

21. (Euler 정리)

10과 서로소인 양의 정수 m 에 대하여 m^{18} 의 마지막 두 자리 수가 21이다. m^{294} 의 마지막 두 자리 수를 구하시오. [2014]

(sol) $\gcd(10, m) = 1, m \in \mathbb{Z}^+$

$$m^{18} = \dots \underline{\quad} \underline{\quad}$$

$$m^{294} = \dots \underline{\quad} \underline{\quad}$$

10의 약수 : 1, 2, 5, 10 $\rightarrow \phi(10) = 18$

$$\gcd(m, 10) = 1 \text{ 이므로 오일러 정리에 의해 } m^{18} \equiv 1 \pmod{10}$$

$$\gcd(10, m) = 1 \text{ 이므로 } \gcd(100, m) = 1$$

그러면 오일러 정리에 의해 $m^{40} = m^{\phi(100)} \equiv 1 \pmod{100}$ 가 성립한다.

또한 m^{18} 의 마지막 두 자리 수가 21이므로 $m^{18} \equiv 21 \pmod{100}$ 이 성립한다.

$$\text{따라서 } m^{294} = (m^{40})^6 \cdot m^{54} \equiv 1^6 \cdot (m^{18})^3 \equiv 21^3 \equiv 61 \pmod{100}$$

즉 m^{294} 의 마지막 두 자리 수는 61

④ Euler 정리

$$n \geq 1, \gcd(a, n) = 1 \text{ 이면 } a^{\phi(n)} \equiv 1 \pmod{n} \text{ or cf.}$$

④ Thm) 임의의 정수 a 와 b 에 대해 $a \equiv b \pmod{n}$ 일 필요충분조건은 a 와 b 는 n 으로 나누었을 때 같은 나머지를 가진다.

22.

자연수 m 에 대하여 집합 T_m 을

$$T_m = \{a \in \mathbb{N} \mid a^{\phi(8m)} \equiv 1 \pmod{8m}, 1 \leq a \leq 8m\}$$

으로 정의할 때, 집합 T_m 의 원소의 개수가 $4\phi(m)$ 이 되도록 하는 100이하의 자연수 m 의 개수를 풀이 과정과 함께 쓰시오. (단, N 은 자연수 전체의 집합이고, $\phi(n)$ ($n \in N$)은 n 이하의 자연수 중에서 n 과 서로소인 수의 개수로 정의되는 오일러 ϕ -함수이다.) [2019]

(sol) $m \in \mathbb{N}$ 에 대해 $T_m = \{a \in \mathbb{N} \mid \gcd(8m, a) = 1, 1 \leq a \leq 8m\}$ 임을 보이자.

(c) $a \in$

정답: 50

$m \in \mathbb{N}$ 에 대해

$$T_m = \{a \in \mathbb{N} \mid \gcd(8m, a) = 1, 1 \leq a \leq 8m\}$$

임을 보이자.

(c) $a \in LHS$ 라 하자.

$ax \equiv 1 \pmod{8m}$ 의 해 $x = a^{\varphi(8m)-1}$ 가 존재하므로 $\gcd(8m, a) \mid 1$ 이 되어 $\gcd(8m, a) = 1$ 이다.

(d) $a \in RHS$ 라 하자.

$\gcd(8m, a) = 1$ 이므로 오일러 정리에 의하여 $a^{\varphi(8m)} \equiv 1 \pmod{8m}$ 이 성립한다.

즉, T_m 의 원소의 개수는 $\varphi(8m)$ 이다.

(i) m 이 홀수인 경우

$$\varphi(8m) = \varphi(8)\varphi(m) = 4\varphi(m)$$

(ii) m 이 짝수인 경우

$$m = 2^k m', k \geq 1, m'$$
은 홀수 꼴이라 하면,

$$\varphi(8m) = \varphi(2^{k+3}m') = \varphi(2^{k+3})\varphi(m') = 2^{k+2}\varphi(m')$$

$$4\varphi(m) = 4\varphi(2^k m') = 4\varphi(2^k)\varphi(m') = 2^{k+1}\varphi(m')$$

이므로 $\varphi(8m) \neq 4\varphi(m)$ 이다.

따라서 m 이 100이하의 자연수 중 홀수인 경우 T_m 의 원소의 개수가 $4\varphi(m)$ 과 같아지므로 50개다.

23. <위수>

정수의 곱셈에서 법 m 에 대한 3의 위수(order of 3 modulo m)를 $\text{ord}_m 3$ 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

(sol) 곱셈에서 법 m 에 대한 3의 위수 = $\text{ord}_m 3$

$$r = \text{ord}_5 3 \Rightarrow 3^r \equiv 1 \pmod{5} \Rightarrow r = 4 \quad (3^4 = 81 \equiv 1 \pmod{5})$$

$$s = \text{ord}_7 3 \Rightarrow 3^s \equiv 1 \pmod{7} \Rightarrow s = 6 \quad (3^6 = 729 \equiv 1 \pmod{7})$$

$$t = \text{ord}_{35} 3 \Rightarrow 3^t \equiv 1 \pmod{35}$$

$$3^{r+s} \equiv 3^t \equiv 1 \pmod{35}$$

$$3^{10} = 59049 \equiv 4 \pmod{35} \quad (\text{X})$$

$$\gcd(3, 5) = \gcd(3, 7) = \gcd(3, 35) = 1 \quad \text{이므로}$$

오일러 정리에 의하여

$$\begin{cases} 3^t \equiv 1 \pmod{3} \\ 3^t \equiv 1 \pmod{7} \end{cases}$$

$$3^4 \equiv 1 \pmod{5}, \quad 3^6 \equiv 1 \pmod{7}, \quad 3^{\phi(35)} \equiv 1 \pmod{35} \text{ 이 성립.}$$

$$\text{따라서 } r|4, \quad s|6, \quad t|24$$

$$\begin{aligned} \phi &\in \text{승법적} \\ \phi(5) \cdot \phi(7) &= 24 \end{aligned}$$

$$\Rightarrow g \equiv \lambda_1 N_1 a_1 + \lambda_2 N_2 a_2$$

$$r=4, \quad s=6 \quad \text{위에서 구했다.}$$

$$\equiv \lambda_1 7 \cdot 1 + \lambda_2 3 \cdot 1$$

$$3^1 \equiv 3 \pmod{35}$$

$$\equiv 4 \cdot 7 \cdot 1 + 6 \cdot 3 \cdot 1 \pmod{21}$$

$$3^2 \equiv 9 \pmod{35}$$

$$= 28 + 16 = 44 \equiv 2 \pmod{21}$$

$$3^3 \equiv 27 \pmod{35}$$

$$\Rightarrow t=12$$

$$3^4 \equiv 11 \pmod{35}$$

$$3^6 \equiv 29 \pmod{35}$$

$$3^{12} \equiv 1 \pmod{35}$$

$$\Rightarrow rst = 4 \times 6 \times 12$$

$$= 288$$

24.

<보기>의 진위를 판정하고 이유를 설명하시오. [2012]

<보기>

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

참 $4k-1$

(*) Thm) 정수 a 가 $\nmid n$ 에 대해 위수 k 를 가짐.

그러면 $a^k \equiv 1 \pmod{n}$ 일 필요충분조건은

$k \mid h$ 이다. 특히 $k \mid \phi(n)$.

(sol) $x^4 \equiv -1 \pmod{p}$ 의 정수해를 a 라 하면 $a^4 \equiv -1 \pmod{p}$ 이므로

$$\gcd(a, p) = \gcd(a^4, p) = \gcd(-1, p) = \gcd(p-1, p) = 1$$

$$\text{또한 } a^4 \equiv -1 \pmod{p} \Rightarrow a^8 \equiv 1 \pmod{p} \Rightarrow \text{ord}_p a \mid 8$$

따라서 $\text{ord}_p a$ 는 $1, 2, 4, 8$ 중 하나이다.

만약 $\text{ord}_p a = 1, 2, 4$ 중 하나이면 $a^4 \equiv 1 \pmod{p}$ 가 성립.

$-1 \equiv a^4 \equiv 1 \pmod{p} \Rightarrow p \mid 1 - (-1) = 2$ 이므로 'p가 홀수인 소수'에 모순.

그러므로 $\text{ord}_p a = 8$. 그러면 페르마 소정리에 의하여 $a^{p-1} \equiv 1 \pmod{p}$

$$\Rightarrow 8 = \text{ord}_p a \mid p-1 \Rightarrow p \equiv 1 \pmod{8}$$

25. <원시근>

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

〈보기〉

Ⓐ 19는 원시근을 갖는다.
 ✗ 3은 8의 원시근이다. $\varphi^3 = 5/2$? n 은 ?

Ⓑ 1보다 큰 정수 m 의 원시근 g 와 양의 정수 i, j 에 대하여, $g^i \equiv g^j \pmod{m}$ 이면 $i \equiv j \pmod{\varphi(m)}$ 이다.
 (단, $\varphi(m)$ 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

(sol) 1. 참 ($\because n$ 이 원시근을 갖는다 $\Leftrightarrow n=2, 4, 2p^k$ (p 는 홀수인 소수))

ㄴ. 거짓 ($\because 3^2 \equiv 1 \pmod{8}$ 이므로 $\text{ord}_8 3 = 2 \neq \frac{\varphi(8)}{4}$)

ㄷ. 참 ($\because g^\lambda = g^j \pmod{m} \Rightarrow g^{j-\lambda} \equiv 1 \pmod{m}$ ($\because \gcd(g, m) = 1$))

$$\Rightarrow \varphi(m) = \text{ord}_m g \mid j - \lambda$$

$$\Rightarrow \lambda \equiv j \pmod{\varphi(m)}$$

26.

$G = \mathbb{Z}_{11} - \{0\}$ 는 곱셈에 대하여 순환군(cyclic group)이 된다.

이 사실을 이용하여 단위원시 10-제곱근(법11에 관한 원시근, primitive 10th root of unity)을 모두 구하시오. [2002]

(sol) $\text{ord}_{11} 2 = r$ 이라 하자. 페르마 소정리에 의하여 $2^{10} \equiv 1 \pmod{11}$ 이므로 $r \mid 10$ 이다.

즉, $r = 1, 2, 5, 10$ 중 하나이다.

$2^1, 2^2, 2^5$ 은 법 11에 대하여 1과 합동이 아니므로 $r = 10$ 이다.

즉 2는 11의 원시근이다. 따라서 $2^1, 2^2, \dots, 2^{10}$ 을 재배열하여 1, 2, ..., 10 중 하나와 유일하게 합동이 되도록 할 수 있다.

그러므로 2^k ($k=1, \dots, 10$) 중에서 위수 10인 원소를 찾으면 충분.

$$\text{ord}_{11} 2^k = \frac{10}{\gcd(k, 10)} \text{ 이므로 } \text{ord}_{11} 2^k = 10 \text{ 이 될 필요충분 조건은 } \gcd(k, 10) = 1$$

따라서 단위원시 10-제곱근은 $2^1, 2^3, 2^7, 2^9$ 이다.

26번 ⑧ Def) $\gcd(a, n) = 1$ 인 경우, $\text{ord}_n a = \emptyset(n)$ 이면 a 를 n 의 원시근(primitive root)이라 함.

Thm) $\text{ord}_n a = k, h > 0 \Rightarrow \text{ord}_n a^k = \frac{k}{\gcd(h, k)}$

Thm) $\gcd(a, n) = 1$ 이고 $a_1, a_2, \dots, a_{\emptyset(n)}$ 을 n 과 서로 소이고 n 보다 작은 양의 정수라 하자.

a 가 n 의 원시근이면 $a, a^2, \dots, a^{\emptyset(n)}$ 는 법 n 에 대해 어떤 순서로 $a_1, a_2, \dots, a_{\emptyset(n)}$ 와 합동.

27.

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]

(sol) 정수 2는 법 29에 대한 원시근

$$\gcd(2, 29) = 1, \text{ord}_{29} 2 = \emptyset(29)$$
$$\begin{array}{c} || \\ 28 \end{array}$$

$$2^{28} \equiv 1 \pmod{29}$$

2는 29의 원시근이므로 $2, 2^2, \dots, 2^{28}$ 은 재배열하여 $1, 2, 3, \dots, 28$ 과 법 29에 대하여 유일하게 합동이 된다.

또한 a 가 $x^4 \equiv 1 \pmod{29}$ 의 근이고 $a \equiv b \pmod{29}$ 이면 b 역시 $x^4 \equiv 1 \pmod{29}$ 의 근이 된다.

따라서 $2, 2^2, 2^3, \dots, 2^{28}$ 중에서 해를 구하면 충분하다.

$$x^4 \equiv 1 \pmod{29}$$

$$\Rightarrow 4 \bar{m}d_2 x \equiv \bar{m}d_2 \equiv 0 \pmod{28}$$

$$\Rightarrow \bar{m}d_2 x \equiv 0 \pmod{7}$$

$$\Rightarrow \bar{m}d_2 x = 7, 14, 21, 28$$

$$\Rightarrow x = 2^{7k} \quad (k \in \{1, 2, 3, 4\})$$

$$\text{따라서 } m = 2^7 \cdot 2^{14} \cdot 2^2 \cdot 2^{28} = 2^{70} \pmod{29}$$

또한 29는 소수이고 29+2이므로 페르마 소정리에 의하여 $2^{28} \equiv 1 \pmod{29}$

$$2^{70} = (2^{28})^2 \cdot 2^{14} \equiv 2^{14} \pmod{29} \Rightarrow k=14$$

28.

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]

$$(sol) \quad \text{ord}_{27} 2 = \phi(27)$$

$$\begin{array}{l} \| \\ 1, 2, 4, 5, 7, 8, 10, 11, 13, 14, \\ 16, 17, 19, 20, 22, 23, 25, 26 \end{array}$$

$$2^{18} \equiv 1 \pmod{27}$$

$$x_n \equiv 16x_{n-1} \equiv 16^2 x_{n-2} \equiv \cdots \equiv 16^n \underbrace{x_{n-n}}_{x_0} = 2^{4n} x_0 \pmod{27}$$

$$x_n \equiv x_0 \pmod{27} \text{ 이면, } 2^{4n} x_0 \equiv x_0 \pmod{27}$$

$$\Rightarrow 1 \equiv 2^{4n} \pmod{27} \quad (\because \gcd(x_0, 27) = 1)$$

$$\Rightarrow 18 = \phi(27) = \text{ord}_{27} 2 \mid 4n \quad (\because 2 \text{는 법 27에 대한 원시근})$$

$$\Rightarrow 9 \mid 2n$$

$$\Rightarrow 9 \mid n \quad (\because \gcd(2, 9) = 1) \Rightarrow \text{따라서 } n \text{은 } 9 \text{의 배수}$$

또한 $x_9 \equiv 2^{36} x_0 \equiv (2^{18})^2 x_0 \equiv x_0 \pmod{27}$ 이므로, $n=9$ 가 $x_n \equiv x_0 \pmod{27}$ 을 만족하는 최소의 자연수

29.

정수 23은 법(modulo) 89에 대한 원시근(primitive root)이고, 89는 소수이다. 정수 $a = 23^{41}$ 에 대하여 $a^n \equiv 23 \pmod{89}$ 를 만족하는 가장 작은 양의 정수 n 의 값을 풀이 과정과 함께 쓰시오. [2016]

$$(sol) \quad \gcd(23, 89) = 1$$

$$\text{ord}_{89} 23 = \phi(89)$$

$$= 88$$

$$a^n \equiv 23 \pmod{89}$$

$$\Rightarrow 23^{41n} \equiv 23 \pmod{89}$$

$$\Rightarrow 23^{41n-1} \equiv 1 \pmod{89}$$

$$\Rightarrow 88 = \phi(89) = \text{ord}_{89} 23 \mid 41n - 1$$

$$\Rightarrow 4111 \equiv 1 \pmod{88}$$

$$\Rightarrow (-15) \cdot 4111 \equiv -15 \pmod{88}$$

$$\because 88 = 41 \times 2 + 6 \Rightarrow 1 = 6 - 5$$

$$41 = 6 \times 6 + 5 \quad = 6 - (41 - 6 \times 6)$$

$$6 = 5 \times 1 + 1 \quad = 41 \times (-1) + 6 \times 7$$

$$= 41 \times (-1) + 7(88 - 41 \times 2)$$

$$= 41 \times (-15) + 7 \times 88 \Rightarrow x = -15$$

$$\Rightarrow 11 \equiv 73 \pmod{88}$$

$$\text{또한 } a^{73} = 23^{41 \cdot 73} \equiv 23^{2993} \equiv (23^{88})^{34} \cdot 23^1 \equiv 23 \pmod{89}$$

이므로 $a^7 \equiv 23 \pmod{89}$ 를 만족하는 가장 작은 양의 정수는 73.

30.

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]

$$(\text{sol}) \quad \gcd(3, 50) = 1, \quad \text{ord}_{50} 3 = \varphi(50) = 20$$

3은 50의 원시근이고 $\varphi(50) = 20$ 이므로 $3, 3^2, \dots, 3^{20}$ 은 재배열하여 1, 3, 7, ..., 49 와 유일하게 합동이 된다.

또한 a 가 $x^{12} \equiv -9 \pmod{50}$ 의 근이고 $a \equiv b \pmod{50}$ 이면 b 역시 $x^{12} \equiv -9 \pmod{50}$ 의 근이 된다.

따라서 먼저 $3, 3^2, 3^3, \dots, 3^{20}$ 중에서 해를 구한 후 mod 50 으로 뺄셈을 줄여주면 문제에서 요구하는 값이 된다.

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

$$12 \text{ind}_3 x \equiv \text{ind}_3(-9)$$

$$= \text{ind}_3(-1) + \text{ind}_3 9$$

$$= 10 + 2$$

$$\equiv 12 \pmod{20}$$

$$\Rightarrow \text{ind}_3 x \equiv 1 \pmod{5}$$

$$\text{ind}_3 x = 1, 6, 11, 16 \Rightarrow x \equiv 3, 3^6, 3^{11}, 3^{16} \pmod{50}$$

따라서 $\mathbb{Z}/50\mathbb{Z}$ 에 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 정수해는 3, 21이 되어 합은 24 ■