

따라서  $\beta$  50에 대하여 서로 합동이 아닌 것은  $3, 3^6, 3^{11}, 3^{16}$ 이다.

또한  $3^6 \equiv 29 \pmod{50}$

$3^{11} \equiv 47 \pmod{50}$

$3^{16} \equiv 21 \pmod{50}$

이므로 1보다 크거나 같고 25보다 작거나 같은 정수에는 3, 21이 되어 합은 24.

31.

④ 정의)  $n$ 의 원시근을 갖는 정수,  $\gcd(a, n) = 1$ 이라 하면 다음은 동치

합동식

$$x^{n+5} - x^n - x^5 + 1 \equiv 0 \pmod{131}$$

의 범 131에 대한 해의 개수가 5가 되도록 하는 130 이하의 자연수  $n$ 의 개수를 풀이 과정과 함께 쓰시오. [2018]

(i)  $x^k \equiv a \pmod{n}$ 의 해가 존재.

$$(ii) a^{\frac{\varphi(n)}{d}} \equiv 1 \pmod{n}, d = \gcd(k, \varphi(n))$$

해가 존재하는 경우 정확히  $d$ 개의 해가 존재

(508) 먼저 131 소수인가?  $11^2 = 121 < 131 < 12^2 = 144 \Rightarrow [\sqrt{131}] = 11 \not\Rightarrow 2, 3, 5, 7, 11 \nmid 131 \Rightarrow 131 : 소수.$

$$\text{준식} \Leftrightarrow x^n(x^5 - 1) - (x^5 - 1) = (x^n - 1)(x^5 - 1) \equiv 0 \pmod{131}$$

$$\Leftrightarrow x^n \equiv 1 \pmod{131} \quad (\#) \quad \text{또는} \quad x^5 \equiv 1 \pmod{131} \quad (**)$$

먼저 131이 소수니까 원시근 존재.  
1이니까 해를 반드시 갖는다.

$$5 \mid 131 - 1 = 130 \Rightarrow 5 \text{개의 해를 가짐.}$$

$$d = (n, \varphi(131))$$

$= (n, 130)$  개의 해를 가짐.  $\rightarrow$  5개 이하의 해를 가져야 하므로 130의 약수 중 5 이하 ( $= 1, 2, 5$ ):  $d = 1, 2, 5$ 인 경우만 조사하자.

i)  $d = 1$ 인 경우. (\*)는 유일해  $x \equiv 1 \pmod{131}$ 를 가지고 이것은 (\*\*)의 해이기도 하므로  $(n, 130) = 1$ 인  $n$ 은 가능하고,

그 개수는  $\varphi(130) = \varphi(2 \cdot 5 \cdot 13) = 1 \cdot 4 \cdot 12 = 48$  개이다.

ii)  $d = 2$ 인 경우.  $n$ 은 짝수이므로, (\*)의 해의  $x \equiv \pm 1 \pmod{131}$ 이다. 그러나  $x \equiv -1 \pmod{131}$ 은 (\*\*)의 해가 아니므로 불가능하다.

iii)  $d = 5$ 인 경우.  $n = 5k (k \in \mathbb{N})$   $\Rightarrow 1 \equiv x^n \equiv x^{5k} \equiv (x^5)^k \pmod{131}$  이므로, (\*)의 5개의 해가 \*의 해가 된다.

$$-\star \qquad \qquad \qquad = (*)$$

따라서,  $(n, 130) = 5$ 인  $n$ 은 가능하고, 그 개수는  $5 = (5k, 130) \Leftrightarrow k = (k, 26)$  이므로  $\varphi(26) = 12$ 이다.

$$2 \times 12$$

iv)  $d > 5$ 이면, (\*)는 6개 이상의 해를 가지므로 불가능하다.

$$\therefore 48 + 12 = 60$$

## 합동방정식

$$(x^{10} - 1)(x^{10} + x^5 + 1)(x^{36} - 1) \equiv 0 \pmod{61}$$

의 법 61에 대한 해의 개수를 풀이 과정과 함께 쓰시오. [2021]

$$(sol) \quad 61 \text{ 소수? } \quad 7^2 = 49 < 61 < 8^2 = 64 \Rightarrow [\sqrt{61}] = 7 \quad 2, 3, 5, 7 + 61 \Rightarrow 61 \text{은 소수}$$

$$(claim) \quad (x^{10} - 1)(x^{10} + x^5 + 1)(x^{36} - 1) \equiv 0 \pmod{61} \Leftrightarrow (x^{10} - 1)(x^5 - 1)(x^{10} + x^5 + 1)(x^{36} - 1) \equiv 0 \pmod{61}$$

$$(\because \Rightarrow) \text{ 자명 } \quad 0 \times (x^5 - 1) \equiv 0 \pmod{61}$$

$$\Leftarrow (x^{10} - 1)(x^5 - 1)(x^{36} - 1) \equiv 0$$

$$(x^{10} - 1)(x^{10} + x^5 + 1)(x^{36} - 1) \neq 0 \text{ 가정}$$

$$x^5 \equiv 1 \text{ 인데 } x^{10} \equiv 1 \quad (\rightarrow \Leftarrow)$$

$$(x^{10} - 1)(x^5 - 1)(x^{36} - 1) \equiv 0 \pmod{61}$$

해는  $61+t$  만족 ( $61$ 의 배수가 아님)

해가 중복되지 않게 하려면  $t$ 는 법 60의 원천임여제에서 선택해주면 됨.  
원시근  $r$ 이라 하자.  $x \equiv r^t \pmod{61}, 1 \leq t \leq 60$

$$60 \mid 10t \text{ or } 60 \mid 15t \text{ or } 60 \mid 36t$$

$\hookrightarrow 10 \mid 6t$   
 $\Leftrightarrow 5 \mid 3t \quad (\gcd(5,3)=1)$

$$\Leftrightarrow 6 \mid t \text{ or } 4 \mid t \text{ or } 5 \mid t \quad \Leftrightarrow 5 \mid t$$

(포항 배제의 원리)

$$\therefore t \text{의 개수} = \left\lfloor \frac{60}{6} \right\rfloor + \left\lfloor \frac{60}{4} \right\rfloor + \left\lfloor \frac{60}{5} \right\rfloor$$

$$- \left\lfloor \frac{60}{12} \right\rfloor - \left\lfloor \frac{60}{20} \right\rfloor - \left\lfloor \frac{60}{30} \right\rfloor + \left\lfloor \frac{60}{60} \right\rfloor$$

$$= \underbrace{10+15+12}_{20} - \underbrace{5+3+2}_{-2} + 1$$

$$= 30 - 2 = 28$$

## 33. &lt;이차합동식&gt;

다음 두 이차합동식의 해가 존재하는지 판별하시오. [2004]

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

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

(50%) 르장드르 기호로 판별

$$(1) \left(\frac{97}{101}\right) = \left(\frac{-4}{101}\right) = \left(\frac{-1}{101}\right)\left(\frac{2^2}{101}\right) = \left(\frac{-1}{101}\right) = (-1)^{\frac{101-1}{2}} = 1 \quad \therefore \text{해가 존재한다.}$$

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

$$\begin{aligned} \Leftrightarrow x^2 + 2x + 1 &\equiv 29 \pmod{89} & \left(\frac{29}{89}\right) = (-1)^{\frac{29-1}{2} \cdot \frac{89-1}{2}} \left(\frac{2}{29}\right) = \left(\frac{2}{29}\right) = -1 & \text{mod } 89 \text{로 적용했을 때 } \pm 1 \text{ 이면 } 1 \\ & \text{ } & \left(\frac{2}{29}\right) = 1 & \pm 1 \text{ 이면 } -1 \quad \therefore \text{해 존재} X \\ & \left(\frac{x+1}{89}\right)^2 \equiv 29 \pmod{89} & \text{ } & \text{ } \\ & \text{ } & \text{ } & \text{ } \end{aligned}$$

$\downarrow$  29가 89의 이차잉여인가?

$\frac{89}{29}$  인데 법 29에 대해 출이연

## 34.

(참, 거짓 판정문제) 합동식

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

의 정수해가 존재한다. [2010]

$$(Pf) \text{ 조식 } \Leftrightarrow \left\{ \begin{array}{l} x^2 + 10x + 20 \equiv 0 \pmod{17} \\ x^2 + 10x + 20 \equiv 0 \pmod{23} \end{array} \right. \quad \left( \frac{5}{17} \right) = -1 \Rightarrow \text{해 존재} X$$

$$\left( \frac{5}{23} \right) = -1 \Rightarrow \text{해 존재} X$$

$$\left( \frac{5}{17 \cdot 23} \right) = \left( \frac{5}{17} \right) \left( \frac{5}{23} \right) = (-1)(-1) = 1$$

$\hookrightarrow$  야코비 기호에서는 1이 나온다고 해 존재 아님 (반례)

35.

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

(sol) 법 111은 소수 아님 (3의 배수)

$$x^2 + 44 \equiv 0 \pmod{3 \cdot 37}$$

$$\begin{aligned} & \left\{ \begin{array}{l} x^2 \equiv -44 \equiv 1 \pmod{3} \\ x^2 \equiv -44 \equiv 30 \pmod{37} \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} x \equiv \pm 1 \pmod{3} \\ x \equiv \pm c \pmod{37} \end{array} \right. \quad \text{이므로 중국인의 나머지 정리에 의해 법 111에 대하여} \\ & \quad \downarrow \quad \text{mod 2가 아님} \quad c \neq -c \\ & \left( \frac{30}{37} \right) = \left( \frac{2}{37} \right) \left( \frac{3}{37} \right) \left( \frac{5}{37} \right) \\ & = (-1) \times 1 \times (-1) = 1 \quad \text{해가 존재.} \quad \therefore m=4 \end{aligned}$$

36.

$1 \leq k \leq 2016$ 인 자연수  $k$ 에 대하여

$$a_k = k! \times (2017-k)!$$

일 때, 르장드르 기호(Legendre symbol)의 합

$$\sum_{k=3}^{2014} \left( \frac{a_k}{2017} \right)$$

의 값을 풀이 과정과 함께 쓰시오. (참고: 2017은 소수이다.)

[2017]

위 징자는 법 2017에 대해 합동이면 르장드르 기호는 같다.

$$\begin{aligned} (\text{sol}) \quad \left( \frac{a_k}{2017} \right) &= \left( \frac{k! \times (2017-k)!}{2017} \right) = \left( \frac{k! \times (2017-k) \times (2016-k) \times \cdots \times 2 \times 1}{2017} \right) \\ &= \left( \frac{k! \times (-k) \times (-k+1) \times \cdots \times -2015 \times -2016}{2017} \right) \\ &= \left( \frac{(-1)^{\frac{2017-k}{2}} \cdot k \cdot (2016!)^{-1}}{2017} \right) = \left( \frac{(-1)^{\frac{2018-k}{2}}}{2017} \right) \left( \frac{k}{2017} \right) = \left( \frac{-1}{2017} \right)^{\frac{2018-k}{2}} \left( \frac{k}{2017} \right) \end{aligned}$$

월순 정리에 의해  
 $2016! \equiv -1 \pmod{2017}$

$$= \left( (-1)^{\frac{2017-1}{2}} \right)^{\frac{2018-k}{2}} \left( \frac{k}{2017} \right)$$

$$\begin{matrix} \left( \frac{2}{2017} \right) & \left( \frac{1}{2017} \right) \\ \left( \frac{-2}{2017} \right) & \left( \frac{-1}{2017} \right) \end{matrix} = \frac{k}{2017}$$

$$\Rightarrow \text{준식} = \sum_{k=3}^{2014} \left( \frac{k}{2017} \right) = -\left( \frac{1}{2017} \right) - \left( \frac{2}{2017} \right) - \left( \frac{2015}{2017} \right) - \left( \frac{2016}{2017} \right)$$

$$= -2 \left( \left( \frac{1}{2017} \right) + \left( \frac{2}{2017} \right) \right) = -2(1+1) = -4$$

1일 맨 무조건 1 2일 맨 8로 나눠주면 1 남음

$$\begin{array}{r} 252 \\ 8 \overline{)2017} \\ 16 \\ \hline 41 \\ 40 \\ \hline 17 \\ 16 \\ \hline 1 \end{array}$$

37.

다음 삼차 합동방정식에 대하여  $\mathbb{Z}_{2015}$ 에 속하는 해의 개수를

풀이 과정과 함께 쓰시오. [2015]

$$x^3 - 8 \equiv 0 \pmod{2015} \quad (\text{참고} : 2015 = 5 \times 13 \times 31)$$

(Sol) 증식  $\Leftrightarrow \begin{cases} x^3 - 8 \equiv 0 \pmod{5} & \Rightarrow \text{해 } 1\text{개} \\ x^3 - 8 \equiv 0 \pmod{13} & \Rightarrow \text{해 } 3\text{개} \text{ (distinct 해)} \\ x^3 - 8 \equiv 0 \pmod{31} & \Rightarrow \text{해 } 3\text{개} \end{cases} \quad \left. \begin{array}{l} \text{증근인의 나머지 정리} \\ \text{(C.R.T)} \end{array} \right\} \quad 9\text{개}$

$\begin{matrix} 0 \\ \parallel \\ x^3 - 8 \end{matrix} \quad \begin{matrix} (-3) \text{이 각각에 대해} \\ \text{이차잉여가 되는지.} \end{matrix}$

$$x^3 - 8 = (x-2)(x^2+2x+4) = (x-2)((x+1)^2+3)$$

$$\left( \frac{-3}{5} \right) = -1 \quad \text{해가 없다.}$$

$$\left( \frac{-3}{13} \right) = \left( \frac{-1}{13} \right) \left( \frac{3}{13} \right) = (-1)^{\frac{13-1}{2}} \cdot 1 = 1$$

$$\left( \frac{-3}{31} \right) = \left( \frac{-1}{31} \right) \left( \frac{3}{31} \right) = (-1)^{\frac{31-1}{2}} \cdot (-1) = 1$$

■

38.

<보기>의 진위를 판정하고 이유를 설명하시오. [2012]

&lt;보기&gt;

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

L(※)

↓ mod (합동식을 취해도 성립한다)

(P) mod 5로 택하면  $5, -65y^2$  날아가고 2011도 확 줄어드니까 5 택하자.

(\*) 의 정수해가 존재한다면,  $x^2 + 2x \equiv 1 \pmod{5}$ 의 해가 존재한다.

↓

$$(x+1)^2 \equiv 2 \pmod{5} . \quad \text{그러나 } \left( \frac{2}{5} \right) = -1 \text{ 이므로 모순이다.}$$

따라서 부정방정식의 정수해는 존재하지 않는다. ■

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 고르시오. [2013]

<보기>		
<input checked="" type="radio"/> 11	<input checked="" type="radio"/> 5	<input checked="" type="radio"/> 17

(sol)  $-2p$  가 935 의 이차잉여이므로  $-2p$  가 5, 11, 17 각각의 이차잉여이다.

또한

$$\begin{cases} p = 5 \Rightarrow \left(\frac{-2p}{p}\right) = 1 \\ p = 11 \Rightarrow \left(\frac{-2p}{11}\right) \\ p = 17 \Rightarrow \left(\frac{-2p}{17}\right) \end{cases}$$

정답: ㄱ, ㄷ  
 $-2p$ 가 935의 이차잉여이므로  $-2p$ 가 5, 11, 17 각각의 이차

잉여이다. 또한

$$\begin{aligned} p = 5 \Rightarrow & \left(\frac{-2p}{17}\right) = \left(\frac{7}{17}\right) = (-1)^{\frac{7-1}{2} \cdot \frac{17-1}{2}} \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = -1 \stackrel{4}{\cancel{1}} \\ p = 11 \Rightarrow & \left(\frac{-2p}{5}\right) = \left(\frac{3}{5}\right) = -1 \stackrel{4}{\cancel{1}} \\ p = 17 \Rightarrow & \left(\frac{-2p}{11}\right) = \left(\frac{-1}{11}\right) = (-1)^{\frac{11-1}{2}} = -1 \stackrel{4}{\cancel{1}} \end{aligned}$$

이므로  $p$ 는 5, 11, 17 중 하나가 될 수 없다.

ㄱ. 이차잉여

$$\begin{aligned} \left(\frac{-11}{p}\right) &= \left(\frac{-1}{p}\right) \left(\frac{11}{p}\right) = (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2} \cdot \frac{11-1}{2}} \left(\frac{p}{11}\right) \\ &= (-1)^{\frac{p-1}{2}(1+5)} = 1 \\ &\because 1 = \left(\frac{-2p}{11}\right) \left(\frac{9}{11}\right) \left(\frac{p}{11}\right) \end{aligned}$$

ㄴ. 이차비잉여

$$1 = \left(\frac{-2p}{5}\right) = \left(\frac{3}{5}\right) \left(\frac{p}{5}\right) = (-1)(-1)^{\frac{p-1}{2} \cdot \frac{5-1}{2}} \left(\frac{5}{p}\right) = -\left(\frac{5}{p}\right)$$

이므로  $\left(\frac{5}{p}\right) = -1$  이다.

ㄷ. 이차잉여

$$\begin{aligned} 1 &= \left(\frac{-2p}{17}\right) = \left(\frac{15}{17}\right) \left(\frac{p}{17}\right) = \left(\frac{3}{17}\right) \left(\frac{5}{17}\right) (-1)^{\frac{p-1}{2} \cdot \frac{17-1}{2}} \left(\frac{17}{p}\right) \\ &= (-1)^{\frac{3-1}{2} \cdot \frac{17-1}{2}} \left(\frac{17}{3}\right) (-1)^{\frac{5-1}{2} \cdot \frac{17-1}{2}} \left(\frac{17}{5}\right) \left(\frac{17}{p}\right) \\ &= \left(\frac{2}{3}\right) \left(\frac{2}{5}\right) \left(\frac{17}{p}\right) = (-1)(-1) \left(\frac{17}{p}\right) = \left(\frac{17}{p}\right) \end{aligned}$$

이므로  $\left(\frac{17}{p}\right) = 1$  이다.

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

는 제가 아니므로 역원이 없는 애들도 있음.

(p6)  $\mathbb{Z}_{2014}$  [1]에서  $f(x)=x^2-14=(ax+b)(cx+d)$  ( $\forall a, b, c, d \in \mathbb{Z}_{2014}$ ) 라 해보자.

그러면  $ac=1$  이므로,  $a$ 는  $\mathbb{Z}_{2014}$ 의 단원이고  $a(-a'b)+b=0$  이므로,  $f(x)$ 는  $\mathbb{Z}_{2014}$ 에서 근을 가진다.  
 $\epsilon \mathbb{Z}_{2014} \Rightarrow$  근이다.

$a, c$ 는 역원이 존재

즉  $x^2 \equiv 14 \pmod{2014}$  는 해를 갖는다.

$$2014 = 2 \cdot 19 \cdot 53 \text{이므로 } \left\{ \begin{array}{l} x^2 \equiv 14 \pmod{2} \Rightarrow x^2 \equiv 14 \pmod{19} \text{도 해를 가진다.} \\ x^2 \equiv 14 \pmod{19} \end{array} \right.$$

$$\left\{ \begin{array}{l} x^2 \equiv 14 \pmod{53} \\ 2 \nmid 14 \quad \left(\frac{14}{19}\right) = \left(\frac{-5}{19}\right) = \left(\frac{-1}{19}\right) \left(\frac{5}{19}\right) = (-1)^{\frac{19-1}{2}} \cdot 1 = -1 \end{array} \right. \text{이므로 모순.}$$

따라서 해를 갖지 않는다.