18/6/20 Numbers Theory 3 C.W.

* matrix Exponentiation

e.g. - nth fibonacci no.

$$f(n) = f(n-1) + f(n-2)$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} f(n) \\ f(n-1) \end{bmatrix} = \begin{bmatrix} f(n+1) \\ f(n) \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

$\therefore$

$$m^{n-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} f(n) \\ f(n-1) \end{bmatrix}$$

$$\begin{bmatrix} \cdot & \cdot \\ \cdot & \cdot \end{bmatrix} \begin{bmatrix} \cdot & \cdot \\ \cdot & \cdot \end{bmatrix}$$

$$\begin{matrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{matrix}$$

$$\begin{matrix} 1 & 1 & 2 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \end{matrix}$$

$$\begin{matrix} 3 \\ 2 \end{matrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} a \\ c \end{bmatrix} \qquad \begin{bmatrix} 1 \\ 1 \end{bmatrix} \qquad \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

↳ Applications of modular exponentiation

let

① $f(n) = a * f(n-1) + b * f(n-2)$

$$\begin{bmatrix} b & a \\ 1 & 0 \end{bmatrix} \begin{bmatrix} f(n) \\ f(n-1) \end{bmatrix} = \begin{bmatrix} f(n+1) \\ f(n) \end{bmatrix}$$

$$f(n+1) = a * f(n) + b f(n-1)$$

② $f(n) = f(n-1) + f(n-2) + c$

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} f(n) \\ f(n-1) \\ c \end{bmatrix} = \begin{bmatrix} f(n+1) \\ f(n) \\ c \end{bmatrix}$$

③ $f(n) = f(n-1) + f(n-3)$

$$\begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} f(n) \\ f(n-1) \\ f(n-2) \end{bmatrix} = \begin{bmatrix} f(n+1) \\ f(n) \\ f(n-1) \end{bmatrix}$$

$$f(n) \longrightarrow f(n-1) \text{ odd}$$
$$\hookrightarrow f(n-2) \text{ even}$$

Dono ko alg alg nikal ke solve karlo

Q: Fibonacci Sum

$\rightarrow$ $T(n) = T(n-1) + F(n)$

$$\underbrace{10 \quad 11}_{12} \quad \underbrace{12 \quad 13}_{14} \quad \underbrace{14 \quad 15}_{16} \quad \underbrace{16 \quad 17}_{18} \quad \underbrace{18 \quad 19}_{20}$$

$F_0 = 0$

$F_1 = 1$

$F_2 = F_1 + F_0$

$F_3 = F_2 + F_1$

$F_4 = F_3 + F_2$

$\vdots$

$f_n = f_{n-1} + f_{n-2}$

$f_n = f_{n-2} + f_{n-3} + \dots + f_1 + 1$

$\cancel{f_n - 1} =$

$f_n - 1 = f_{n-2} + f_{n-3} + \dots + f_1$

$= S_{n-2}$

$\Rightarrow \quad S_n = f_{n+2} - 1$

Q. Fermat's little theorem

If p is prime no.

$\Rightarrow$ $(a^{p}) \bmod p = a$

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

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

Application

- 1> In mod inverse.

eg - $(A.B) \bmod m = 1$ $\quad B = A^{-1}$

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

$(a^{p-1}) \bmod p = 1$

$a^{-1} * (a^{p-1}) \bmod p = a^{-1}$

$(a^{-1} * (a^{p-1}) \bmod p) \bmod p = a^{-1} \bmod p$

$(a^{-1} * a^{p-1}) \bmod p = a^{-1} \bmod p$

$(a^{p-2}) \bmod p = a^{-1} \bmod p$

If we need to calculate $a^{-1} \% m$
where m is prime,

then, $\quad a^{-1} \% m = (a^{m-2}) \bmod m$

Wilson's Theorem

If p is a prime.

$$\boxed{(p-1)! \bmod p = -1 \text{ or } (p-1)}$$

Application.

↳ when we need to calculate $(n!) \bmod p$

$(n!) \% p$

$n >= p$ then $(n!) \% p = 0$

$\boxed{n < p}$

$(1 * 2 * \ldots n) \% p$

$[1 * 2 * n * (n+1) \ldots * (p-1)] \% p$

$= -1$

$(a * b) \% m = (a \% m * b \% m) \% m$

$\Rightarrow (n! \bmod p) * ((n+1) * \ldots * (p-1)) \% p = -1$

$(n!) \% p = (-1) * (n+1)^{-1} \bmod p *$

$(n+2)^{-1} \bmod p *$

$\ldots * (p-1)^{-1} \bmod p$

$= x + p$

On applying ~~Fe~~ Fermat's theorem,

$$(n!)\%p = -1 * (n+1)^{p-2} \bmod p - \dots (p-1)^{p-2} \bmod p.$$

$$= -1 * \{(n+1) \dots (p-1)\}^{p-2} \bmod p$$

Q Income on nth day

→ $f(n) = f(n-1) + f(n-2) + f(n-1) * f(n-2)$

$f(0), f(1)$ are given

$$f(n) = f(n-1)(1 + f(n-2)) + f(n-2)$$

$$f(n) = (1 + f(n-1))(1 + f(n-2)) - 1$$

$$1 + f(n) = (1 + f(n-1))(1 + f(n-2))$$

let $G(n) = 1 + f(n)$

$$G(n) = G(n-1) * G(n-2)$$

$G(0), G(1)$ can be calculated.

$G(0) = a$

$G(1) = b$

$G(2) = ab$

$G(3) = ab^2$

$G(4) = a^2 b^3$

$G(5) = a^3 b^5$

$G(n) = a^{fib(n-1)} b^{fib(n)}$

$$G(n) = \left(a^{fib(n-1)} * b^{fib(n)}\right) \% m$$

$$= \left(a^{fib(n-1)} \% m * b^{fib(n)} \% m\right) \% m$$

$$\boxed{a^{p-1} \bmod p = 1} \quad p \Rightarrow \text{when } p \text{ is prime}$$

$$fib(n-1) = k * (p-1) + fib(n-1) \% (p-1)$$

$$a^{fib(n-1)} \% m = \left(a^{k*(p-1)+x}\right) \% m$$

$$= \underbrace{\left(a^{k*(m-1)}\right) \% m}_{=1} * a^{x} \% m$$

$$= \left(a^{x}\right) \% m$$

$$x = fib(n-1) \% (p-1)$$

$$G(n) = \left(\left(a^{fib(n-1) \% (m-1)}\right) \% m * \left(b^{fib(n) \% (m-1)}\right) \% m\right) \% m$$

Concepts used

1> matrix exponentiation

1> modular exponentiation

1> Fermat's Theorem

1> Recurrence Relation