

Euler Totient

ফাই (phi)

$$\phi(n) = x$$

1 থেকে n পর্যন্ত কতগুলো number n এর সাথে
co-prime $\rightarrow n=10$ $\phi(10)=4$

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 \end{array}$$

$$\phi(p) = p - 1$$

p

$$\boxed{1 \dots p-1}, \boxed{p}$$

$$p-1$$

$$\phi(p^k) = p^k - p^{k-1}$$

$$\text{gcd}(a, p) = 1$$

$$a < p$$

p 2nd prime

$$N = p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \dots \times p_k^{\alpha_k}$$

$$\phi(N) = \phi(p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \dots \times p_k^{\alpha_k})$$

$$= \phi(p_1^{\alpha_1}) \times \phi(p_2^{\alpha_2}) \dots \phi(p_k^{\alpha_k})$$

$$= \left(p_1^{\alpha_1} - p_1^{\alpha_1-1}\right) \left(p_2^{\alpha_2} - p_2^{\alpha_2-1}\right) \dots \left(p_k^{\alpha_k} - p_k^{\alpha_k-1}\right)$$

$$= \left(p_1^{\alpha_1} - \frac{p_1^{\alpha_1}}{p_1}\right) \dots$$

$$= p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2} \left(1 - \frac{1}{p_2}\right) \dots p_k^{\alpha_k} \left(1 - \frac{1}{p_k}\right)$$

$$= N \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \left(1 - \frac{1}{p_3}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

$$\phi(N) = N \cdot \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$$

$$\begin{array}{ll} p_1 = 2 & \alpha_1 = 2 \\ p_2 = 3 & \alpha_2 = 1 \\ p_3 = 5 & \alpha_3 = 1 \end{array}$$

Euler's Theorem

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

$$\boxed{\text{gcd}(a, p) = 1}$$

congruence

$$a^{p-1} \% p = 1 \iff a \equiv 1 \pmod{p}$$

$$a = 77$$

$$p = 997$$

$$77^{996} \% 997$$

$$\boxed{77} \cdot \boxed{13949} \% \boxed{997}$$

$$= (77^{(996 \times 14) + 5}) \% 997$$

$$= (77^{\boxed{996} \times \boxed{14} \cdot 77^5}) \% 997$$

\boxed{x}

$$\phi(60) = 60 \left(\frac{2-1}{2} \right) \left(\frac{3-1}{3} \right) \left(\frac{5-1}{5} \right)$$

=

=

$$\boxed{n} \rightarrow a \% m$$

$$\boxed{n \% \phi(m)} \rightarrow a \% m$$

$$= (77 \cdot 77) / 5$$

$$= 77^2 \% 997$$

$$\rightarrow [n \% \phi(m) + \phi(m)] \% m$$

$$\boxed{n \geq \log_2 m}$$

Exponential

$$\phi(1) = 1$$

$$n! = n(n-1)(n-2) \dots 1$$

$$f(n, m) = n^{n-1} \% m$$

$$n=5 \rightarrow \begin{array}{|c|} \hline 1 \\ \hline 2 \\ \hline 3 \\ \hline 4 \\ \hline 5 \\ \hline \end{array} \% 997$$

$$5^{196} \% 997$$

$$\begin{array}{|c|} \hline 2^1 \\ \hline 3 \\ \hline 4 \\ \hline 5 \\ \hline \end{array}$$

$$\begin{array}{|c|} \hline 262144 \\ \hline 5 \\ \hline \end{array}$$

$$\boxed{a^b \% M \mid O(\log_2(b))}$$

$$1 \leq a \leq 10^9$$

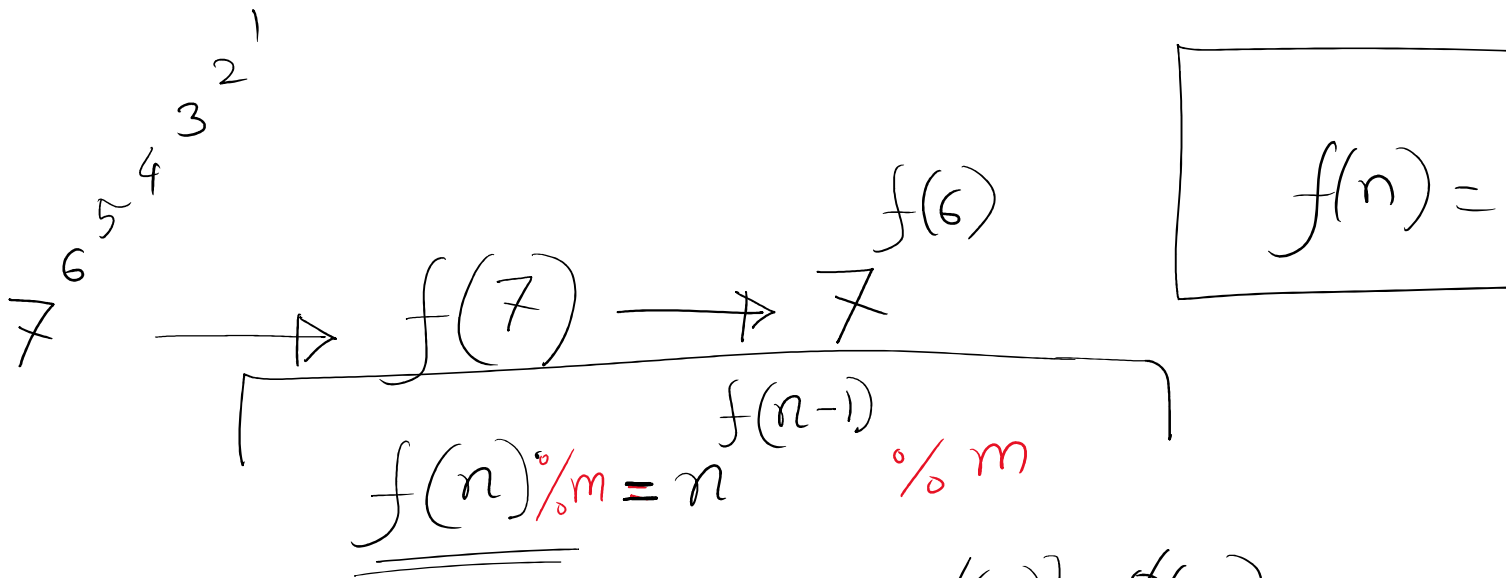
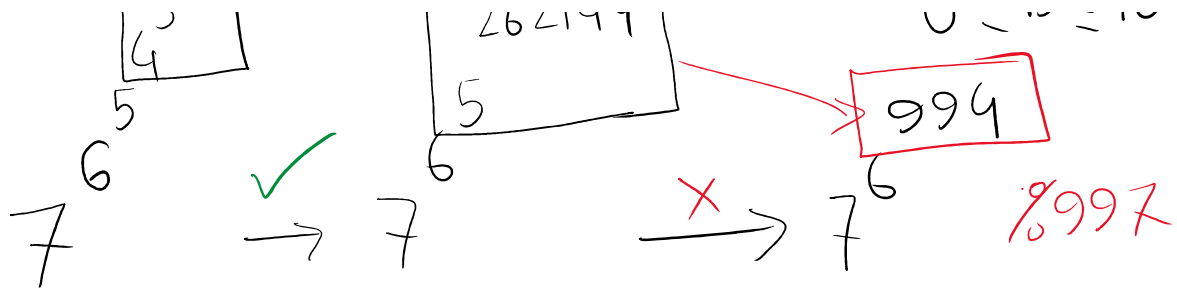
$$0 \leq b \leq 10^9$$

$$\rightarrow 2014$$

$$\begin{aligned}
 (3) &= 3 \left(\frac{3-1}{3} \right) \\
 (6) &= 6 \left(\frac{2-1}{2} \right) \left(\frac{3-1}{3} \right) \\
 (9) &= 9 \left(\frac{3-1}{3} \right) \left(\frac{3-1}{3} \right) \\
 (12) &= 12 \left(\frac{2-1}{2} \right) \left(\frac{3-1}{3} \right)
 \end{aligned}$$

$$t = i + i ; \text{mult} \leq n ; \text{mult} += i$$

$$\begin{aligned}
 (\text{mult}) & /= i ; \\
 (\text{mult}) & * = (i - 1) ;
 \end{aligned}$$



$$[f(n-1) \% \phi(m)] + \phi(m) \% m = n$$

$$f(7) \% 997 = 7 \quad [984] + 996 \% 997$$

$$f(6) \% \phi(997) = (297) + 328 \% 996$$

$$\Rightarrow f(6) \% 996 = 6 = 984$$

$$f(5) \% 328 = 297$$

$$f(4) \% 111 = 11$$

$$f(n-1)$$
$$n$$

$$1) n \rightarrow \phi(n)$$

$$1 \leq n \leq 10^{15}$$

$$2) n \rightarrow \phi[1, n]$$

$$1 \leq n \leq 10^6$$

$$f(4) \% 160 = 64$$

$${}^nC_r = \frac{n!}{r!(n-r)!}$$

$$= \frac{\text{fact}[n]}{\text{fact}[r] \times \text{fact}[n-r]}$$

$$= (\text{fact}[n] \times (x^{M-2} \% M)) \% M$$

$$1 \leq n \leq 10$$

$$1 \sim 10^6 \dots$$

$$\text{fact}[i] \bmod (10^6 + 3)$$

$$= \frac{\text{fact}[n]}{x}$$

$$\left(\text{fact}[n] \times \frac{1}{x} \right) \% M$$

1

1

1

$$a^{p-1} \equiv 1 \pmod{p}$$

$$a^{p-1-1} \equiv a^{-1} \pmod{p}$$

$$a^{p-2} \equiv a^{-1} \pmod{p}$$

$$a^{p-2} \% p \equiv a^{-1} \% p$$