

$$10175, 2277$$

$$10175 : 2277 = 4 \text{ ob } 1067$$
$$\begin{array}{r} 10175 \\ - 9108 \\ \hline 1067 \end{array}$$

$$10175 = 4 \cdot 2277 + 1067 \quad (4)$$

$$2277 : 1067 = 2 \text{ ob } 143$$

$$2277 = 2 \cdot 1067 + 143 \quad (3)$$

$$1067 : 143 = 7$$

$$1067 = 7 \cdot 143 + 66 \quad (2)$$

$$143 : 66 = 2$$

$$143 = 2 \cdot 66 + 11 \quad (1)$$

$$66 : 11 = 6 \text{ ob } 0$$

$$\begin{aligned} 11 &= 143 - 2 \cdot 66 = 143 - 2 \cdot (1067 - 7 \cdot 143) = \\ &= 15 \cdot 143 - 2 \cdot 1067 = 15 \cdot (2277 - 2 \cdot 1067) - \\ &\quad - 2 \cdot 1067 = 15 \cdot 2277 - 32 \cdot 1067 = \\ &= 15 \cdot 2277 - 32 \cdot (10175 - 4 \cdot 2277) \\ &= 143 \cdot 2277 - 32 \cdot 10175 \end{aligned}$$

$$(10175, 2277) = 2277 \cdot x + 10175 \cdot y$$

$$\varphi(m) = |\{a \in \mathbb{N} \mid a \leq m; (a, m) = 1\}|$$

$$m = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$$

$$\varphi(m) = (p_1 - 1) \cdot p_1^{\alpha_1 - 1} \cdot \dots \cdot (p_k - 1) \cdot p_k^{\alpha_k - 1}$$

$$\varphi(120) = \varphi(6 \cdot 20) = \varphi(2 \cdot 3 \cdot 2 \cdot 2 \cdot 5) =$$

$$= \varphi(2^3 \cdot 3 \cdot 5) =$$

$$= 1 \cdot 2^2 \cdot 2 \cdot 3^0 \cdot 4 \cdot 5^0 =$$

$$= 32$$

$$\varphi(n) = 6 \quad \varphi(n) = (p_1 - 1) p_1^{\alpha_1 - 1} \cdot \dots \cdot (p_k - 1) p_k^{\alpha_k - 1}$$

$$\varphi(n) = 2 \cdot 3$$

$$\varphi(n) = 2 \cdot 3$$

$$\frac{\varphi(n)}{\varphi(n)} = \frac{2 \cdot 3}{1 \cdot 6}$$

$$\varphi(n) = 6$$

$$\textcircled{1} \varphi(n) = 1 \cdot 2 \cdot 3$$

$$(p_1 - 1) = 1$$

$$p_1 = 2$$

$$n = 2 \cdot m$$

$$\varphi(m) = 6$$

$$p_1 \alpha_1 = 1 \quad \alpha_1 = 2 \quad \alpha_1 \geq 3$$

$$\varphi(m) = 4 \cdot k$$

$$i) \alpha_1 = 1$$

$$n = 2 \cdot m; 2 \cdot m$$

$$\varphi(n) = \varphi(2 \cdot m) = \varphi(2) \cdot \varphi(m)$$

$$= \varphi(m) = 6$$

$$= 2 \cdot 3$$

$$= 6$$

$$\varphi(m) = 2 \cdot 3$$

$$(p_2 - 1) = 2$$

$$p_2 = 3$$

$$\alpha_2 = 1$$

$$\alpha_2 = 2$$

$$\alpha_2 \geq 3$$

$$m = 2 \cdot 3 \cdot m_2$$

$$\varphi(m) = \varphi(2) \cdot \varphi(3) \cdot \varphi(m_2)$$

$$\varphi(m) = 2 \cdot \varphi(m_2)$$

$$\varphi(m_2) = 3$$

X

$$m = 2 \cdot 3 \cdot m_2$$

$$\varphi(m) = 6 \cdot \varphi(m_2)$$

$$\varphi(m) = 18$$

$$\textcircled{2} \varphi(n) = 2 \cdot 3$$

$$n = 9$$

$$\textcircled{3} \varphi(n) = 6$$

$$n = 7$$

$n \in \mathbb{N}$

$$\varphi(n) = \frac{n}{2}$$

$k \in \mathbb{N}$

$$n = 2^k \cdot m$$

$$\frac{2^k \cdot m}{2}$$

$$n = 2^k$$

$$\varphi(2^k \cdot m) = \frac{2^k \cdot m}{2}$$

$$\varphi(2^k) \cdot \varphi(m) = \frac{2^{k-1} \cdot m}{2^{k-1} \cdot m}$$

$$\varphi(m) = \frac{2^{k-1} \cdot m}{2^{k-1} \cdot m}$$

$$\varphi(m) = m$$

$$m = 1$$

$$\underline{16^{15} + 29^{14} + 42^{13}} \equiv X \pmod{13}$$

$$16^{15} \equiv 3^{15} \equiv 3^{12} \cdot 3^3 \equiv 27 \equiv 1 \pmod{13}$$

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

$$29^{14} \equiv 3^{14} \equiv 3^{12} \cdot 3^2 \equiv 9 \pmod{13}$$

$$42^{13} \equiv 3^{13} \equiv 3^{12} \cdot 3 \equiv 3 \pmod{13}$$

$$X \equiv 1 + 9 + 3 \equiv 13 \equiv 0 \pmod{13}$$

$$a \equiv b \pmod{13} \Rightarrow 13 | (a - b)$$

$17 \cdot n \equiv 1 \pmod{181}$ $\boxed{17}^{-1}_{181}$

\mathbb{Z}_{181}^*

$n \equiv 17^{-1} \pmod{181}$

$\boxed{17}^{-1}_{181}$

$17n \equiv 1 \pmod{181}$
 $17n = 1 - 181x$
 $17n + 181x = 1$
 $(17, 181)$

$181 : 17 = 10 \text{ r } 11$	$181 = 10 \cdot 17 + 11$
$17 : 11 = 1 \text{ r } 6$	$17 = 1 \cdot 11 + 6$
$11 : 6 = 1 \text{ r } 5$	$11 = 1 \cdot 6 + 5$
$6 : 5 = 1 \text{ r } 1$	$6 = 1 \cdot 5 + 1$
$5 : 1 = 5 \text{ r } 0$	

$1 = 6 - 1 \cdot 5 = 6 - (11 - 1 \cdot 6) = 2 \cdot 6 - 11 =$
 $= 2 \cdot (17 - 1 \cdot 11) - 11 = -3 \cdot 11 + 2 \cdot 17 =$
 $= -3(11 - 10 \cdot 17) + 2 \cdot 17 = 32 \cdot 17 - 3 \cdot 111$

$n \equiv 32 \pmod{181}$ $\boxed{32}_{181} = \boxed{17}^{-1}_{181}$

$$s = (1, 3, 7, 8, 6, 9, 5) \circ (2, 4) \quad ||$$

$$t = (1, 5, 3) \circ (6, 8)$$

$$s = (1, 5) \circ (1, 9) \circ (1, 6) \circ (1, 8) \circ (1, 7) \circ (1, 4) \circ (2, 4) \\ \circ (3, 5) \circ (3, 5)$$

$$t = (1, 2) \circ (1, 5) \circ (6, 8) \\ s \circ t = (1, 3, 7, 8, 6, 9, 5) \circ (2, 4) \circ (1, 5, 3) \circ (6, 8) = \\ (2, 4) \circ (5, 7, 8, 9)$$

$$s^{-1} = (1, 5, 9, 6, 8, 7, 3) \circ (2, 4)$$

$$s^{20} = (1, 3, 7, 8, 6, 9, 5)^{20} =$$

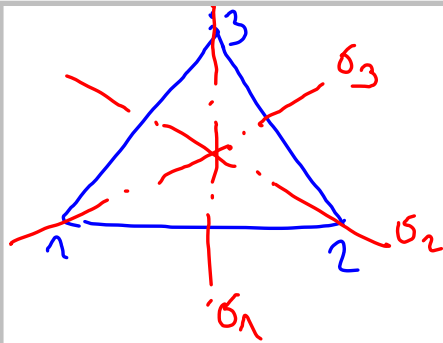
$$= (1, 3, 7, 8, 6, 9, 5) = (1, 5, 9, 6, 8, 7, 3)$$

$$s^2 = (1, 7, 6, 3, 3, 8, 9)$$

$$(s^{120} \circ t^{-3})^{14} = [(1, 3, 7, 8, 6, 9, 5) \circ (6, 8)]^{14} =$$

$$= (1, 3, 7, 8, 9, 5)^{14} =$$

$$= (1, 5, 9, 8, 7, 3)$$



$$\sigma_1: \begin{matrix} 1 \rightarrow 2 \\ 2 \rightarrow 1 \\ 3 \rightarrow 3 \end{matrix} \quad \underline{\underline{(1,2)}}$$

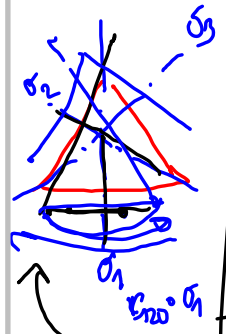
$$\sigma_2: \begin{matrix} 1 \rightarrow 3 \\ 3 \rightarrow 1 \\ 2 \rightarrow 2 \end{matrix} \quad \underline{\underline{(1,3)}}$$

$$\sigma_3: \begin{matrix} 2 \rightarrow 3 \\ 3 \rightarrow 2 \\ 1 \rightarrow 1 \end{matrix} \quad \underline{\underline{(2,3)}}$$

$$r_{120}: \underline{\underline{(1,2,3)}}$$

$$r_{240}: \underline{\underline{(1,3,2)}} \quad \sigma_2 \circ r_{120}$$

id $\sigma_2 \circ r_{120}$



\circ	id	σ_1	σ_2	σ_3	r_{120}	r_{240}
id	id	σ_1	σ_2	σ_3	r_{120}	r_{240}
σ_1	σ_1	id	r_{120}	r_{240}	σ_3	σ_2
σ_2	σ_2	r_{240}	id	r_{120}	σ_1	σ_3
σ_3	σ_3	r_{120}	r_{240}	id	σ_2	σ_1
r_{120}	r_{120}	σ_2	σ_3	σ_1	r_{240}	id
r_{240}	r_{240}	σ_3	σ_1	σ_2	id	r_{120}

$$v_{120} \circ \sigma_2$$

$$\begin{matrix} 1 \rightarrow 1 \\ 2 \rightarrow 3 \\ 3 \rightarrow 2 \end{matrix}$$

$$v_{240} \circ \sigma_1 = \sigma_3$$

$$v_{240} \circ \sigma_2$$

