중국인의 나머지 정리

10.

K고등학교의 전체 학생을 같은 인원수의 9팀으로 나누면 1명이 남고, 같은 인원수의 10팀으로 나누면 2명이 남으며, 같은 인원수의 11팀으로 나누면 10명이 남는다. K고등학교 전체 학생수 x가 $x \equiv a \pmod{990}$을 만족할 때, 정수 a의 값을 구하시오. (단, $0 \le a < 990$) [2006]

$x \equiv 1 \pmod 9$	$99x \equiv 1 \pmod{10}$	$90x_3 \equiv 1 \pmod{11}$	$\Rightarrow x \equiv 5\cdot 110 + 9\cdot 99\cdot 2 + 6\cdot 90\cdot 10$
$x \equiv 2 \pmod{10}$	$99x - 10y = 1$	$90x - 11y = 1$	$= 550 + 1782 + 5400$
$x \equiv 10 \pmod{11}$	$\gcd(99, 10) = 1$	$\gcd(90, 11) = 1$	$= 7732 \pmod{990}$
$x \equiv x_1 N_1 a_1 + x_2 N_2 a_2 + x_3 N_3 a_3 \pmod{990}$	$99 = 10\times 9 + 9$	$90 = 11\times 8 + 2$	$990 \times 7 = 6930 \quad 7732 - 6930 = 802$
$x_1 = 5,\ N_1 = 110,\ a_1 = 1,\ x_2 = 9,\ N_2 = 99,\ a_2 = 2,\ x_3 = 6,\ N_3 = 90,\ a_3 = 10$	$10 = 9\times 1 + 1$	$11 = 2\times 5 + 1$	$\Rightarrow x \equiv 802 \pmod{990}$
$110x \equiv 1 \pmod 9$	$\Downarrow$	$2 = 1\times 2$	$\therefore a = 802$
$110x - 9y = 1$	$1 = 10 - 9$	$1 = 11 - 2\times 5$	
$\gcd(110, 9) = 1 \quad \Rightarrow 1 = 9 - 2\times 4$	$= 10 - (99 - 10\times 9)$	$= 11 - 5(90 - 11\times 8)$	
$110 = 9\times 12 + 2 \quad = 9 - 4(110 - 9\times 12)$	$= 99\times(-1) + 10\times 10$	$= 90\times(-5) + 11\times 9$	
$9 = 2\times 4 + 1 \quad = 110\times(-4) + 9\times(\ )$	$x \equiv -1 \equiv 9 \pmod{10}$	$x \equiv -5 \equiv 6 \pmod{11}$	
$2 = 1\times 2 \quad x \equiv -4 \equiv 5 \pmod 9$			

11.

11. 다음 연립일차합동식의 해를 구하시오. [2003]

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

① 중국인의 나머지 정리 쓰기 위해 식정리

$8x \equiv 4 \pmod{22}$	ii) $3x \equiv 5 \pmod{25} \Rightarrow x \equiv 5\times 17 \pmod{25}$	① $25x \equiv 1 \pmod{11}$ ② $11x \equiv 1 \pmod{25}$
$\Rightarrow 4x \equiv 2 \pmod{11}$	$3x \equiv 1 \pmod{25} \quad = 85 \equiv 10 \pmod{25}$	$25x - 11y = 1,\ \gcd(25, 11) = 1$
② 식 정리 위해 역원 구하기	$3x - 25y = 1 \quad x \equiv 10 \pmod{25}$	$25 = 11\times 2 + 3 \quad \Rightarrow 1 = 3 - 2$
i) $4x \equiv 1 \pmod{11} \Rightarrow x \equiv \cancel{3}6 \pmod{11}$	$\gcd(3, 25) = 1$	$11 = 3\times 3 + 2 \quad = 3 - (11 - 3\times 3)$
$4x - 11y = 1$	$25 = 3\times 8 + 1$	$3 = 2\times 1 + 1 \quad = 11\times(-1) + 3\times 4$
$\gcd(4, 11) = 1$	$3 = 1\times 3$	$= 11\times(-1) + 4(25 - 11\times 2)$
$11 = 4\times 2 + 3$	$1 = 25 - 3\times 8$	$= 11\times(-9) + 25\times 4$
$4 = 3\times 1 + 1$	$x = -8 \equiv 17 \pmod{25}$	$x_1 = 4,\ x_2 = -9 \equiv 16 \pmod{25}$
$1 = 4 - 3$	$\Rightarrow x \equiv 3 \pmod{11}$	$\Rightarrow x \equiv 4\times 25\times \cancel{3}6 + 16\times 11\times 10 \pmod{275}$
$= 4 - (11 - 4\times 2)$	$x \equiv 10 \pmod{25}$	$= \cancel{300 + 1760 = 2060}$
$= 11\times(-1) + 4\times 3$ $x = 3$ (법 11에 관한 4의 역원)	$x \equiv x_1 N_1 a_1 + x_2 N_2 a_2 \pmod{11\times 25}$ $4 \quad 25 \quad \cancel{3}6 \quad 16 \quad 11 \quad 10$	$\cancel{275\times 7 = 1925,\ 2060 - 1925 = 135}$ $\therefore x \equiv \cancel{135}\ 160 \pmod{275}$

12.

<보기>의 진위를 판정하고 이유를 설명하시오. [2012]

<보기>

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

(sol) 거짓

a가 주어진 연립방정식의 해라고 가정하자

$6+36k = a = 4+28t$ 를 만족하는 정수 k, t 가 존재한다.

그러면 $6+36k = 4+28t$

$2 = 28t-36k = 4(7t-9k) \Rightarrow 4 \mid 2$ 이므로 $\rightarrow\leftarrow$ ∎

< Fermat 정리 >

13.

다음 합동식을 만족하는 정수 x, y는 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 $x=35, y=-1$

(sol) 19는 소수이고 $19 \nmid 9$ 이므로, $9^{18} \equiv 1 \pmod{19}$

따라서 $9^{36} \equiv 1 \pmod{19}$ 이 성립.

14.

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

(sol) $2^{15} \cdot 14^{10} + 2 \equiv x \pmod{11}$

페르마 정리에 의해, $11 \nmid 2$, $11 \nmid 14$ 이므로

$2^{10} \equiv 1 \pmod{11}$ 이고 $14^{10} \equiv 1 \pmod{11}$ 이다.

그리고 $2^5 \equiv -1 \pmod{11}$ 이므로 $2^5 \cdot 2^{10} \cdot 14^{10} \equiv -1 \pmod{11}$

$2^{15} \cdot 14^{10} + 2 \equiv 1 \pmod{11}$, 따라서 나머지는 1 ∎

14.

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

페르마 정리
$a^{p-1} \equiv 1 \pmod{p}$ 사용
$11 \nmid 2$, $11 \nmid 14$ 이므로 $2^{11-1} = 2^{10} \equiv 1 \pmod{11}$
$14^{11-1} = 14^{10} \equiv 1 \pmod{11}$
$\rightarrow 2^{10} \cdot 14^{10} \equiv 1 \pmod{11}$
$2^{15} \cdot 14^{10} \equiv 32 \pmod{11}$
$2^{15} \cdot 14^{10} + 2 \equiv 34 \pmod{11}$
$\equiv 1 \pmod{11}$
따라서 나머지는 1이다.

15.

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

홀수인 소수 p는 $gcd(3, p) = 1$ 이므로 $3^{p-1} \equiv 1 \pmod{p}$
$\downarrow$
$2p$ 되면

$\begin{cases} 3^{p-1} \equiv 1 \pmod{2} \\ 3^{p-1} \equiv 1 \pmod{p} \end{cases}$?

(sol) 참
$gcd(p, 3) = 1$ 이므로 $(p \nmid 3)$ 페르마 소정리에 의하여 $3^{p-1} \equiv 1 \pmod{p}$
또한 $3^{p-1} - 1$ 은 짝수이므로 $3^{p-1} \equiv 1 \pmod{2}$
p는 홀수이므로 $gcd(2, p) = 1$ 이다.
따라서 $3^{p-1} \equiv 1 \pmod{2p}$.

16.

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

(sol) $n^7 \equiv 5 \pmod 7$

$$(n+2)^7 = n^7 + \underbrace{{}_7C_1}_{7} n^6 \cdot 2^1 + \underbrace{{}_7C_2}_{7\cdot 3} n^5 \cdot 2^2 + \underbrace{{}_7C_3}_{7\cdot 5} n^4 \cdot 2^3 + \underbrace{{}_7C_3}_{7\cdot 5} n^3 \cdot 2^4 + \underbrace{{}_7C_2}_{7\cdot 3} n^2 \cdot 2^5 + \underbrace{{}_7C_1}_{7} n \cdot 2^6 + 2^7$$

$$\equiv 5 + \underbrace{2^7}_{128} = 133 \pmod 7$$

$$\begin{array}{r} 19 \\ 7\overline{)133} \\ \underline{7} \\ 63 \\ 63 \end{array}$$

$\equiv 0 \pmod 7$ ⇒ 일요일

(sol2) 7은 소수이므로 $n^7 \equiv n \pmod 7$, $(n+2)^7 \equiv (n+2) \pmod 7$ 이 성립한다.

그러면 $(n+2)^7 - n^7 \equiv 2 \pmod 7$

⇒ $\exists k \in \mathbb{Z}$ s.t $(n+2)^7 - n^7 = 2 + 7k$

$(n+2)^7 = n^7 + 2 + 7k$

오늘 $\xrightarrow{n^7}$ 금 $\xrightarrow{7k}$ 금 $\xrightarrow{2}$ 일

※ Thm) p: 소수 ⇒ $\forall a \in \mathbb{Z}$, $a^p \equiv a \pmod p$

17.

합동방정식 $x \equiv 25^{99} \pmod{19 \cdot 13}$과 연립합동방정식 $\begin{cases} x \equiv a \pmod{19} \\ x \equiv b \pmod{13} \end{cases}$이 동치가 되도록 하는 정수 a, b의 값을 각각 구하시오. 또한 합동방정식의 정수해 x의 값을 풀이 과정과 함께 쓰시오.
(단, $0 \le a < 19$, $0 \le b < 13$, $0 \le x < 247$) [2020]

(sol)

$\begin{cases} x \equiv 25^{99} \pmod{19} \\ x \equiv 25^{99} \pmod{13} \end{cases}$

$19 \nmid 25$, $13 \nmid 25$ 이므로 우선 $25^{18} \equiv 1 \pmod{19}$ $\Rightarrow$ $25^{9} \equiv x_1 \pmod{19}$ $\quad x_1 \equiv 1 \pmod{19}$

$25 \equiv -1 \pmod{13}$ $\Rightarrow$ $(25^{99}) \equiv (-1)^{99} \pmod{13}$ $\quad x_2 \equiv 12 \pmod{13}$

$\Rightarrow$ $a = 1$, $b = 12$ 이다.

$\begin{cases} x \equiv a \equiv 1 \pmod{19} \\ x \equiv b \equiv -1 \pmod{13} \end{cases}$ 을 만족하는 정수해 x는

$x = x_1 N_1 a_1 + x_2 N_2 a_2$

$= x_1 13 \cdot 1 + x_2 \cdot 19 \cdot (-1) = 3 \times 13 \times 1 + 11 \times 19 \times (-1)$

$13x \equiv 1 \pmod{19}$ $\qquad = 39 - 209 = -170 \pmod{19 \cdot 13}$

$13x - 19y = 1$ $\qquad \equiv 77 \pmod{19 \cdot 13}$

$19 = 13 \times 1 + 6$ $\Rightarrow$ $1 = 13 - 6 \times 2$

$13 = 6 \times 2 + 1$ $\qquad = 13 - 2(19 - 13)$

$6 = 1 \times 6$ $\qquad = 13 \times 3 + 19 \times (-2)$

$x_1 \equiv 3 \pmod{19}$

$x_2 \equiv -2 \pmod{13}$

$x_2 \equiv 11 \pmod{13}$

18. < Wilson 정리 >

100!를 101로 나누었을 때 나머지를 구하시오. [1994]

(sol) $100! \equiv x \pmod{101}$

㊟ p 소수 ⇒ $(p-1)! \equiv -1 \pmod{p}$

101은 소수 ⇒ $(101-1)! \equiv -1 \pmod{101}$

$100! \equiv -1 \pmod{101}$

따라서 나머지 100 ∎

19.

(참, 거짓 판정문제) 홀수인 소수 p는 합동식

$$(p-2)! \equiv 1 \pmod{p}$$

를 만족시킨다. [2011]

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

$(p-1)(p-2)! \equiv -1 \pmod{p}$

p는 소수이므로

$-(p-2)! = (p-1)(p-2)! \equiv (p-1)! \equiv -1 \pmod{p}$

양변에 -1 곱하면 $(p-2)! \equiv 1 \pmod{p}$

$p^m \mid n!$ 을 만족하는 m의 최댓값

20.

$500! \times 200!$이 35^n으로 나누어 떨어질 때 정수 n의 최댓값을 구하시오. [1993]

(sol) $500! \times 200! \equiv 0 \pmod{35^n}$

㊟ n은 양의 정수, p 소수이면 $n!$을 나누는 가장 큰 p의 거듭제곱의 지수는 $\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]$

정답: 114

$$\begin{cases} \sum_{n=1}^{\infty}\left[\frac{500}{5^n}\right]=\left[\frac{500}{5}\right]+\left[\frac{500}{25}\right]+\left[\frac{500}{125}\right]=100+20+4=124 \\ \sum_{n=1}^{\infty}\left[\frac{500}{7^n}\right]=\left[\frac{500}{7}\right]+\left[\frac{500}{7^2}\right]+\left[\frac{500}{7^3}\right]=71+10+1=82 \end{cases}$$

$$\begin{cases} \sum_{n=1}^{\infty}\left[\frac{200}{5^n}\right]=\left[\frac{200}{5}\right]+\left[\frac{200}{5^2}\right]+\left[\frac{200}{5^3}\right]=40+8+1=49 \\ \sum_{n=1}^{\infty}\left[\frac{200}{7^n}\right]=\left[\frac{200}{7}\right]+\left[\frac{200}{7^2}\right]=28+4=32 \end{cases}$$

따라서 $500! \times 200!$을 나누는 5의 최대지수는 $124+49=173$이고 $500! \times 200!$을 나누는 7의 최대지수는 $82+32=114$이다. 그러므로 $500! \times 200!$을 나누는 35의 최대지수는 114이다.

정리 n은 양의 정수, p는 소수이면 $n!$을 나누는 가장 큰 p의 거듭제곱의 지수는

$$\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]$$

이다.