0) \in \mathbb{Z}$ 에 대해 $\gcd(ka, kb) = |k| \gcd(a, b)$

최소공배수 $\text{lcm}(a, b)$

영이 아닌 두 정수 a, b 의 최소공배수는 다음을 만족하는 양의 정수 m 이며 $\text{lcm}(a, b)$ 로 표현된다.

- (i) $a|m, b|m$
- (ii) $a|c, b|c$ 이면 $c > 0$ 일 때 $m|c$ 이다.

- (1) 양의 정수 a, b 에 대해 $\gcd(a, b)\text{lcm}(a, b) = ab$.
 (2) $\forall a, b \in \mathbb{Z}, \text{lcm}(a, b) = ab \Leftrightarrow \gcd(a, b) = 1$
 (3) $ax + by = c$ 이 해를 가진다 $\Leftrightarrow \gcd(a, b) | c$
 특수해 x_0, y_0 에 대하여 모든 해는 다음과 같다.

$$x = x_0 + \left(\frac{b}{d}\right)t, y = y_0 - \left(\frac{a}{d}\right)t, t \in \mathbb{Z}$$

3. 소수와 그 분포

소수, 합성수

만약 정수 p 의 양의 약수가 1과 p 뿐일 때, 1보다 큰 p 를 소수라 하자. 1보다 큰 정수 중 소수가 아닌 정수를 합성수라 한다.

- (1) p 가 소수, $p|a_1 a_2 \cdots a_n$ 이면 $1 \leq k \leq n$ 인 어떤 k 에 대해 $p|a_k$ 이다.
 (2) 만약 $p, q_1, q_2, \dots, q_n$ 이 소수이고 $p|q_1 q_2 \cdots q_n$ 이면 $1 \leq k \leq n$ 인 어떤 k 에 대해 $p = q_k$ 이다.
 (3) (산술의 기본정리) 모든 1보다 큰 양의 정수 n 은 인수가 나타나는 순서를 고려하지 않을 때, 소수들의 곱으로 유일하게 표현된다.
 (4) 모든 양의 정수 $n > 1$ 에 대하여

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

을 만족하는 양수 k_i 와 소수 $p_i (p_1 < p_2 < \cdots < p_r)$ 가 존재한다.

- (5) (유클리드) 무한히 많은 소수가 존재한다.
 (6) (디리클레) a 와 b 가 서로 소인 양의 정수이면, 다음 수열은 무한히 많은 소수를 포함한다.

$$a, a+b, a+2b, a+3b, \dots$$

4. 합동이론

합동

n 을 주어진 양의 정수라 하자. n 이 차 $a-b$ 를 나누면 정수 a 와 b 를 법 (또는 모듈로) n 에 대해 합동이라 말하며 기호로 표현하면 다음과 같다.

$$a \equiv b \pmod{n}$$

- (1) 임의의 정수 a 와 b 에 대해 $a \equiv b \pmod{n}$ 일 필요충분조건은 a 와 b 는 n 으로 나누었을 때, 음이 아닌 같은 나머지를 가진다.
- (2) $a \equiv b \pmod{n} \Leftrightarrow a$ 와 b 는 n 으로 나눈 나머지가 같다.
- (3) $n > 1$ 이 고정되고, a, b, c, d 를 임의의 정수라 하면 다음 성질이 성립한다.
 - (i) $a \equiv a \pmod{n}$
 - (ii) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$
 - (iii) $a \equiv b \pmod{n}, b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$
 - (iv) $a \equiv b \pmod{n}, c \equiv d \pmod{n} \Rightarrow$
 $a+c \equiv b+d \pmod{n}, ac \equiv bd \pmod{n}$
 - (v) $a \equiv b \pmod{n} \Rightarrow \forall k \in \mathbb{N}, a^k \equiv b^k \pmod{n}$
- (3) $ca \equiv cb \pmod{n} \Rightarrow a \equiv b \pmod{\frac{n}{d}}, d = \gcd(c, n)$
- (4) $ca \equiv cb \pmod{n}, \gcd(c, n) = 1 \Rightarrow a \equiv b \pmod{n}$
- (5) $ca \equiv cb \pmod{p}, p \nmid c (p: \text{소수}) \Rightarrow a \equiv b \pmod{p}$

정수의 2진법과 10진법 표현

- (1) $P(x) = \sum_{k=0}^m c_k x^k$ 를 정수계수 c_k 를 가진 x 의 다항 함수라 하자. $a \equiv b \pmod{n}$ 이면 $P(a) \equiv P(b) \pmod{n}$ 이다.
- (2) a 가 합동식 $P(a) \equiv 0 \pmod{n}$ 의 해이고 $a \equiv b \pmod{p}$ 이면 b 또한 해이다.
- (3) $N = a_m 10^m + a_{m-1} 10^{m-1} + \dots + a_1 10 + a_0, 0 \leq a_k \leq 10$ 에 대하여 $S = a_0 + a_1 + \dots + a_m$ 이라 하면 $9|N$ 일 필요충분조건은 $9|S$ 이다.
- (4) $N = a_m 10^m + a_{m-1} 10^{m-1} + \dots + a_1 10 + a_0, 0 \leq a_k \leq 10$ 에 대하여 $T = a_0 - a_1 + a_2 - \dots + (-1)^m a_m$ 이라 하면 $11|N$ 일 필요충분조건은 $11|T$ 이다.

선형 합동식과 중국인의 나머지 정리

- (1) $ax \equiv b \pmod{n}$ 의 해가 존재한다 $\Leftrightarrow \gcd(a, n) | b$
 $d | b$ 이면 법 n 에 대해 d 개의 서로 합동이 아닌 해를 가진다.
- (2) $\gcd(a, n) = 1$ 이면 선형 합동식 $ax \equiv b \pmod{n}$ 은 법 n 에 대해 유일한 해를 가진다.

- (3) (중국인의 나머지 정리) $n_1, n_2, \dots, n_r$ 을 $i \neq j$ 에 대해 $\gcd(n_i, n_j) = 1$ 인 양의 정수라 하자. 그러면 연립 선형 합동식

$$x \equiv a_1 \pmod{n_1}$$

$$x \equiv a_2 \pmod{n_2}$$

$$\vdots$$

$$x \equiv a_r \pmod{n_r}$$

은 법 $n_1 n_2 \dots n_r$ 에 대해 유일한 공통 해를 가진다.

5. 페르마 정리

페르마의 작은 정리와 유사소수

- (1) (페르마 정리) p 가 소수, $p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}$
- (2) $\forall p: \text{소수}, \forall a \in \mathbb{Z}, a^p \equiv a \pmod{p}$
- (3) (윌슨의 정리) p 가 소수이면 $(p-1)! \equiv -1 \pmod{p}$
- (4) p 가 홀수인 소수라 하자.
 $x^2 + 1 \equiv 0 \pmod{p}$ 가 해를 가짐 $\Leftrightarrow p \equiv 1 \pmod{4}$

6. 수론 함수

수론함수(산술함수)

정의역이 양의 정수의 집합인 임의의 함수를 수론 함수 또는 산술 함수라 부른다.

$\tau(n), \sigma(n)$

양의 정수 n 에 대해 τ, σ 를 다음과 같이 정의한다.

$\tau(n)$: n 의 양의 약수의 개수

$\sigma(n)$: n 의 양의 약수들의 합

- (1) $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ 이 $n > 1$ 의 소인수분해라 하자.
 - (i) $\tau(n) = (k_1 + 1)(k_2 + 1) \dots (k_r + 1)$
 - (ii) $\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \frac{p_2^{k_2+1} - 1}{p_2 - 1} \dots \frac{p_r^{k_r+1} - 1}{p_r - 1}$

승법적

수론 함수 f 를 $\gcd(m, n) = 1$ 일 때

$$f(mn) = f(m)f(n)$$

이면 승법적이라 말한다.

- (1) 함수 τ 와 σ 는 승법 함수이다.
- (2) $\gcd(m, n) = 1$ 이면 mn 의 양의 약수의 집합은 $d_1 | m, d_2 | n$ 이고 $\gcd(d_1, d_2) = 1$ 인 모든 곱 $d_1 d_2$ 로 구성된다. 더군다나 이 곱은 모두 다르다.
- (3) f 가 승법 함수이고 $F(n) = \sum_{d|n} f(d)$ 라고 정의하면 F 도 또한 승법 함수이다.

$\mu(n)$

양의 정수 n 에 대해 μ 를 다음과 같이 정의 한다.

$$\mu(n) = \begin{cases} 1, & n=1 \\ 0, & p^2 | n, p \text{는 소수} \\ (-1)^r, & n=p_1 p_2 \cdots p_r, p_i \text{는 서로 다른 소수} \end{cases}$$

- (1) 함수 μ 는 승법함수이다.
- (2) 양의 정수 $n \geq 1$ 에 대해

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & n=1 \\ 0, & n>1 \end{cases}$$

- (3) (외비우스 역공식)

F 와 f 를 $F(n) = \sum_{d|n} f(d)$ 인 수론함수라 하자.

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

- (4) F : 승법함수, $F(n) = \sum_{d|n} f(d) \Rightarrow f$: 승법함수

$[x]$

임의의 실수 x 에 대해 $[x]$ 를 x 보다 작거나 같은 가장 큰 정수라 한다.

- (1) n 가 양의 정수, p 가 소수이면 $n!$ 을 나누는 가장 큰

$$p \text{의 거듭제곱의 지수는 } \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor \text{이다.}$$

7. 오일러 정리

$\phi(n)$

$n \geq 1$ 에 대해 $\phi(n)$ 을 n 과 서로 소이면서 n 을 넘지 않는 양의 정수의 개수라 정의한다.

- (1) p : 소수, $k > 0 \Rightarrow \phi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$
- (2) $\forall a, b, c \in \mathbb{Z}$,
 $\gcd(a, bc) = 1 \Leftrightarrow \gcd(a, b) = 1, \gcd(a, c) = 1$
- (3) 함수 ϕ 는 승법함수이다.
- (4) 정수 $n > 1$ 이 $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ 인 소인수 분해이면

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

- (5) $n > 1$ 이고 $\gcd(a, n) = 1$ 이라 하자.
 $a_1, a_2, \dots, a_{\phi(n)}$ 이 n 보다 작고 n 과 서로 소인 양의 정수이면 $aa_1, aa_2, \dots, aa_{\phi(n)}$ 은 법 n 에 대해 어떤 순서로 $a_1, a_2, \dots, a_{\phi(n)}$ 과 합동이다.
- (6) (오일러) $n \geq 1, \gcd(a, n) = 1 \Rightarrow a^{\phi(n)} \equiv 1 \pmod{n}$
- (7) (가우스) 양의 정수 $n \geq 1$ 에 대해 $n = \sum_{d|n} \phi(d)$.

8. 원시근과 지표

법 n 에 대한 a 의 위수

$n > 1$ 그리고 $\gcd(a, n) = 1$ 이라 하자. 법 n 에 대한 a 의 위수는 $a^k \equiv 1 \pmod{n}$ 인 가장 작은 양의 정수 k 이다.

$\text{ord}_n a^h = k$ 라 하면 다음이 성립한다.

- (1) $a^k \equiv 1 \pmod{n} \Leftrightarrow k|h$; 특히, $k|\phi(n)$
- (2) $a^i \equiv a^j \pmod{n} \Leftrightarrow i \equiv j \pmod{k}$
- (3) $a, a^2, \dots, a^k$ 는 법 n 에 대해 서로 합동이 아니다.
- (4) $h > 0 \Rightarrow \text{ord}_n a^h = \frac{k}{\gcd(h, k)}$

원시근

$\gcd(a, n) = 1$ 이고 법 n 에 대한 a 의 위수가 $\phi(n)$ 이면 a 를 정수 n 의 원시근이라 한다.

- (1) $\gcd(a, n) = 1$ 이고 $a_1, a_2, \dots, a_{\phi(n)}$ 을 n 과 서로 소인 n 보다 작은 양의 정수라 하자. a 가 n 의 원시근이면, $a, a^2, \dots, a^{\phi(n)}$ 은 법 n 에 대해 어떤 순서로 $a_1, a_2, \dots, a_{\phi(n)}$ 와 합동이다.
- (2) n 이 원시근을 가지면 정확히 $\phi(\phi(n))$ 개의 원시근이 존재한다.
- (3) p 를 소수라 하고 $d|p-1$ 이면 법 p 에 대해 위수 d 를 갖는 정확히 $\phi(d)$ 개의 합동이 아닌 해가 존재한다.
- (4) 정수 $n > 1$ 에 대하여 다음은 동치이다.
(i) n 의 원시근이 존재한다.
(ii) $n = 2, 4, p^k$ 또는 $2p^k$ (p 는 홀수인 소수)

지표

r 을 n 의 원시근이라 놓자.

$\gcd(a, n) = 1$ 이면 $a \equiv r^k \pmod{n}$ 인 가장 작은 양의 정수 k 를 r 에 대한 a 의 지표라 부른다.

- (1) n 이 원시근 r 을 가지고 ind_a 를 r 에 대한 a 의 원시근이라 놓으면 다음 성질이 성립한다.
(i) $\text{ind}(ab) \equiv \text{ind}a + \text{ind}b \pmod{\phi(n)}$
(ii) $\text{ind}a^k \equiv k \text{ind}a \pmod{\phi(n)}, k > 0$
(iii) $\text{ind}1 \equiv 0 \pmod{\phi(n)}, \text{ind}r \equiv 1 \pmod{\phi(n)}$
- (2) n 이 원시근을 갖는 정수, $\gcd(a, n) = 1$ 이라 하면 다음은 동치이다.
(i) $x^k \equiv a \pmod{n}$ 의 해가 존재한다.
(ii) $a^{\frac{\phi(n)}{d}} \equiv 1 \pmod{n}, d = \gcd(k, \phi(n))$
해가 존재하는 경우 정확히 d 개의 해가 존재한다.

9. 이차상호법칙

이차 잉여류, 이차 비잉여류

p 는 홀수인 소수, $\gcd(a, p) = 1$ 이라 하자.

이차 합동식 $x^2 \equiv a \pmod{p}$ 가 해를 가지면 a 를 p 의 이차 잉여류, 갖지 않으면, a 를 p 의 이차 비잉여류라 한다.

(1) p 는 홀수인 소수, $\gcd(a, p) = 1$ 이라 하자.

$$(i) a \text{가 } p \text{의 이차 잉여류} \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

$$(ii) a \text{가 } p \text{의 이차 비잉여류} \Leftrightarrow a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

르장드르 기호

p 는 홀수인 소수, $\gcd(a, p) = 1$ 이라 하자.

그러면 르장드르 기호 $\left(\frac{a}{p}\right)$ 는 다음과 같이 정의된다.

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{는 } p \text{의 이차 잉여류} \\ -1, & a \text{는 } p \text{의 이차 비잉여류} \end{cases}$$

(1) p : 홀수인 소수, $\gcd(a, p) = \gcd(b, p) = 1$ 이라 하자. 이면 다음이 성립한다.

$$(i) a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

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

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

$$(iv) \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$$

$$(v) \left(\frac{1}{p}\right) = 1, \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

(2) p 를 홀수인 소수라 하면 $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$ 이다. 따라서

정확히 $\frac{p-1}{2}$ 개의 p 의 이차잉여류와 $\frac{p-1}{2}$ 개의 p 의

이차 비잉여류가 존재한다.

(3) p 를 홀수인 소수라 하면 다음이 성립한다.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

(4) (이차상호법칙) p, q : 서로 다른 홀수인 소수이면

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

문제

풀이는 충분히 고민 후 참고하시길 바랍니다.

고등과정

1. $\left[x + \frac{1}{10}\right] + \left[x + \frac{2}{10}\right] + \cdots + \left[x + \frac{9}{10}\right] = 53$ 일 때,
 $[10x]$ 의 값은? (단, $[x]$ 는 x 를 넘지 않는 최대 정수이다.) [1995]

- ① 55 ② 56
 ③ 57 ④ 58

2. 피보나치 수열 $\{f_n\}$ 은 다음과 같이 정의된다.

$$f_1 = f_2 = 1, \quad f_n = f_{n-1} + f_{n-2} \quad (n \geq 3)$$

피보나치 수열의 유래를 간단히 쓰고 다음 등식이 성립함을 보이시오. [1998]

$$f_{n+1}f_{n-1} = f_n^2 + (-1)^n \quad (n \geq 2)$$

정수론 기초

3. (참, 거짓 판정문제) p 가 소수일 때, $p!+1$ 을 나누는 소수는 p 보다 크다. [2011]

4. <보기>에서 옳은 것을 모두 고른 것은? [2009]

- <보기> —
- ㄱ. 정수 a, b 가 서로소이기 위한 필요충분조건은 적당한 정수 s, t 에 대하여 $as+bt=1$ 이 성립하는 것이다.
- ㄴ. 양의 정수 m 과 n 에 대하여 2^m-1 과 2^n-1 이 서로소이기 위한 필요충분조건은 m 과 n 이 서로소인 것이다.
- ㄷ. 양의 정수가 25진법으로 표현될 때 3자리 수이기 위한 필요충분조건은 5진법으로 표현될 때 6자리 수 인 것이다.

- ① ㄱ ② ㄴ ③ ㄱ, ㄴ
 ④ ㄱ, ㄷ ⑤ ㄴ, ㄷ

5. $500! \times 200!$ 이 35^n 으로 나누어 떨어질 때 정수 n 의 최댓값은? [1993]

- ① 32 ② 82 ③ 114 ④ 146

7. 정수 x, y, z 에 관한 다음 방정식의 일반해를 구하시오. [2008]

$$3x + 4y + 5z = 2$$

디오판투스 방정식

6. 방정식 $2x + 3y = 55$ 를 만족하는 양의 정수해 (x, y) 의 개수는? [1992]

- ① 10 ② 9 ③ 8 ④ 7

8. 절댓값이 10이하인 두 정수 x, y 가 $32x + 14y = (32, 14)$ 를 만족시킬 때, $|x| + |y|$ 의 값은? (단, (a, b) 는 a 와 b 의 최대공약수이다.) [2009 모의평가]

- ① 4 ② 6 ③ 8 ④ 10 ⑤ 12

9. (참, 거짓 판정문제) 부정방정식 $7x + 31y = 2$ 의 정수해가 존재한다. [2010]

11. (참, 거짓 판정문제) 합동식 $6x \equiv 22 \pmod{32}$ 의 정수해는 법 32에 대하여 1개 뿐이다. [2010]

선형합동식 관련

10. 정수 x, y, z 에 관한 합동식 $x^2 + y^2 \equiv 3z^2 \pmod{4}$ 의 해집합은

$$\{(x, y, z) \mid x \equiv y \equiv z \equiv 0 \pmod{2}\}$$

임을 보이시오. [2007]

12. 옳은 것만을 <보기>에서 있는 대로 고른 것은? [2012]

— <보기> —

ㄱ. 연립합동식 $\begin{cases} x \equiv 4 \pmod{28} \\ x \equiv 6 \pmod{36} \end{cases}$ 의 정수해가 존재한다.

ㄴ. 홀수인 소수 p 에 대하여 합동식 $x^4 \equiv -1 \pmod{p}$ 의 정수해가 존재하면 $p \equiv 1 \pmod{8}$ 이다.

ㄷ. 부정방정식 $x^2 + 2x + 5 - 65y^2 = 2011$ 의 정수해가 존재한다.

- ① ㄱ ② ㄴ ③ ㄷ
④ ㄱ, ㄷ ⑤ ㄴ, ㄷ

중국인의 나머지 정리

13. 다음 연립일차합동식의 해를 구하시오. [2003]

$$\begin{cases} 8x \equiv 4 \pmod{22} \\ 3x \equiv 5 \pmod{25} \end{cases}$$

14. K 고등학교의 전체 학생을 같은 인원수의 9팀으로 나누면 1명이 남고, 같은 인원수의 10팀으로 나누면 2명이 남으며, 같은 인원수의 11팀으로 나누면 10명이 남는다. K 고등학교 전체 학생수 x 가 $x \equiv a \pmod{990}$ 을 만족할 때, 정수 a 의 값을 구하시오. (단, $0 \leq a < 990$) [2006]

Wilson 정리

15. $100!$ 를 101로 나누었을 때 나머지는? [1994]

- ① 1 ② 2 ③ 99 ④ 100

16. (참, 거짓 판정문제) 홀수인 소수 p 는 합동식 $(p-2)! \equiv 1 \pmod{p}$ 를 만족시킨다. [2011]

페르마 정리

17. 정수 $2^{15}14^{10}+2$ 를 11로 나누었을 때의 나머지는?
[1992]

- ① 1 ② 4 ③ 7 ④ 10

18. 다음 합동식을 만족하는 정수 x, y 는 어느 것인가?
[1995]

$$9^x \equiv y \pmod{19}$$

- ① $x=35, y=1$ ② $x=36, y=-1$
③ $x=36, y=1$ ④ $x=35, y=-1$

19. 오늘부터 n^7 째 되는 날이 금요일이면 오늘부터 $(n+2)^7$ 째 되는 날은 무슨 요일인가? [1995]

- ① 금요일 ② 토요일
③ 일요일 ④ 월요일

20. (참, 거짓 판정문제) 홀수인 소수 p ($p \neq 3$)은 합동식 $3^{p-1} \equiv 1 \pmod{2p}$ 를 만족시킨다. [2011]

원시근

21. 정수의 곱셈에서 법 m 에 대한 3의 위수(order of 3 modulo m)을 $\text{ord}_m 3$ 으로 나타낸다.

$$r = \text{ord}_5 3$$

$$s = \text{ord}_7 3$$

$$t = \text{ord}_{35} 3$$

일 때, 세 수 r, s, t 의 곱 rst 의 값은?

[2009 모의평가]

- ① 48 ② 144 ③ 288
④ 24^2 ⑤ 35^2

22. $G = \mathbb{Z}_{11} - \{0\}$ 는 곱셈에 대하여 순환군(cyclic group)이 된다. 이 사실을 이용하여 단위원시 10-제곱근(법 11에 관한 원시근, primitive 10th root of unity)을 모두 구하시오. [2002]

23. 원시근(primitive root)과 관련된 <보기>의 명제 중 옳은 것을 모두 고른 것은? [2009]

— <보기> —

ㄱ. 19는 원시근을 갖는다.

ㄴ. 3은 8의 원시근이다.

ㄷ. 1보다 큰 정수 m 의 원시근 g 와 양의 정수

i, j 에 대하여, $g^i \equiv g^j \pmod{m}$ 이면

$i \equiv j \pmod{\phi(m)}$ 이다. (단, $\phi(m)$ 은

$1, 2, \dots, m$ 중 m 과 서로소인 수의 개수이다.)

- ① ㄱ ② ㄴ ③ ㄱ, ㄷ
④ ㄴ, ㄷ ⑤ ㄱ, ㄴ, ㄷ

24. 정수 2는 법 29에 대한 원시근(primitive root)이다. 1보다 크거나 같고 28보다 작거나 같은 정수 중 합동식 $x^4 \equiv 1 \pmod{29}$ 의 해를 모두 곱한 값을 m 이라 할 때, $2^k \equiv m \pmod{29}$ 를 만족시키는 최소의 양의 정수 k 는? [2010]

- ① 1 ② 4 ③ 7 ④ 14 ⑤ 28

25. 정수 x_0 과 27은 서로소이고, 모든 자연수 n 에 대하여

$$x_n \equiv 16x_{n-1} \pmod{27}, 0 < x_n < 27$$

 이 성립할 때, $x_n \equiv x_0 \pmod{27}$ 이 되는 최소의 자연수
 n 의 값은? (단, 2는 법 27에 관한 원시근(primitive
 root)이다.) [2012]

① 4 ② 9 ③ 13 ④ 18 ⑤ 26

26. 정수 3은 법 50에 대한 원시근(primitive root)이다.
 1보다 크거나 같고 25보다 작거나 같은 정수 중 합동식

$$x^{12} \equiv -9 \pmod{50}$$

 의 해를 모두 더한 값은? [2013]

① 22 ② 24 ③ 26 ④ 28 ⑤ 30

이차합동식

27. 다음 두 이차합동식의 해가 존재하는지 판별하시오.
 [2004]

(1) $x^2 \equiv 97 \pmod{101}$

(2) $x^2 + 2x \equiv 28 \pmod{89}$

28. (참, 거짓 판정문제) 합동식

$$x^2 + 10x + 20 \equiv 0 \pmod{17 \cdot 23}$$

의 정수해가 존재한다. [2010]

29. 이차합동식 $x^2 + 44 \equiv 0 \pmod{111}$ 의 정수해는 법 111에 대하여 m 개다. m 의 값은? [2011]

- ① 1 ② 2 ③ 3 ④ 4 ⑤ 5

30. 소수 $p(p > 2)$ 에 대하여 $-2p$ 가 $935(=5 \times 11 \times 17)$ 의 이차잉여(quadratic residue)일 때, p 의 이차잉여만을 <보기>에서 있는 대로 고른 것은? [2013]

<보기>		
ㄱ. -11	ㄴ. 5	ㄷ. 17

- ① ㄱ ② ㄴ ③ ㄷ
 ④ ㄱ, ㄴ ⑤ ㄱ, ㄷ

31. 다항식환 $Z_{2014}[x]$ 에서 $f(x) = x^2 - 14$ 를 두 일차식의 곱 $f(x) = (ax + b)(cx + d)$ 로 나타낼 수 없음을 증명하시오. [2014][4점]