Class 19

Saturday, March 20, 2021 9:55 PM

Modular Arithmetic

1) $(a \overset{*}{\pm} b) \% m = ((a \% m) \overset{*}{\pm} (b \% m)) \% m$

$(\underbrace{a + b}) \% m$

$(a \times b) \% m$

$(\underbrace{10^{17} \times 10^{17}}) \% 5$

$(0 \sim 4) \quad (0 \sim 4)$

— o —

Euler Totient

$\phi(n)$ = count of co-prime number with n from 1 to n.

$\phi(6) =$ 1, 6   2, 6   3, 6   4, 6   5, 6   6, 6

1   2   3   2   1   6

$= 2$

$$\phi(n) = n \cdot \prod_{i=0}^{k-1} \frac{P_i - 1}{P_i}$$

[যেখানে, k = number of unique primes in the prime fact. of n]

$$\phi(12) = 12 \cdot \frac{2-1}{2} \cdot \frac{3-1}{3}$$

$= 4$

$12 \rightarrow 2^2 \times 3^1$

$P_0 = 2 \quad P_1 = 3$

$$\phi(4) = 4 \cdot \frac{1}{2} = 2$$

$$\phi(p) = \cancel{p} \cdot \frac{p-1}{\cancel{p}} = p - 1$$

$1 \ldots n$

2/3   4/5

$\phi(n) = n \cdot (\text{something})$

$\phi(12) = 12 \cdot \underbrace{\frac{1}{2} \cdot \frac{2}{3}}$

1 2 3 4 5 6 7 8 9 10 11 12 13

$i \to$	1	2	3	4	5	6	7	8	9	10	11	12	13
$\phi \to$	1	$\cancel{2}$ 1	$\cancel{3}$ 2	$\cancel{4}$ 2	$\cancel{5}$ 4	$\cancel{6}$ $\cancel{3}$ 2	$\cancel{7}$ 6	$\cancel{8}$ 4	$\cancel{9}$ 6	$\cancel{10}$ $\cancel{5}$ 4	$\cancel{11}$ 10	$\cancel{12}$ $\cancel{6}$ 4	$\cancel{13}$ 12

$$x \cdot \frac{p-1}{p} = \frac{x\cancel{p}}{\cancel{p}} - \frac{x}{p}$$

$$= x - \frac{x}{p}$$

$$= phi - \frac{phi}{p}$$

$$F_n = \{ \ldots\ldots \} \qquad F_3 = \{ 1/3, 2/3, 1/2 \}$$

$$F_{n+1} = \{ F_n, \underbrace{\ldots\ldots}\} \qquad F_4 = \{ F_3, \underbrace{1/4, 3/4} \}$$

$$F_n = F_{n-1} + \underbrace{\phi(n)}$$

$$\phi(4)$$

$$\{1 \ldots\ldots 4\} \qquad \frac{1, 3}{4}$$

$$\{1 \ldots 3\}$$

1) $$\boxed{a^{\phi(m)} \% m = 1} \qquad [\because \gcd(a,m) = 1]$$

$a^{p-1} \% p = 1$

$4^6 \% 7 = 1$

$7^9 \equiv 7^0$

7^1

7^2

7

$4^1 \% 17$

$4^2 \% 17$

$4^3 \% 17$

$4^{10215} \% 17$

$7^{\boxed{1+0+1+1+2+3+5+7+9}} \% 17$

$= 7^2 \% 17$

$= 11$

$7^{n \to 1011\,2\,3\,5\,7\,9} \% 17 \Longrightarrow \underbrace{7, 11, 1}$

$3 \to 3k$

$a^0 \% m = 1$

$\boxed{1 \sim 16}$

$7^0 \to 1$

$7^1 \to 7$

$7^2 \to 15$

$7^3 \to 3$

$7^4 \to 4$

$7^5 \to 11$

$7^6 \to 9$

$7^7 \to 12$

$7^8 \to 16$

$7^9 \to 10$

$7^{10} \to 2$

$7^{11} \to 14$

$7^{12} \to 13$

$7^{13} \to 6$

$7^{14} \to 8$

$7^{15} \to 5$

$7^{16} \to 1$

$7^{32} \to 1$

$7^5 \rightarrow 11 \quad 7 \rightarrow 14 \quad 7^0 \rightarrow 1$

$(7^{16} \cdot 7^{16}) \% 17$

$(1 \cdot 1) \% 17$

$7 \% 17$

$a^{\phi(m)} \% m = 1$

$a^{16} \% 17 = 1$

$\phi(19)$

$7 \% 19 = 1$

$7^{18} \% 19 = 1$

1 3 2 1 3 2 1 3 2

3k

100位

1 2 3 4 5 6 1 2 3 3 4 4 4 9 9 9 9 1 2 3 ...

53219 % 12

$a^{\cdots} \% 13$

$\phi(13) = 12$

$a^{b} \% 13$

$[0 \sim 12]$

$[0 < a < 10^{18}]$ $[0 < b < 10^{100}]$

1

$n-3 \cdots\cdots$

$n-2$

$n-1$

n

$\% \, (10^9+7)$

$[0 < n < 10^{15}]$

20%

10^5

$(0.8)^{100000}$

$80\% \quad 0.8$

$(0.8)^2$

$(0.8)^3$

$(0.8)^4$

$p \times p$

0.8×0.8

0.8×0.2