$(G, \circ)$ $\quad$ $(H$

$(\mathbb{Z}_{10}, \underline{+})$ $\quad$ $H \subseteq G$

$\{\underline{0}, \ldots, \underline{9}\}$

$(G, \circ)$ $\quad$ $(H, \circ)$

$(\mathbb{Z}_{10}, +)$ $\quad$ $H \subseteq G$

$(\{0, \ldots, 9\}, +)$

$(\{0, 2, 4, 6, 8\}, +)$

$(G, \circ)$ $\quad$ $(H, \circ)$

$(\mathbb{Z}_{10}, \pm)$ $\quad$ $H \subseteq G$

$(\{0, \ldots, 9\}, +)$

$(\{0, 2, 4, 6, 8\}, +)$

$(\{0, 5\}, +)$ $\quad$ $(\{0\}, +)$

$(H, \circ)$

$(G, \circ)$ $(H, \circ)$

$(\mathbb{Z}_{10}, +)$ $H \subseteq G$

$(\{0, \ldots, 9\}, +)$

$(\{0, 2, 4, 6, 8\}, +)$

$(\{0, 5\}, +)$ $(\{0\}, +)$

$(H, \circ)$ $(G, \circ)$

$(G, \circ)$ $\quad$ $(H, \circ)$

$(\mathbb{Z}_{10}, \pm)$ $\quad$ $H \subseteq G$

$(\{0, \ldots, 9\}, +)$

$(\{0, 2, 4, 6, 8\}, +)$

$(\{0, 5\}, +)$ $\quad$ $(\{0\}, +)$

$(H, \circ)$ $\quad$ $(G, \circ)$

$R \subseteq A \times A$

$[x] = \{y \,/\, (x, y) \in R\}$

$(G, \circ)$ $\quad$ $(H, \circ)$

$(\mathbb{Z}_{10}, \pm)$ $\quad$ $H \subseteq G$

$(\{0, \ldots, 9\}, +)$

$(\{0, 2, 4, 6, 8\}, +)$

$(\{0, 5\}, +)$ $\quad$ $(\{0\}, +)$

$(H, \circ)$ $\quad$ $(G, \circ)$

$R \subseteq A \times A$

$[x] = \{y \mid (x, y) \in R\}$

$(G, \circ)$ $\quad$ $(H, \circ)$

$(\mathbb{Z}_{10}, \pm)$ $\quad$ $H \subseteq G$

$(\{0, -, 9\}, +)$

$(\{0, 2, 4, 6, 8\}, +)$

$(\{0, 5\}, +)$ $\quad$ $(\{0\}, +)$

$(H, \circ)$ $\quad$ $(G, \circ)$

$R \subseteq A \times A$

$[x] = \{y \,/\, (x, y) \in R\}$

$[a] \neq [b]$ $\quad$ $[a] \cap [b] = \emptyset$

$\mathbb{N}_1 =$ $\quad$ $[a] = \{a\}$

$(G, \circ)$ $\quad$ $(H, \circ)$

$(\mathbb{Z}_{10}, +)$ $\quad$ $H \subseteq G$

$(\{0, \ldots, 9\}, +)$

$(\{0, 2, 4, 6, 8\}, +)$

$(\{0, 5\}, +)$ $\quad$ $(\{0\}, +)$

$(H, \circ)$ $\quad$ $(G, \circ)$

$\sim \subseteq G \times G$

$G = [a_1]_\sim \cup \ldots \cup [a_k]_\sim$

$|G| = \underbrace{|[a_1]_\sim|}_{= |H|} + \ldots + |[a_k]_\sim|$

$(G, \circ)$ $\quad$ $(H, \circ)$

$(\mathbb{Z}_{10}, +)$ $\quad$ $H \subseteq G$

$(\{0, \ldots, 9\}, +)$

$(\{0, 2, 4, 6, 8\}, +)$

$(\{0, 5\}, +)$ $\quad$ $(\{0\}, +)$

$(H, \circ)$ $\quad$ $(G, \circ)$

$\sim \subseteq G \times G$

$G = [a_1]_\sim \cup \ldots \cup [a_k]_\sim$

$|G| = \underbrace{|[a_1]_\sim|}_{l} + \ldots + |[a_k]_\sim|$

$|H|$ $\quad$ $|[a_i]_\sim| = |[a_j]_\sim|$

$|G| = k \cdot l$

$(G, \circ)$ $\quad$ $(H, \circ)$

$(\mathbb{Z}_{10}, \pm)$ $\quad$ $H \subseteq G$

$(\{0, \ldots, 9\}, +)$

$(\{0, 2, 4, 6, 8\}, +)$

$(\{0, 5\}, +)$ $\quad$ $(\{0\}, +)$

$(H, \circ)$ $\quad$ $(G, \circ)$

$\sim \subseteq G \times G$

$G = [a_1]_\sim \cup \ldots \cup [a_k]_\sim$

$|G| = \underbrace{|[a_1]_\sim|}_{\ell} + \ldots + |[a_k]_\sim|$

$\| \qquad\qquad |[a_i]_\sim| = |[a_j]_\sim|$

$|H|$

$|G| = k \cdot \ell$

$(G, \circ)$ $\quad$ $(H, \circ)$

$(\mathbb{Z}_{10}, +)$ $\quad$ $H \subseteq G$

$(\{0, \ldots, 9\}, +)$

$(\{0, 2, 4, 6, 8\}, +)$

$(\{0, 5\}, +)$ $\quad$ $(\{0\}, +)$

$(H, \circ)$ $\quad$ $(G, \circ)$

$\sim \subseteq G \times G$

$G = [a_1]_\sim \cup \ldots \cup [a_k]_\sim$

$|G| = \underbrace{|[a_1]_\sim|}_{\ell} + \ldots + |[a_k]_\sim|$

$\parallel$

$|H|$

$|[a_i]_\sim| = |[a_j]_\sim|$

$|G| = k \cdot \ell$

$(G, \circ)$ $\quad$ $(H, \circ)$

$(\mathbb{Z}_{10}, \pm)$ $\quad$ $H \subseteq G$

$(\{0, \ldots, 9\}, +)$

$(\{0, 2, 4, 6, 8\}, +)$

$(\{0, 5\}, +)$ $\quad$ $(\{0\}, +)$

$(H, \circ)$ $\quad$ $(G, \circ)$

$\sim \subseteq G \times G$

$G = [a_1]_\sim \cup \ldots \cup [a_k]_\sim$

$|G| = \underbrace{|[a_1]_\sim|}_{l} + \ldots + |[a_k]_\sim|$

$|[a_1]_\sim| = |H|$

$|[a_i]_\sim| = |[a_j]_\sim|$

$|G| = k \cdot l$

$(G, \circ)$ $\quad$ $(H, \circ)$

$(\mathbb{Z}_{10}, \pm)$ $\quad$ $H \subseteq G$

$(\{0, \ldots, 9\}, +)$

$(\{0, 2, 4, 6, 8\}, +)$

$(\{0, 5\}, +)$ $\quad$ $(\{0\}, +)$

$(H, \circ)$ $\quad$ $(G, \circ)$

$\sim \subseteq G \times G$

$G = [a_1]_\sim \cup \ldots \cup [a_k]_\sim$

$|G| = \underbrace{|[a_1]_\sim|}_{\ell} + \ldots + |[a_k]_\sim|$

$\| \quad |[a_i]_\sim| = |[a_j]_\sim|$

$|H|$

$|G| = k \cdot \ell$

$(G, \circ)$ $\quad$ $(H, \circ)$

$(\mathbb{Z}_{10}, \pm)$ $\quad$ $H \subseteq G$

$(\{0, \ldots, 9\}, +)$

$(\{0, 2, 4, 6, 8\}, +)$

$(\{0, 5\}, +)$ $\quad$ $(\{0\}, +)$

$(H, \circ)$ $\quad$ $(G, \circ)$

$\sim \subseteq G \times G$

$G = [a_1]_\sim \cup \ldots \cup [a_k]_\sim$

$|G| = \underbrace{|[a_1]_\sim|}_{\ell} + \ldots + |[a_k]_\sim|$

$\| \qquad\qquad |[a_i]_\sim| = |[a_j]_\sim|$

$|H|$

$|G| = k \cdot \ell$

$(G, \circ)$ $\qquad$ $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$(\{0, 5\}, +)$

$(H, \circ)$ $\qquad$ $(G, \circ)$

$\sim \subseteq G \times G$

$G = [a_1]_\sim \cup \ldots \cup [a_k]_\sim$

$|G| = \underbrace{|[a_1]_\sim|}_{\ell} + \ldots + |[a_k]_\sim|$

$\| \qquad\qquad \|$

$|H| \qquad\qquad |[a_i]_\sim| = |[a_j]_\sim|$

$|G| = k \cdot \ell$

$(G, \circ)$ $\qquad$ $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$(\{0, 5\}, +)$

$\{0, \ldots, 9\} = \{0, 5\} \cup$

$(\{0, 2, 4, 6, 8\}, +)$

$(H, \circ)$ $\qquad$ $(G, \circ)$

$\sim \subseteq G \times G$

$G = [a_1]_\sim \cup \ldots \cup [a_k]_\sim$

$|G| = \underbrace{|[a_1]_\sim|}_{\ell} + \ldots + |[a_k]_\sim|$

$\| \qquad\qquad |[a_i]_\sim| = |[a_j]_\sim|$

$|H|$

$|G| = k \cdot \ell$

$(G, \circ)$ $\qquad$ $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$(\{0, 5\}, +)$

$\{0, \ldots, 9\} = \{0, 5\} \cup$

$(\underline{\{0, 2, 4, 6, 8\}}, +)$

$\{1, 2, 3, 5, 7\}$

$(H, \circ)$ $\qquad$ $(G, \circ)$

$\sim \subseteq G \times G$

$G = [a_1]_\sim \cup \ldots \cup [a_k]_\sim$

$|G| = \underbrace{|[a_1]_\sim|}_{\ell} + \ldots + |[a_k]_\sim|$

$\| \qquad\qquad |[a_i]_\sim| = |[a_j]_\sim|$

$|H|$

$|G| = k \cdot \ell$

$(G, \circ)$ $\qquad$ $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$(\{0, 5\}, +)$

$\{0, \ldots, 9\} = \{0, 5\} \cup$

$(\underline{\{0, 2, 4, 6, 8\}}, +)$

$\{1, 3, 5, 7, 9\}$

$(H, \circ)$ $\qquad$ $(G, \circ)$

$\sim \subseteq G \times G$

$G = [a_1]_\sim \cup \ldots \cup [a_k]_\sim$

$|G| = \underbrace{|[a_1]_\sim|}_{l} + \ldots + |[a_k]_\sim|$

$\| \qquad\qquad |[a_i]_\sim| = |[a_j]_\sim|$

$|H|$

$|G| = k \cdot l$

$(G, \circ)$ $\qquad$ $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$(\{0, 5\}, +)$

$\{0, \ldots, 9\} = \{0, 5\} \cup$

$(\{2, 4, 6, 8\}, +)$

$\{\ldots, 9\}$

$(H, \circ)$ $\qquad$ $(G, \circ)$

$\sim \subseteq G \times G$

$G = [a_1]_\sim \cup \ldots \cup [a_k]_\sim$

$|G| = \underbrace{|[a_1]_\sim|}_{l} + \ldots + |[a_k]_\sim|$

$\parallel$

$|H|$

$|[a_i]_\sim| = |[a_j]_\sim|$

$|G| = k \cdot l$

$(G, \circ)$ $\qquad$ $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$(\{0, 5\}, +)$

$\{0, \ldots, 9\} = \{0, 5\} \cup$

$(\underline{\{0, 2, 4, 6, 8\}}, +)$

$\{1, 3, 5, 7, 9\}$

$(H, \circ)$ $\qquad$ $(G, \circ)$

$\sim \subseteq G \times G$

$G = [a_1]_\sim \cup \ldots \cup [a_k]_\sim$

$|G| = \underbrace{|[a_1]_\sim|}_{\overset{\ell}{=}} + \ldots + |[a_k]_\sim|$

$|H|$ $\qquad$ $|[a_i]_\sim| = |[a_j]_\sim|$

$|G| = k \cdot \ell$

$(G, \circ)$ $\qquad$ $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$(\{0, 5\}, +)$

$\{0, \ldots, 9\} = \{0, 5\} \cup$

$(\underline{\{0, 2, 4, 6, 8\}}, +)$

$\{1, 3, 5, 7, 9\}$

$(H, \circ)$ $\qquad$ $(G, \circ)$

$a \sim b \iff b \circ a^{-1} \in H$

$(G, \circ)$ $\qquad$ $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$(\{0, 5\}, +)$

$\{0, \ldots, 9\} = \{0, 5\} \cup$

$(\underline{\{0, 2, 4, 6, 8\}}, +)$

$\{1, 3, 5, 7, 9\}$

$(H, \circ)$ $\qquad$ $(G, \circ)$

$a \sim b \iff b \circ a^{-1} \in H$

$(G, \circ)$ $\qquad$ $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$(\{0, 5\}, +)$

$\{0, \ldots, 9\} = \{0, 5\} \cup$

$(\underline{\{0, 2, 4, 6, 8\}}, +)$

$\{1, 3, 5, 7, 9\}$

$(H, \circ)$ $\qquad$ $(G, \circ)$

$a \sim b \iff b \circ a^{-1} \in H$

$[e]_\sim = \{a \in G \,/\, a \sim e$

$(G, \circ)$ $\qquad$ $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$(\{0, 5\}, +)$

$\{0, \ldots, 9\} = \{0, 5\} \cup$

$(\underline{\{0, 2, 4, 6, 8\}}, +)$

$\{1, 3, 5, 7, 9\}$

$(H, \circ)$ $\qquad$ $(G, \circ)$

$a \sim b \iff b \circ a^{-1} \in H$

$[e]_\sim = \{a \in G \,/\, e \sim a$

$a \circ e^{-1} \in H$

$(G, \circ)$ $\quad$ $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$(\{0, 5\}, +)$ $\quad$ $x \circ e = x$

$\{0, \ldots, 9\} = \{0, 5\} \cup$

$(\underline{\{0, 2, 4, 6, 8\}}, +)$

$\{1, 3, 5, 7, 9\}$

$(H, \circ)$ $\quad$ $(G, \circ)$

$a \sim b \iff b \circ a^{-1} \in H$

$[e]_\sim = \{a \in G \,/\, e \sim a$

$a \circ e^{-1} \in H$

$(G, \circ)$ $\quad$ $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$(\{0, 5\}, +)$ $\quad$ $x \circ e = x$

$\{0, \ldots, 9\} = \{0, 5\} \cup$

$$\frac{(\{0, 2, 4, 6, 8\}, +)}{\{1, 3, 5, 7, 9\}}$$

$(H, \circ)$ $\quad$ $(G, \circ)$

$a \sim b \iff b \circ a^{-1} \in H$

$$\begin{aligned}[e]_\sim &= \{a \in G \mid e \sim a\} \\ &= \{a \in G \mid a \circ e^{-1} \in H\} \\ &= \{a \in G \mid a \circ e \in H\} \\ &= \{a \in G \mid a \in H\} = H\end{aligned}$$

$\longrightarrow$ $a \sim x$ $\quad$ $x + 0^{-1}$

$(G, \circ)$ $\quad$ $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$(\{0, 5\}, +)$ $\quad$ $x \circ e = x$

$\{0, \ldots, 9\} = \{0, 5\} \cup$

$(\underline{\{0, 2, 4, 6, 8\}}, +)$

$\{1, 3, 5, 7, 9\}$

$(H, \circ)$ $\quad$ $(G, \circ)$

$a \sim b \iff b \circ a^{-1} \in H$

$[e]_\sim = \{a \in G \,/\, e \sim a\}$

$= \{a \in G \,/\, a \circ e^{-1} \in H\}$

$= \{a \in G \,/\, a \circ e \in H\}$

$= \{a \in G \,/\, a \in H\} = H$

$0 \sim x$ $\quad$ $\underset{\times G}{x + 0} \in \{0, 2, 4, 6, 8\}$

$(G, \circ)$ $\quad$ $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$(\{0, 5\}, +)$ $\quad$ $x \circ e = x$

$\{0, \ldots, 9\} = \{0, 5\} \cup$

$$\frac{(\{0, 2, 4, 6, 8\}, +)}{\{1, 3, 5, 7, 9\}}$$

$(H, \circ)$ $\quad$ $(G, \circ)$

$a \sim b \iff b \circ a^{-1} \in H$

$[e]_\sim = \{a \in G \,/\, e \sim a\}$

$= \{a \in G \,/\, a \circ e^{-1} \in H\}$

$= \{a \in G \,/\, a \circ e \in H\}$

$= \{a \in G \,/\, a \in H\} = H$

$1 \sim x$ $\quad$ $\underset{\times G}{x + 0} \in \{0, 2, 4, 6, 8\}$

$(G, \circ)$ $\quad$ $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$(\{0, 5\}, +)$ $\quad$ $x \circ e = x$

$\{0, \ldots, 9\} = \{0, 5\} \cup$

$$\frac{(\{0, 2, 4, 6, 8\}, +)}{\{1, 3, 5, 7, 9\}}$$

$(H, \circ)$ $\quad$ $(G, \circ)$

$a \sim b \iff b \circ a^{-1} \in H$

$[e]_\sim = \{a \in G \,/\, e \sim a\}$

$= \{a \in G \,/\, a \circ e^{-1} \in H\}$

$= \{a \in G \,/\, a \circ e \in H\}$

$= \{a \in G \,/\, a \in H\} = H$

$1 \sim x \quad x + 1^{-1} \in \{0, 2, 4, 6, 8\}$

$(G, \circ) \quad . \quad (H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$(\{0, 5\}, +) \qquad x \circ e = x$

$\{0, \ldots, 9\} = \{0, 5\} \cup$

$$\frac{(\{0, 2, 4, 6, 8\}, +)}{\{1, 3, 5, 7, 9\}}$$

$(H, \circ) \qquad (G, \circ)$

$a \sim b \iff b \circ a^{-1} \in H$

$[e]_\sim = \{a \in G \,/\, e \sim a\}$

$= \{a \in G \,/\, a \circ e^{-1} \in H\}$

$= \{a \in G \,/\, a \circ e \in H\}$

$= \{a \in G \,/\, a \in H\} = H$

$1 \sim x \qquad x + 1^{-1} \in \{0, 2, 4, 6, 8\}$

$(G,\circ)$ $\quad$ $(H,\circ)$

$(\{0,\dots,9\},+) = (G,\circ)$

$(\{0,5\},+)$ $\quad$ $x \circ e = x$

$\{0,\dots,9\} = \{0,5\} \cup$

$$\frac{(\{0,2,4,6,8\},+)}{\{1,3,5,7,9\}}$$

$(H,\circ)$ $\quad$ $(G,\circ)$

$a \sim b \iff b \circ a^{-1} \in H$

$$\begin{aligned}[e]_\sim &= \{a \in G \mid e \sim a\} \\ &= \{a \in G \mid a \circ e^{-1} \in H\} \\ &= \{a \in G \mid a e \in H\} \\ &= \{a \in G \mid a \in H\} = H\end{aligned}$$

$1 \sim x \quad x + 9 \in \{0,2,4,6,8\}$

$[1]_\sim = \{1,3,5,7,9\}$

$(G, \circ) \quad . \quad (H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$(\{0, 5\}, +) \qquad x \circ e = x$

$\{0, \ldots, 9\} = \{0, 5\} \cup$

$(\underline{\{0, 2, 4, 6, 8\}}, +)$

$\{1, 3, 5, 7, 9\}$

$(H, \circ) \qquad (G, \circ)$

$a \sim b \iff b \circ a^{-1} \in H$

$[e]_\sim = \{a \in G \,/\, e \sim a\}$

$= \{a \in G \,/\, a \circ e^{-1} \in H\}$

$= \{a \in G \,/\, a e \in H\}$

$= \{a \in G \,/\, a \in H\} = H$

$1 \sim x \qquad x + 9 \in \{0, 2, 4, 6, 8\}$

$[1]_\sim = \{1, 3, 5, 7, 9\}$

$(G, \circ)$ $\quad$ $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$(\{0, 5\}, +)$ $\quad$ $x \circ e = x$

$\{0, \ldots, 9\} = \{0, 5\} \cup$

$(\underline{\{0, 2, 4, 6, 8\}}, +)$

$\{1, 3, 5, 7, 9\}$

$(H, \circ)$ $\quad$ $(G, \circ)$

$a \sim b \iff b \circ a^{-1} \in H$

$3 \sim x \iff x + 7 \in \{0, 5\}$

$[0] = \{0, 2, 4, 6, 8\}$

$[2] = \{0, 2, 4, 6, 8\}$

$(G, \circ)$ $\quad$ $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$(\{0, 5\}, +)$ $\quad$ $x \circ e = x$

$\{0, \ldots, 9\} = \{0, 5\} \cup$

$(\underline{\{0, 2, 4, 6, 8\}}, +)$

$\{1, 3, 5, 7, 9\}$

$(H, \circ)$ $\quad$ $(G, \circ)$

$a \sim b \iff b \circ a^{-1} \in H$

$3 \sim x \iff x + 7 \in \{0, 5\}$

$[3] = \{3, 8\}$

$[0] = \{0, 2, 4, 6, 8\}$

$[2] = \{0, 2, 4, 6, 8\}$

$(G, \circ)$ $\quad$ $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$(\{0, 5\}, +)$ $\quad$ $x \circ e = x$

$\{0, \ldots, 9\} = \{0, 5\} \cup$

$(\underline{\{0, 2, 4, 6, 8\}}, +)$

$\{1, 3, 5, 7, 9\}$

$(H, \circ)$ $\quad$ $(G, \circ)$

$a \sim b \iff b \circ a^{-1} \in H$

$a \sim a$

$(G, \circ)$ $\quad$ $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$(\{0, 5\}, +)$ $\quad$ $x \circ e = x$

$\{0, \ldots, 9\} = \{0, 5\} \cup$

$(\underline{\{0, 2, 4, 6, 8\}}, +)$

$\{1, 3, 5, 7, 9\}$

$(H, \circ)$ $\quad$ $(G, \circ)$

$a \sim b \iff b \circ a^{-1} \in H$

$a \sim a \iff a \circ a^{-1} \in H$

$\iff e \in H$ ✓

$(G, \circ)$ $\quad . \quad (H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$(\{0, 5\}, +)$ $\quad x \circ e = x$

$\{0, \ldots, 9\} = \{0, 5\} \cup$

$(\underline{\{0, 2, 4, 6, 8\}}, +)$

$\{1, 3, 5, 7, 9\}$

$(H, \circ)$ $\qquad (G, \circ)$

$a \sim b \iff b \circ a^{-1} \in H$

$a \sim a \iff a \circ a^{-1} \in H$

$\iff e \in H$ ✓

P.d. $a \sim b \Rightarrow b \sim a$

$a \sim b \iff b \circ a^{-1} \in H$ //

P.d. $b \sim a \iff a \circ b^{-1} \in H$

$(b \circ a^{-1}) \circ (a \circ b^{-1})$

$(G, \circ)$. $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$a \sim b$ y $b \sim c \Rightarrow a \sim c$

$b \circ a^{-1} \in H$

$c \circ b^{-1} \in H$

p.d.

c

$(H, \circ)$ $(G, \circ)$

$a \sim b \Leftrightarrow b \circ a^{-1} \in H$

$a \sim a \Leftrightarrow a \circ a^{-1} \in H$

$\Leftrightarrow e \in H$ ✓

p.d. $a \sim b \Rightarrow b \sim a$

$a \sim b \Leftrightarrow b \circ a^{-1} \in H$ //

p.d. $b \sim a \Leftrightarrow a \circ b^{-1} \in H$ ✓

$(b \circ a^{-1}) \circ (a \circ b^{-1})$

$(G, \circ)$. $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$a \sim b$ y $b \sim c \Rightarrow a \sim c$

$b \circ a^{-1} \in H$

$c \circ b^{-1} \in H$

$(c \circ b^{-1}) \circ (b \circ a^{-1})$

p.d.

$c \circ a^{-1} \in H$

$(H, \circ)$ $(G, \circ)$

$a \sim b \Leftrightarrow b \circ a^{-1} \in H$

$a \sim a \Leftrightarrow a \circ a^{-1} \in H$

$\Leftrightarrow e \in H$ ✓

p.d. $a \sim b \Rightarrow b \sim a$

$a \sim b \Leftrightarrow b \circ a^{-1} \in H$ //

p.d. $b \sim a \Leftrightarrow a \circ b^{-1} \in H$ ✓

$(b \circ a^{-1}) \circ (a \circ b^{-1})$

$(G, \circ)$ $\quad$ $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$a \sim b$ y $b \sim c \Rightarrow a \sim c$

$b \circ a^{-1} \in H$

$c \circ b^{-1} \in H$

p.d. $c \circ a^{-1} \in H$

$(c \circ b^{-1}) \circ (b \circ a^{-1}) \in H \Rightarrow$

$c \circ (\underbrace{b^{-1} \circ b}_{e}) \circ a^{-1} \in H \Rightarrow$

$(c \circ e) \circ a^{-1} \in H \Rightarrow c \circ a^{-1} \in H$ //

$(H, \circ)$ $\quad$ $(G, \circ)$

$a \sim b \Leftrightarrow b \circ a^{-1} \in H$

$a \sim a \Leftrightarrow a \circ a^{-1} \in H$

$\Leftrightarrow e \in H$ ✓

p.d. $a \sim b \Rightarrow b \sim a$

$a \sim b \Leftrightarrow b \circ a^{-1} \in H$ //

p.d. $b \sim a \Leftrightarrow a \circ b^{-1} \in H$ ✓

$(b \circ a^{-1}) \circ (a \circ b^{-1})$

$(G, \circ)$. $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$a \sim b$ y $b \sim c \Rightarrow a \sim c$

p.d.

$b \circ a^{-1} \in H$

$c \circ b^{-1} \in H$

$c \circ a^{-1} \in H$

$(c \circ b^{-1}) \circ (b \circ a^{-1}) \in H \Rightarrow$

$c \circ (\underbrace{b^{-1} \circ b}_{e}) \circ a^{-1} \in H \Rightarrow$

$(c \circ e) \circ a^{-1} \in H \Rightarrow c \circ a^{-1} \in H$ //

$(H, \circ)$ $(G, \circ)$

$a \sim b \Leftrightarrow b \circ a^{-1} \in H$

$a \sim a \Leftrightarrow a \circ a^{-1} \in H$

$\Leftrightarrow e \in H$ ✓

p.d. $a \sim b \Rightarrow b \sim a$

$a \sim b \Leftrightarrow b \circ a^{-1} \in H$ //

p.d. $b \sim a \Leftrightarrow a \circ b^{-1} \in H$ ✓

$(b \circ a^{-1}) \circ (a \circ b^{-1})$

$(G, \circ)$. $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$a \sim b$ y $b \sim c \Rightarrow a \sim c$

$b \circ a^{-1} \in H$

$c \circ b^{-1} \in H$

p.d. $c \circ a^{-1} \in H$

$(c \circ b^{-1}) \circ (b \circ a^{-1}) \in H \Rightarrow$

$c \circ (\underbrace{b^{-1} \circ b}_{e}) \circ a^{-1} \in H \Rightarrow$

$(c \circ e) \circ a^{-1} \in H \Rightarrow c \circ a^{-1} \in H$ //

$(H, \circ)$ $(G, \circ)$

$a \sim b \Leftrightarrow b \circ a^{-1} \in H$

$a \sim a \Leftrightarrow a \circ a^{-1} \in H$

$\Leftrightarrow e \in H$ ✓

p.d. $a \sim b \Rightarrow b \sim a$

$a \sim b \Leftrightarrow b \circ a^{-1} \in H$ //

p.d. $b \sim a \Leftrightarrow a \circ b^{-1} \in H$ ✓

$(b \circ a^{-1}) \circ (a \circ b^{-1})$

$(G, \circ)$. $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$a \sim b$ y $b \sim c \Rightarrow a \sim c$

$b \circ a^{-1} \in H$

$c \circ b^{-1} \in H$

p.d. $c \circ a^{-1} \in H$

$(c \circ b^{-1}) \circ (b \circ a^{-1}) \in H \Rightarrow$

$c \circ (\overset{e}{b^{-1} \circ b}) \circ a^{-1} \in H \Rightarrow$

$(c \circ e) \circ a^{-1} \in H \Rightarrow c \circ a^{-1} \in H$ //

$(H, \circ)$ $(G, \circ)$

$a \sim b \Leftrightarrow b \circ a^{-1} \in H$

$a \sim a \Leftrightarrow a \circ a^{-1} \in H$

$\Leftrightarrow e \in H$ ✓

p.d. $a \sim b \Rightarrow b \sim a$

$a \sim b \Leftrightarrow b \circ a^{-1} \in H$ //

p.d. $b \sim a \Leftrightarrow a \circ b^{-1} \in H$ ✓

$(b \circ a^{-1}) \circ (a \circ b^{-1})$

$(G, \circ)$ $\quad$ $(H, \circ)$

$(\{0, \ldots, 9\}, +) = (G, \circ)$

$a \sim b$ y $b \sim c \Rightarrow a \sim c$

$b \circ a^{-1} \in H$

$c \circ b^{-1} \in H$

p.d. $c \circ a^{-1} \in H$

$(c \circ b^{-1}) \circ (b \circ a^{-1}) \in H \Rightarrow$

$c \circ (\underbrace{b^{-1} \circ b}_{e}) \circ a^{-1} \in H \Rightarrow$

$(c \circ e) \circ a^{-1} \in H \Rightarrow c \circ a^{-1} \in H$ //

$(H, \circ)$ $\quad$ $(G, \circ)$

$a \sim b \Leftrightarrow b \circ a^{-1} \in H$

$a \sim a \Leftrightarrow a \circ a^{-1} \in H$

$\Leftrightarrow e \in H$ ✓

p.d. $a \sim b \Rightarrow b \sim a$

$a \sim b \Leftrightarrow b \circ a^{-1} \in H$ //

p.d. $b \sim a \Leftrightarrow a \circ b^{-1} \in H$ ✓

$(b \circ a^{-1}) \circ (a \circ b^{-1})$

$(G, \circ)$ $\quad$ $(H, \circ)$

n $\quad$ $a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$(H, \circ)$ $\quad$ $(G, \circ)$

$a \sim b \iff b \circ a^{-1} \in H$

$a \sim a \iff a \circ a^{-1} \in H$

$\iff e \in H$ ✓

P.d. $a \sim b \Rightarrow b \sim a$

$a \sim b \iff b \circ a^{-1} \in H$ //

P.d. $b \sim a \iff a \circ b^{-1} \in H$ ✓

$(b \circ a^{-1}) \circ (a \circ b^{-1})$

$(G, \circ)$ $\quad$ $(H, \circ)$

(n) $\quad a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$(H, \circ)$ $\quad$ $(G, \circ)$

$a \sim b \iff b \circ a^{-1} \in H$

$a \sim a \iff a \circ a^{-1} \in H$

$\iff e \in H$ ✓

P.d. $a \sim b \Rightarrow b \sim a$

$a \sim b \iff b \circ a^{-1} \in H$ //

P.d. $b \sim a \iff a \circ b^{-1} \in H$ ✓

$(b \circ a^{-1}) \circ (a \circ b^{-1})$

$(G, \circ)$ $\quad$ $(H, \circ)$

(n) $\quad a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$(H, \circ)$ $\quad$ $(G, \circ)$

$a \sim b \iff b \circ a^{-1} \in H$

$a \sim a \iff a \circ a^{-1} \in H$

$\iff e \in H$ ✓

P.d. $a \sim b \Rightarrow b \sim a$

$a \sim b \iff b \circ a^{-1} \in H$ //

P.d. $b \sim a \iff a \circ b^{-1} \in H$ ✓

$(b \circ a^{-1}) \circ (a \circ b^{-1})$

$(G, \circ)$ $\quad$ $(H, \circ)$

n $\quad$ $a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|}$

$(H, \circ)$ $\quad$ $(G, \circ)$

$a \sim b \iff b \circ a^{-1} \in H$

$a \sim a \iff a \circ a^{-1} \in H$

$\iff e \in H$ ✓

P.d. $a \sim b \Rightarrow b \sim a$

$a \sim b \iff b \circ a^{-1} \in H$ //

$\sim a \iff a \circ b^{-1} \in H$ ✓

$(b \circ a^{-1}) \circ (a \circ b^{-1})$

$(G, \circ)$ $\quad$ $(H, \circ)$

n $\quad$ $a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(H, \circ)$ $\quad$ $(G, \circ)$

$a \sim b \iff b \circ a^{-1} \in H$

$a \sim a \iff a \circ a^{-1} \in H$

$\iff e \in H$ ✓

P.d. $a \sim b \Rightarrow b \sim a$

$a \sim b \iff b \circ a^{-1} \in H$ //

$\sim a \iff a \circ b^{-1} \in H$ ✓

$(b \circ a^{-1}) \circ (a \circ b^{-1})$

$(G, \circ)$ $\quad (H, \circ)$

n $\quad a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$

$a \sim a \iff a \circ a^{-1} \in H$

$\iff e \in H$ ✓

P.d. $a \sim b \Rightarrow b \sim a$

$a \sim b \iff b \circ a^{-1} \in H$ //

$\sim a \iff a \circ b^{-1} \in H$ ✓

$(b \circ a^{-1}) \circ (a \circ b^{-1})$

$(G, \circ)$ $\quad$ $(H, \circ)$

n $\quad$ $a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$

$(J_n, \cdot)$

$a \sim a \iff a \circ a^{-1} \in H$

$\iff e \in H$ ✓

P.d. $a \sim b \Rightarrow b \sim a$

$a \sim b \iff b \circ a^{-1} \in H$ //

$\sim a \iff a \circ b^{-1} \in H$ ✓

$(b \circ a^{-1}) \circ (a \circ b^{-1})$

$(G, \circ)$ $\quad$ $(H, \circ)$

n $\quad$ $a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $\quad$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$

$a \sim a \iff a \circ a^{-1} \in H$

$\iff e \in H$ ✓

P.d. $a \sim b \Rightarrow b \sim a$

$a \sim b \iff b \circ a^{-1} \in H$ //

$\sim a \iff a \circ b^{-1} \in H$ ✓

$(b \circ a^{-1}) \circ (a \circ b^{-1})$

$(G, \circ)$ $(H, \circ)$

n $a \in \{1, \ldots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \ldots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$

$\mathbb{Z}_8^* =$

$(G, \circ)$ $(H, \circ)$

n $a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$(G, \circ)$ $(H, \circ)$

n $a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$J_8 = \{$

$a^7 \bmod 8 = 1$

$(G, \circ)$ $(H, \circ)$

n $a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$J_8 = \{1$

$a^7 \bmod 8 = 1$

$7^7 \bmod 8 = (-1)^7 \bmod 8$

$= -1 \bmod 8$

$= 7$

$(G, \circ)$ $(H, \circ)$

n $a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$J_8 = \{1$

$a^7 \bmod 8 = 1$

$7^7 \bmod 8 = (-1)^7 \bmod 8$

$= -1 \bmod 8$

$= 7$

$(G, \circ)$ $(H, \circ)$

n $a \in \{1, \ldots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \ldots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$J_8 = \{1$

$a^7 \bmod 8 = 1$

$7^7 \bmod 8 = (-1)^7 \bmod 8$

$= -1 \bmod 8$

$= 7$

$(G, \circ)$ $(H, \circ)$

n $a \in \{1, \ldots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \ldots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$J_8 = \{1$

$a^7 \bmod 8 = 1$

$7^7 \bmod 8 = (-1)^7 \bmod 8$

$= -1 \bmod 8$

$= 7$

$3^7 \bmod 8$

$(G, \circ)$ $(H, \circ)$

n $a \in \{1, \ldots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \ldots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$J_8 = \{1$

$a^7 \bmod 8 = 1$

$(a^2 \cdot a^2 \cdot a^2 \cdot a) \bmod 8$

$1 \quad 1 \quad 1$

$(G, \circ)$ $\quad$ $(H, \circ)$

n $\quad$ $a \in \{1, \ldots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \ldots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $\quad$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$ $\quad$ $\frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$J_8 = \{1\}$

$a^7 \bmod 8 = 1$

$(a^2 \cdot a^2 \cdot a^2 \cdot a) \bmod 8$

$1 \quad 1 \quad 1$

$(G, \circ)$ $\quad$ $(H, \circ)$

n $\quad$ $a \in \{1, \ldots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \ldots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $\quad$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$ $\quad$ $\frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$J_8 = \{1\}$ $\quad$ $\cancel{A}$

$a^7 \bmod 8 = 1$

$(a^2 \cdot a^2 \cdot a^2 \cdot a) \bmod 8$

$1 \quad 1 \quad 1$

$(G, \circ)$ $(H, \circ)$

n $a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$ $\frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$J_8 = \{1\}$ $\cancel{\times}$

$a^7 \bmod 8 = 1$

$(a^2 \cdot a^2 \cdot a^2 \cdot a) \bmod 8$

$1 \quad 1 \quad 1$

$(G, \circ)$ $(H, \circ)$

n $a \in \{1, \ldots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \ldots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$ $\frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$J_8 = \{1\}$ $\cancel{\mathbb{Z}}$

$a^7 \bmod 8 = 1$

$(a^2 \cdot a^2 \cdot a^2 \cdot a) \bmod 8$

$1 \quad 1 \quad 1$

$(G, \circ)$ $(H, \circ)$

n $a \in \{1, \ldots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \ldots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$ $\frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$J_8 = \{1\}$

$a^7 \bmod 8 = 1$

$(a^2 \cdot a^2 \cdot a^2 \cdot a) \bmod 8$

$1 \quad 1 \quad 1$

$(G, \circ)$ $\quad$ $(H, \circ)$

n $\quad$ $a \in \{1, \ldots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \ldots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $\quad$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$ $\quad$ $\frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$J_8 = \{1\}$ $\quad$ $\cancel{\mathbb{Z}}$

561

$a^7 \bmod 8 = 1$

$(a^2 \cdot a^2 \cdot a^2 \cdot a) \bmod 8$

$1 \quad 1 \quad 1$

$(G, \circ)$ $(H, \circ)$

n $a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{errore}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$ $\frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$J_8 = \{1\}$

561

$561 = 3 \cdot 187$

$= \boxed{3 \cdot 11 \cdot 17}$

$(G, \circ)$ $(H, \circ)$

n $a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$ $\frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$J_8 = \{1\}$

561

$561 = 3 \cdot 187$

$= \boxed{3 \cdot 11 \cdot 17}$

$(G, \circ)$ $\quad$ $(H, \circ)$

n $\quad$ $a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{errore}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $\quad$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$ $\quad$ $\frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$J_8 = \{1\}$ $\quad$ $\cancel{\mathbb{Z}}$

561

$561 = 3 \cdot 187$

$= \boxed{3 \cdot 11 \cdot 17}$

$(G, \circ)$ $\quad$ $(H, \circ)$

n $\quad$ $a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{errore}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $\quad$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$ $\quad$ $\frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$J_8 = \{1\}$ $\quad$ $\cancel{\mathbb{Z}}$

561

$561 = 3 \cdot 187$

$= \boxed{3 \cdot 11 \cdot 17}$

$(G, \circ)$ $(H, \circ)$

n $a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$ $\frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$J_8 = \{1\}$

561

$561 = 3 \cdot 187$

$= \boxed{3 \cdot 11 \cdot 17}$

$(G, \circ)$ $\quad$ $(H, \circ)$

n $\quad$ $a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{errore}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $\quad$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$ $\quad$ $\frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$J_8 = \{1\}$

561

$561 = 3 \cdot 187$

$= \boxed{3 \cdot 11 \cdot 17}$

$(G, \circ)$ $(H, \circ)$

n $a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{errore}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$ $\frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$J_8 = \{1\}$

561

$561 = 3 \cdot 187$

$= \boxed{3 \cdot 11 \cdot 17}$

$(G, \circ)$ $(H, \circ)$

n $a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{errore}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$ $\frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$J_8 = \{1\}$

561

$561 = 3 \cdot 187$

$= \boxed{3 \cdot 11 \cdot 17}$

$(G, \circ)$ $\quad$ $(H, \circ)$

n $\quad$ $a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{errore}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $\quad$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$ $\quad$ $\frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$J_8 = \{1\}$ $\quad$ $\cancel{\mathbb{Z}}$

561

$561 = 3 \cdot 187$

$= \boxed{3 \cdot 11 \cdot 17}$

$a^{\frac{n-1}{2}} \bmod n$

$(G, \circ)$ $\quad$ $(H, \circ)$

n $\quad$ $a \in \{1, \ldots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \ldots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $\quad$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$ $\quad$ $\frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$b^2 \equiv a \bmod n$

$\bmod 7$

$\cancel{\mathbb{Z}}$

561

$a^{\frac{n-1}{2}} \bmod n$

$(G, \circ)$ $\quad$ $(H, \circ)$

n $\quad$ $a \in \{1, \ldots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \ldots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{errore}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $\quad$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$ $\quad$ $\frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$b^2 \equiv a \bmod n$

$3^2 \equiv 2 \bmod 7$

$\cancel{A}$

561

$a^{\frac{n-1}{2}} \bmod n$

$(G, \circ)$ $\quad$ $(H, \circ)$

n $\quad$ $a \in \{1, \ldots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \ldots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $\quad$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$ $\quad$ $\frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$b^2 \equiv a \bmod n$

$3^2 \equiv 2 \bmod 7$

$\cancel{\mathbb{Z}}$

561

$a^{n-1} \bmod n$

$(G, \circ)$ $(H, \circ)$

n $a \in \{1, \ldots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \ldots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$ $\frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$b^2 \equiv a \bmod n$

$3^2 \equiv 2 \bmod 7$

561

$a^{n-1} \bmod n$

$(G, \circ)$ $(H, \circ)$

n $a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$ $\frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$b^2 \equiv a \bmod n$ $\cancel{A}$

$3^2 \equiv 2 \bmod 7$ 561

$x^2 \equiv 1 \bmod 7$ $a^{n-1} \bmod n$

$(G, \circ)$ $(H, \circ)$

n $a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$ $\frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$b^2 \equiv a \bmod n$ $\cancel{A}$

$3^2 \equiv 2 \bmod 7$ 561

$x^2 \equiv 1 \bmod 7$ $a^{n-1} \bmod n$

$(G, \circ)$ $(H, \circ)$

n $a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$ $\frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$b^2 \equiv a \bmod n$ $\cancel{A}$

$3^2 \equiv 2 \bmod 7$ 561

$x^2 \equiv 1 \bmod 7$ $a^{n-1} \bmod n$

$(G, \circ)$ $(H, \circ)$

n $a \in \{1, \dots, n-1\}$

$a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} / MCD(a, n) = 1\}$

$J_n = \{a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1\}$

$|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$Pr(\text{error}) = \frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$(\mathbb{Z}_n^*, \cdot)$ $|J_n| \mid |\mathbb{Z}_n^*|$

$(J_n, \cdot)$ $\frac{|J_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, \cdot)$

$b^2 \equiv a \bmod n$ $\cancel{A}$

$3^2 \equiv 2 \bmod 7$ 561

$x^2 \equiv 1 \bmod 7$ $a^{n-1} \bmod n$