

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

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

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

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

$$1 + f_n = \underline{\underline{G_n}}$$

$$G_n = (G_{n-1}) (G_{n-2})$$

$$G_0 = a$$

$$G_1 = b$$

$$G_2 = ab$$

$$G_3 = ab^2$$

$$G_4 = a^2b^3$$

$$G_5 = a^3b^5$$

$$G_n = a^{f_{n-1}} b^{f_n}$$

$$a^2b^3$$

$$a = 1+1=2$$

$$b = 2+1=3$$

$$2^2 \times 3^3$$

$$= 4 \times 27$$

$$= 108$$

$$C_n = \begin{pmatrix} a^{f_{n-1}} & b^{f_n} \end{pmatrix} \text{ dom}$$

$$C_n \text{ to } (0^{q+2})$$

$$C_n = (a^{f_{n-1}} \text{ dom} \times b^{f_n} \text{ dom}) \text{ dom}$$

prim  $\infty$

$f_n \rightarrow$  can be big

$\hookrightarrow f_n \rightarrow$  matrix expo

$\rightarrow O(\log n)$

$a^{b-1} \text{ top} = 1 \rightarrow$  By Fermat Theorem.

$$f_{n+1} = K \times (p-1) + f_{n+1} \cdot p_0(p-1)$$

$$14 = 2 \times 5 + 4$$

$$a^{f_{n-1}} \pmod p = \left( a^{k \cdot (p-1) + \overbrace{f_{n-1} \pmod{p-1}}^{\gamma}} \right) \pmod p$$

$$= \left( a^{k(p-1) + \gamma} \right) \pmod p$$

$$= \left( a^{k(p-1)} \pmod p \right) \times \left( a^{\gamma} \pmod p \right)$$

$\downarrow$   
1

fermat num

$$a^{f_{n-1}} \pmod p = \underline{\underline{a^{\gamma} \pmod p}}$$

modular expo

$$\gamma = \underline{\underline{f_{n-1} \pmod{p-1}}}$$

# # Euler Toint function

→

$\phi(n)$

phi n

$(n > 1)$

→ No. of  $n$  such that

$1 \leq m < n$  &  $\gcd(m, n) = 1$

$m, n$  are co-prime.

$$\phi(3) = 2 \rightarrow (1, 2)$$

$$\phi(4) = 2 \quad (1, 3)$$

$$\phi(5) = 4 \quad \underline{\underline{(1, 2, 3, 4)}}$$

$$\phi(a \times b) = \phi(a) \times \phi(b) \quad \text{if } \underline{\underline{\gcd(a, b) = 1}}$$

$$\phi(\underline{\underline{n}})$$

$$n = p_1^a p_2^b p_3^c \dots p_x^z$$

$$\boxed{10 = 2^1 \times 5^1}$$

$$\phi(n) = \phi(p_1^a p_2^b p_3^c \dots)$$

$$\phi(p_1^x p_2^y) = \phi(p_1^x) \phi(p_2^y)$$

because

$$\underline{\underline{\gcd(p_1^x, p_2^y) = 1}}$$

$$\phi(n) = \phi(p_1^a) \phi(p_2^b) \phi(p_3^c) \dots$$

$$\phi(p^a)$$

$$p^a = 1, 2, 3, \dots, p, \dots, 2p, \dots, 3p, \dots, p^a$$

$$\text{Total count} = p^a$$

$$p^a - (\text{Total not coprime to } p^a)$$

↪ all multiples of  $p$



$$\phi(\underline{p^a}) = p^a - p^{a-1} \\ \Rightarrow p^a \left(1 - \frac{1}{p}\right)$$

$$\phi(n) = p_1^a \left(1 - \frac{1}{p_1}\right) p_2^b \left(1 - \frac{1}{p_2}\right) \dots$$

$$\phi(n) = \underbrace{p_1^a \times p_2^b \times p_3^c \dots}_{\dots} \times \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots$$

$$\phi(n) = n \times \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \times \left(1 - \frac{1}{p_3}\right) \dots$$

1 2 3 4 5 6 7 8 9

Sier → 1 2 3 4 5 6 7 8 9

$4x(1-\frac{1}{2})$   
 $2x(1-\frac{1}{2})$   
 $2x \frac{1}{2} \rightarrow 1$   
 $3x(1-\frac{1}{3})$   
 $\rightarrow 2$

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

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

if  $p \rightarrow \text{prime}$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
s →	1	<del>2</del>	<del>3</del>	<del>4</del>	<del>5</del>	<del>6</del>	<del>7</del>	<del>8</del>	<del>9</del>	<del>10</del>	11	<del>12</del>	13	<del>14</del>
		1	2	2	4	<del>3</del>	6	4	6	<del>5</del>		6		<del>7</del>
						2	6	4	6	4		4		6