Class 18

Wednesday, June 1, 2022 11:01 PM

$a^b \% M \rightarrow (3^n + 1) \% M$; $1 \le n \le 10^{10000}$

$2 \le M \le 10^{19}$

$[0, M-1]$

$\log_2(n) = \log_2(10^{10000})$

$a^{P-1} \% P = 1$ $\quad 2^{96} \% 97 = 1$

$2^4 \% 5 = 1$

$3^{19257123} \% 11 = 3^3 \% 11$

$\phi(M)$

$(3^n + 1) \% M$

$\phi(13) = 12$ $\quad \phi(11) = 10$

$\phi(12) = 12\left(\frac{2-1}{2}\right)\left(\frac{3-1}{3}\right) = 4$

$= (3^{n \% \phi(M)} + 1) \% M$

$= (3^{n \% (M-1)} + 1) \% M$

$3^{97} \% 11 = 3^{97}$

19) 123456789563 (64

114

94

76

19) 1234 (

num = 0 × 10 + 2

= 10 + 2 = 12 % 19

= 12

= 12 × 10 + 3 = 123

19) 1234(

94

18

(18)

$= 12$

$= 12 \times 10 + 3 = 123$

$\% 19$

$= 9$

$$\frac{(3^N + 1)}{2} \% M$$

$$\left(\frac{3^N + 1}{2}\right) \% M = \left(\frac{A}{2}\right) \% M = (A \cdot \frac{1}{2}) \% M$$

$$= (A \cdot 2^{-1}) \% M$$

$$= ((A \% M) \cdot (2^{-1} \% M)) \% M$$

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

$\Rightarrow (a^p \cdot a^{-1}) \% p = 1$

$\Rightarrow ((a^p \% p) \cdot (a^{-1} \% p)) \% p = 1$

$\Rightarrow (a \cdot (a^{-1} \% p)) \% p = 1a^0$

$\Rightarrow$

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

$a^{p-1} \% p = a^{1-1} = a^0$

$a^{p-1+p-2} = a^{p-2}$

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

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

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

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

$(0.5)\%M \rightarrow$

$(3^n + 1)\%M$ x X

$a^b \% m$

$b \geq \log_2 m$

$= a^{[b \% \phi(m)] + \phi(m)} \% m$

Exponial

$f(n) = n^{n-1^{n-2^{n-3^{n-4^{\cdots 1}}}}} \% m$

$f(5) = 5^{4^{3^{2^1}}} = 5^{f(4)}$

$f(n, m) = n^{n-2^{\cdots 1}} \% m$

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

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

$f(a_1, b_1) = n^{f(a_2, b_2)} \% m$