$a, b \in \mathbb{Z}$

$7 = 2 \cdot 3 + 1$ $\qquad$ $7 = 1 \cdot 3 + 4$

$a, b \in \mathbb{Z}$

$7 = 2 \cdot 3 + 1$ $\qquad$ $7 = 1 \cdot 3 + 4$

$a = \alpha \cdot b + \beta$ $\qquad$ $0 \leq \beta < b$

$-8 = \alpha \cdot 3 + \beta$ $\qquad$ $0 \leq \beta < 3$

$= (-3) \cdot 3 + 1$

$= (-2) \cdot 3 \cancel{+ 1}$

$0 \leq \beta < |b|$

$-8 = 3 \cdot (-3) + 1$

$0 \leq 1 < |-3|$

$7 = 1 \cdot 3 + 4$

$a = \alpha \cdot b + \beta$

$0 \leq \beta < b$

$-8 = \alpha \cdot 3 + \beta$

$0 \leq \beta < 3$

$= (-3) 3 + 1$

$= (-2) \cdot \cancel{3 + (-2)}$

$0 \le \beta < |b|$

$-8 = 3 \cdot (-3) + 1$

$0 \le 1 < |-3|$

$7 = 1 \cdot 3 + 4$

$a = \alpha \cdot b + \beta$

$0 \le \beta < b$

$-8 = \alpha \cdot 3 + \beta$

$0 \le \beta < 3$

$= (-3) 3 + 1$

$b \equiv c \mod n$

$= (-2) \cdot \cancel{3 + (-2)}$

$0 \le \beta < |b|$

$-8 = 3 \cdot (-3) + 1$

$0 \le 1 < |-3|$

$7 = 1 \cdot 3 + 4$

$n \mid b - c$

$a = \alpha \cdot b + \beta$

$0 \le \beta < b$

$7 \equiv 2 \mod 5$

$-8 = \alpha \cdot 3 + \beta$

$0 \le \beta < 3$

$= (-3) \cdot 3 + 1$

$b \equiv c \mod n$

$= (-2) \cdot \cancel{3 + (-2)}$

$0 \le \beta < |b|$

$-8 = 3 \cdot (-3) + 1$

$0 \le 1 < |-3|$

$7 = 1 \cdot 3 + 4$

$n \mid b - c$

$a = \alpha \cdot b + \beta$

$0 \le \beta < b$

$7 \equiv 2 \mod 5$

$-8 = \alpha \cdot 3 + \beta$

$0 \le \beta < 3$

$1 + 7 \equiv 1 + 2 \mod 5$

$= (-3) 3 + 1$

$b \equiv c \mod n$

$= (-2) \cdot \cancel{3 + (-2)}$

$-8 = 3\cdot(-3) + 1$

$0 \le 1 < |-3|$

$0 \le \beta < |b|$

$7 = 1\cdot 3 + 4$

$n \mid b - c$

$a = \alpha \cdot b + \beta$

$0 \le \beta < b$

$7 \equiv 2 \mod 5$

$-8 = \alpha \cdot 3 + \beta$

$0 \le \beta < 3$

$1 + 7 \equiv 1 + 2 \mod 5$

$= (-3)\,3 + 1$

$b \equiv c \mod n$

$a \equiv (a \bmod n) \bmod n$

$= (-2)\cdot \cancel{3 + (-2)}$

$-8 = 3\cdot(-3) + 1$

$0 \le 1 < |-3|$

$0 \le \beta < |b|$

$7 = 1\cdot 3 + 4$

$n \mid b - c$

$a = \alpha \cdot b + \beta$

$0 \le \beta < b$

$7 \equiv 2 \mod 5$

$-8 = \alpha \cdot 3 + \beta$

$0 \le \beta < 3$

$1 + 7 \equiv 1 + 2 \mod 5$

$= (-3)\,3 + 1$

$b \equiv c \mod n$

$a \equiv (a \bmod n) \bmod n$

$= (-2)\cdot \cancel{3 + (-2)}$

a^b

$0 \leq \beta < |b|$

$7 = 1 \cdot 3 + 4$

$0 \leq \beta < b$

$0 \leq \beta < 3$

$b \equiv c \mod n$

a^b

a^{100}

$t = a^{50}$

$t \cdot t$

$0 \leq \beta < |b|$

$7 = 1 \cdot 3 + 4$

$0 \leq \beta < b$

$0 \leq \beta < 3$

$b \equiv c \mod n$

a^b

a^{100}

$t = a^{50}$

$t \cdot t$

$a^b \bmod n$

$0 \le \beta < |b|$

$7 = 1 \cdot 3 + 4$

$0 \le \beta < b$

$0 \le \beta < 3$

$b \equiv c \bmod n$

a^b

a^{100}

$t = a^{50}$

$t \cdot t$

$a^b \bmod n$

$0 \le \beta < |b|$

$7 = 1 \cdot 3 + 4$

$0 \le \beta < b$

$0 \le \beta < 3$

$b \equiv c \bmod n$

a^b

a^{100}

$a^b \bmod n$

$a^{100} \bmod n$

$t = a^{50}$; $t = a^{50} \bmod n$

$t \cdot t$ $\quad$ $t \cdot t \bmod n$

$0 \le \beta < |b|$

$7 = 1 \cdot 3 + 4$

$0 \le \beta < b$

$0 \le \beta < 3$

$b \equiv c \bmod n$

a^b

a^{100}

$a^b \bmod n$

$a^{100} \bmod n$

$t = a^{50}$; $t = a^{50} \bmod n$

$t \cdot t$ $\quad$ $t \cdot t \bmod n$

$0 \le \beta < |b|$

$7 = 1 \cdot 3 + 4$

$0 \le \beta < b$

$0 \le \beta < 3$

$\equiv c \bmod n$

a^b

a^{100}

$a^b \bmod n$

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

$a^{100} \bmod n$

$t = a^{50}$; $t = a^{50} \bmod n$

$t \cdot t$ $\quad$ $t \cdot t \bmod n$

$0 \leq \beta < |b|$

$7 = 1 \cdot 3 + 4$

$0 \leq \beta < b$

$0 \leq \beta < 3$

$b \equiv c \bmod n$

a^b

a^{100}

$a^b \bmod n$

$a^{100} \bmod n$

$t = a^{50}$

$t \cdot t$

$t = a^{50} \bmod n$

$t \cdot t \bmod n$

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

$0 \leq \beta < |b|$

$7 = 1 \cdot 3 + 4$

$0 \leq \beta < b$

$0 \leq \beta < 3$

$b \equiv c \bmod n$

a^b

a^{100}

$a^b \bmod n$

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

$a^{100} \bmod n$

$t = a^{50}$; $t = a^{50} \bmod n$

$t \cdot t$ $\quad$ $t \cdot t \bmod n$

$0 \leq \beta < |b|$

$7 = 1 \cdot 3 + 4$

$0 \leq \beta < b$

$0 \leq \beta < 3$

$b \equiv c \bmod n$

a^b

a^{100}

$a^b \bmod n$

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

$a^{100} \bmod n$

$t = a^{50}$; $t = a^{50} \bmod n$

$t \cdot t$ $\quad$ $t \cdot t \bmod n$

$0 \leq \beta < |b|$

$7 = 1 \cdot 3 + 4$

$0 \leq \beta < b$

$0 \leq \beta < 3$

$b \equiv c \bmod n$

a^b

a^{100}

$a^b \bmod n$

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

$a^{100} \bmod n$

$t = a^{50}$; $t = a^{50} \bmod n$

$t \cdot t$ $\quad$ $t \cdot t \bmod n$

$0 \leq \beta < |b|$

$7 = 1 \cdot 3 + 4$

$0 \leq \beta < b$

$0 \leq \beta < 3$

$b \equiv c \bmod n$

a^b

a^{100}

$a^b \bmod n$

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

$a^{100} \bmod n$

$t = a^{50}$; $t = a^{50} \bmod n$

$t \cdot t$ $\quad$ $t \cdot t \bmod n$

$0 \leq \beta < |b|$

$7 = 1 \cdot 3 + 4$

$0 \leq \beta < b$

$0 \leq \beta < 3$

$b \equiv c \bmod n$

a^b

a^{100}

$a^b \bmod n$

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

$a^{100} \bmod n$

$t = a^{50}$

$t \cdot t$

$t = a^{50} \bmod n$

$t \cdot t \bmod n$

$0 \leq \beta < |b|$

$7 = 1 \cdot 3 + 4$

$0 \leq \beta < b$

$0 \leq \beta < 3$

$b \equiv c \bmod n$

a^b

a^{100}

$a^b \bmod n$

$T(b)$

$a^{100} \bmod n$

$t = a^{50}$; $t = a^{50} \bmod n$

$t \cdot t$ $\quad$ $t \cdot t \bmod n$

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

$0 \le \beta < |b|$

$7 = 1 \cdot 3 + 4$

$0 \le \beta < b$

$0 \le \beta < 3$

$b \equiv c \bmod n$

a^b

a^{100}

$a^b \bmod n$

$T(b) = T(\lfloor \frac{b}{2} \rfloor) + c$

$a^{100} \bmod n$

$t = a^{50}$; $t = a^{50} \bmod n$

$t \cdot t$ $\quad$ $t \cdot t \bmod n$

n

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

$0 \le \beta < |b|$

$7 = 1 \cdot 3 + 4$

$0 \le \beta < b$

$0 \le \beta < 3$

$b \equiv c \bmod n$

a^b

a^{100}

$a^b \bmod n$

$T(b) = T(\lfloor \frac{b}{2} \rfloor) + c$

$a^{100} \bmod n$

$t = a^{50}$

$t \cdot t$

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

$t = a^{50} \bmod n$

$t \cdot t \bmod n$

n

$\log_2 n$

$0 \le \beta < |b|$

$7 = 1 \cdot 3 + 4$

$0 \le \beta < b$

$0 \le \beta < 3$

$b \equiv c \bmod n$

a^b

a^{100}

$a^b \bmod n$

$T(b) = T(\lfloor \frac{b}{2} \rfloor) + c$

$a^{100} \bmod n$

$t = a^{50}$

$t \cdot t$

$t = a^{50} \bmod n$

$t \cdot t \bmod n$

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

n

$\log_2 b$

$O(b) \geq 1$

$0 \leq \beta < |b|$

$7 = 1 \cdot 3 + 4$

$0 \leq \beta < b$

$0 \leq \beta < 3$

$b \equiv c \bmod n$

a^b

a

a^{100}

$12 = 2^2 \cdot 3$

$a^b \bmod n$

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

$T(b) = T\left(\left\lfloor \frac{b}{2} \right\rfloor\right) + c$

a^b

a^{100}

$a^b \bmod n$

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

$T(b) = T\left(\left\lfloor \frac{b}{2} \right\rfloor\right) + c$

a

$10 = 2 \cdot 5 = 2^1 \cdot 3^0 \cdot 5^1$

$12 = 2^2 \cdot 3 = 2^2 \cdot 3^1 \cdot 5^0$

$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}$

$b = p_1^{\beta_1} \cdots p_\ell^{\beta_\ell}$

$MCD(a,b) = p_1^{\min(\alpha_1,\beta_1)}$

a^b

a^{100}

$a^b \bmod n$

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

$T(b) = T\left(\left\lfloor \frac{b}{2} \right\rfloor\right) + c$

a

$2 \leftarrow \begin{cases} 10 = 2 \cdot 5 = 2^1 \cdot 3^0 \cdot 5^1 \\ 12 = 2^2 \cdot 3 = 2^2 \cdot 3^1 \cdot 5^0 \end{cases}$

$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}$

$b = p_1^{\beta_1} \cdots p_\ell^{\beta_\ell}$

$MCD(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdots p_\ell^{\min(\alpha_\ell,\beta_\ell)}$

a^b

a^{100}

$a^b \bmod n$

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

$T(b) = T\left(\left\lfloor \frac{b}{2} \right\rfloor\right) + c$

a

$N = P \cdot Q$

$2 \leftarrow \begin{cases} 10 = 2 \cdot 5 = 2^1 \cdot 3^0 \cdot 5^1 \\ 12 = 2^2 \cdot 3 = 2^2 \cdot 3^1 \cdot 5^0 \end{cases}$

$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}$

$b = p_1^{\beta_1} \cdots p_\ell^{\beta_\ell}$

$MCD(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdots p_\ell^{\min(\alpha_\ell,\beta_\ell)}$

a^b

a

$10 = 2 \cdot 5 = 2^1 \cdot 3^0 \cdot 5^1$

$2 \leftarrow$

$12 = 2^2 \cdot 3 = 2^2 \cdot 3^1 \cdot 5^0$

a^{100}

$N = P \cdot Q$

$100 = 25 \cdot 4$

$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}$

$a^b \bmod n$

$b = p_1^{\beta_1} \cdots p_\ell^{\beta_\ell}$

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

$MCD(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdots p_\ell^{\min(\alpha_\ell,\beta_\ell)}$

$T(b) = T\left(\left\lfloor \frac{b}{2} \right\rfloor\right) + c$

a^b

a

$10 = 2 \cdot 5 = 2^1 \cdot 3^0 \cdot 5^1$

$2 \leftarrow$

$12 = 2^2 \cdot 3 = 2^2 \cdot 3^1 \cdot 5^0$

a^{100}

$N = P \cdot Q$

$a^b \bmod n$

$100 = 25 \cdot 4$

$\quad\quad\;\; \| \quad\;\; \|$

$5 \cdot 5 \quad 2 \cdot 2$

$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}$

$b = p_1^{\beta_1} \cdots\cdots p_\ell^{\beta_\ell}$

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

$T(b) = T\left(\left\lfloor \frac{b}{2} \right\rfloor\right) + c$

$MCD(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdots\cdots p_\ell^{\min(\alpha_\ell,\beta_\ell)}$

a^b

a^{100}

$a^b \bmod n$

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

$T(b) = T\left(\left\lfloor \frac{b}{2} \right\rfloor\right) + c$

a

$N = P \cdot Q$

$100 = 25 \cdot 4$

$\quad\;\; \| \qquad \|$

$\quad 5 \cdot 5 \quad 2 \cdot 2$

$10 = 2 \cdot 5 = 2^1 \cdot 3^0 \cdot 5^1$

$2 \leftarrow$

$12 = 2^2 \cdot 3 = 2^2 \cdot 3^1 \cdot 5^0$

$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}$

$b = p_1^{\beta_1} \cdots p_\ell^{\beta_\ell}$

$MCD(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdots p_\ell^{\min(\alpha_\ell,\beta_\ell)}$

a^b

a^{100}

$a^b \bmod n$

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

$T(b) = T(\lfloor \frac{b}{2} \rfloor) + c$

$MCD(a,b) = MCD(a-b, b)$

$a > b$

$MCD(12, 10) = MCD(\underset{2}{12-10}, 10)$

e)

a^b

a^{100}

$a^b \bmod n$

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

$T(b) = T\left(\left\lfloor \frac{b}{2} \right\rfloor\right) + c$

$MCD(a,b) = MCD(a-b, b)$

$a > b$

$MCD(12, 10) = MCD(\underset{2}{12-10}, 10)$

e)

a^b

$MCD(a,b) = MCD(b, a \bmod b)$,

a^{100}

$a^b \bmod n$

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

$T(b) = T(\lfloor \frac{b}{2} \rfloor) + c$

2)

a^b

a^{100}

$a^b \bmod n$

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

$T(b) = T\left(\left\lfloor \frac{b}{2} \right\rfloor\right) + c$

$MCD(a,b) = MCD(b, a \bmod b)$

$MCD(10,12) = MCD(12, 10 \bmod 12)$

$= MCD(12, 10)$

$= MCD(10, 12 \bmod 10)$

$= MCD(10, 2)$

a^b

a^{100}

$a^b \bmod n$

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

$T(b) = T(\lfloor \frac{b}{2} \rfloor) + c$

$MCD(a,b) = MCD(b, a \bmod b)$,

$MCD(10,12) = MCD(12, 10 \bmod 12)$

$= MCD(12, 10)$

$= MCD(10, 12 \bmod 10)$

$= MCD(10, 2)$

$= MCD(2, 10 \bmod 2)$

$= MCD(2, 0) = 2$

$x > 0$

$MCD(x, 0) = x$

e)

a^b

a^{100}

$a^b \bmod n$

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

$T(b) = T(\lfloor \frac{b}{2} \rfloor) + c$

$a > b$

$MCD(a,b) = MCD(b, a \bmod b)$,

$MCD(10,12) = MCD(12, 10 \bmod 12)$

$= MCD(12, 10)$

$= MCD(10, 12 \bmod 10)$

$= MCD(10, 2)$

$= MCD(2, 10 \bmod 2)$

$= MCD(2, 0) = 2$

$x > 0$

$MCD(x, 0) = x$

e)

a^b

a^{100}

$a^b \bmod n$

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

$T(b) = T\left(\left\lfloor \frac{b}{2} \right\rfloor\right) + c$

$MCD(a,b) = MCD(b, a \bmod b)$

$a > b$

a^b

a^{100}

$a^b \bmod n$

$$MCD(a,b) = MCD(b, a \bmod b),$$
$$a > b$$

$$\boxed{a \bmod b \leq \frac{a}{2}}$$

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

$$T(b) = T\left(\left\lfloor \frac{b}{2} \right\rfloor\right) + c$$

a^b

a^{100}

$a^b \bmod n$

$$MCD(a,b) = MCD(b, a \bmod b),$$

$a \geq b$

$$\boxed{a \bmod b < \frac{a}{2}}$$

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

$$T(b) = T\left(\left\lfloor \frac{b}{2} \right\rfloor\right) + c$$

a^b

a^{100}

$a^b \bmod n$

$a^{\frac{b-1}{2}}$

$T(b) = T(\lfloor \frac{b}{2} \rfloor) + c$

$MCD(a,b) = MCD(b, a \bmod b)$,

$a \geq b > 0$

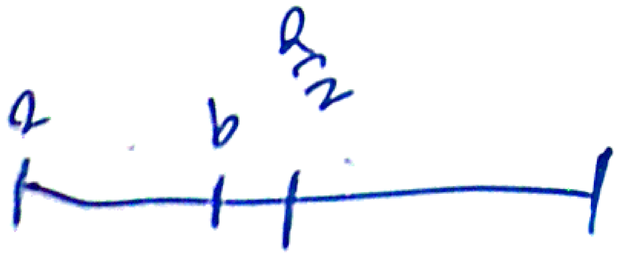
$$\boxed{a \bmod b < \frac{a}{2}}$$

$b = \frac{a}{2}$ $\quad a \bmod b = 0 < \frac{a}{2}$

$b < \frac{a}{2}$ $\quad a \bmod b$.

$$MCD(a,b) = MCD(b, a \bmod b)$$

$a \geq b > 0$



$$\boxed{a \bmod b < \frac{a}{2}}$$

$$T(b) = T\left(\left\lfloor \frac{b}{2} \right\rfloor\right) +$$

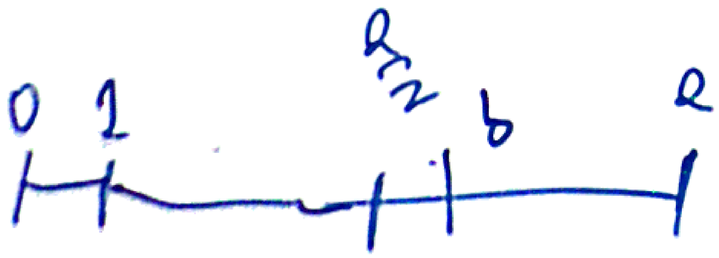
$b = \frac{a}{2}$ $\quad a \bmod b = 0 \leq \frac{a}{2}$

$b < \frac{a}{2}$ $\quad a \bmod b < b < \frac{a}{2}$ //

$b > \frac{a}{2}$ $\quad a \bmod b$

$$MCD(a,b) = MCD(b, a \bmod b)$$

$a \geq b > 0$



$$\boxed{a \bmod b < \frac{a}{2}}$$

$$T(b) = T\left(\left\lfloor \frac{b}{2} \right\rfloor\right) + \ldots$$

$b = \frac{a}{2}$ $\quad a \bmod b = 0 \leq \frac{a}{2}$

$b < \frac{a}{2}$ $\quad a \bmod b < b < \frac{a}{2}$ //

$b > \frac{a}{2}$ $\quad a \bmod b$

$$MCD(a,b) = MCD(b, a \bmod b),$$

$$a \geq b > 0$$

$$\boxed{a \bmod b < \frac{a}{2}}$$

$b = \frac{a}{2}$ $\quad a \bmod b = 0 < \frac{a}{2}$

$b < \frac{a}{2}$ $\quad a \bmod b < b < \frac{a}{2}$ //

$b > \frac{a}{2}$ $\quad a \bmod b$

$$MCD(a,b) = MCD(b, a \bmod b),$$

$$a \geq b > 0$$

$$\boxed{a \bmod b < \frac{a}{2}}$$

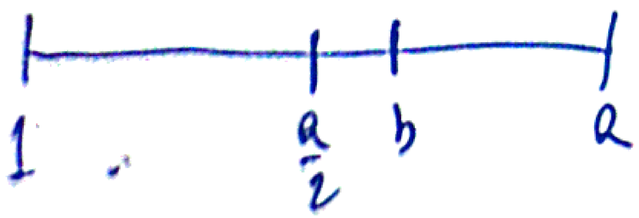
$b = \frac{a}{2}$ $\quad a \bmod b = 0 < \frac{a}{2}$

$b < \frac{a}{2}$ $\quad a \bmod b < b < \frac{a}{2}$ //

$b > \frac{a}{2}$ $\quad a \bmod b = a - b$

$$MCD(a,b) = MCD(b, a \bmod b),$$

$$a \geq b > 0$$



$$\boxed{a \bmod b < \frac{a}{2}}$$

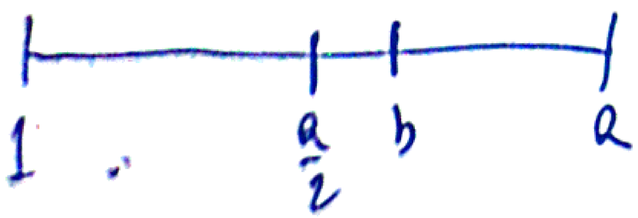
$b = \frac{a}{2}$ $\quad a \bmod b = 0 < \frac{a}{2}$

$b < \frac{a}{2}$ $\quad a \bmod b < b < \frac{a}{2}$ //

$b > \frac{a}{2}$ $\quad a \bmod b = a - b < a - \frac{a}{2} = \frac{a}{2}$

$$MCD(a,b) = MCD(b, a \bmod b)$$

$$a \geq b > 0$$



$$\boxed{a \bmod b < \frac{a}{2}}$$

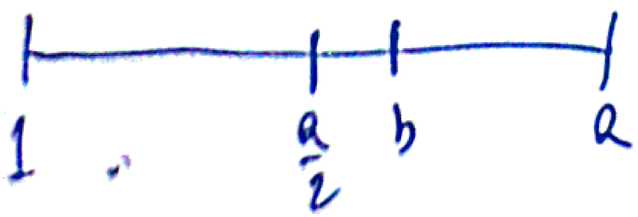
$b = \frac{a}{2}$ $\quad a \bmod b = 0 < \frac{a}{2}$

$b < \frac{a}{2}$ $\quad a \bmod b < b < \frac{a}{2}$ //

$b > \frac{a}{2}$ $\quad a \bmod b = a - b < a - \frac{a}{2} = \frac{a}{2}$

$$MCD(a,b) = MCD(b, a \bmod b)$$

$a \geq b > 0$



$$\boxed{a \bmod b < \frac{a}{2}}$$

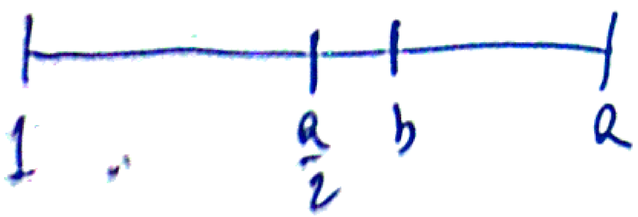
$b = \frac{a}{2}$ $\quad a \bmod b = 0 < \frac{a}{2}$

$b < \frac{a}{2}$ $\quad a \bmod b < b < \frac{a}{2}$

$b > \frac{a}{2}$ $\quad a \bmod b = a - b < a - \frac{a}{2} = \frac{a}{2}$

$$MCD(a,b) = MCD(b, a \bmod b)$$

$a \geq b > 0$



$$\boxed{a \bmod b < \frac{a}{2}}$$

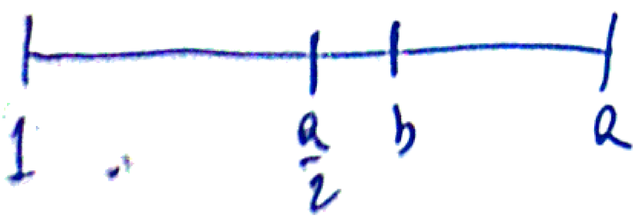
$b = \frac{a}{2}$ $\quad a \bmod b = 0 < \frac{a}{2}$

$b < \frac{a}{2}$ $\quad \boxed{a \bmod b < b} < \frac{a}{2}$ //

$b > \frac{a}{2}$ $\quad a \bmod b = a - b < a - \frac{a}{2} = \frac{a}{2}$

$$MCD(a,b) = MCD(b, a \bmod b)$$

$a \geq b > 0$



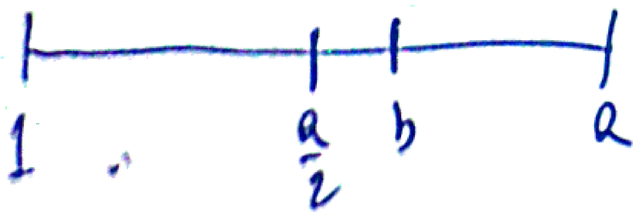
$$\boxed{a \bmod b < \frac{a}{2}}$$

$b = \frac{a}{2}$ $\quad a \bmod b = 0 < \frac{a}{2}$

$b < \frac{a}{2}$ $\quad \boxed{a \bmod b < b} < \frac{a}{2}$ //

$b > \frac{a}{2}$ $\quad a \bmod b = a - b < a - \frac{a}{2} = \frac{a}{2}$

$$3 \cdot 4 \equiv 1 \mod 11$$

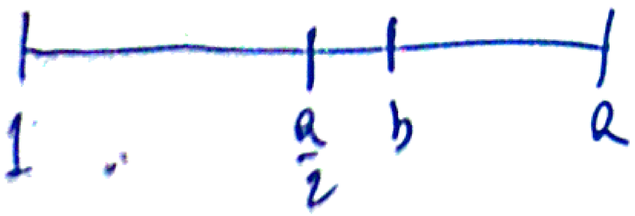


$b < \frac{a}{2}$ $\quad \boxed{a \bmod b < b} < \frac{a}{2}$ //

$b > \frac{a}{2}$ $\quad a \bmod b = a - b < a - \frac{a}{2} = \frac{a}{2}$

$3 \cdot 4 \equiv 1 \mod 11$

$3 \cdot 15 \equiv 1 \mod 11$

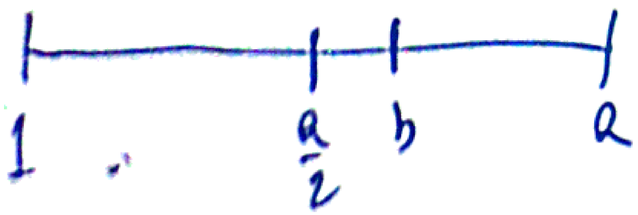


$b < \frac{a}{2}$ $\quad \boxed{a \bmod b < b} < \frac{a}{2}$ //

$b > \frac{a}{2}$ $\quad a \bmod b = a - \frac{a}{2} = \frac{a}{2}$

$$3 \cdot 4 \equiv 1 \mod 11$$

$$3 \cdot 15 \equiv 1 \mod 11$$

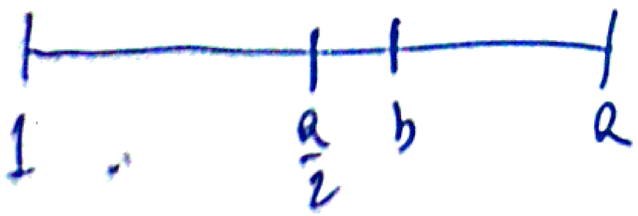


$b < \frac{a}{2}$ $\quad \boxed{a \bmod b < b} < \frac{a}{2}$ //

$b > \frac{a}{2}$ $\quad a \bmod b = a - b < a - \frac{a}{2} = \frac{a}{2}$

$$3 \cdot 4 \equiv 1 \mod 11$$

$$3 \cdot 15 \equiv 1 \mod 11$$

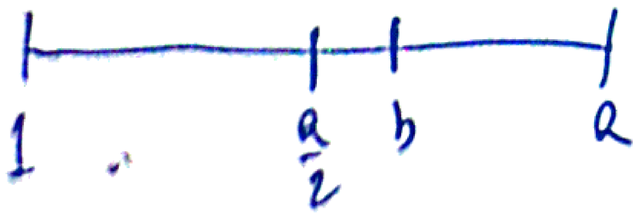


$b < \frac{a}{2}$ $\quad \boxed{a \bmod b < b} < \frac{a}{2}$ //

$b > \frac{a}{2}$ $\quad a \bmod b = a - b < a - \frac{a}{2} = \frac{a}{2}$

$3 \cdot 4 \equiv 1 \mod 11$

$3 \cdot 15 \equiv 1 \mod 11$



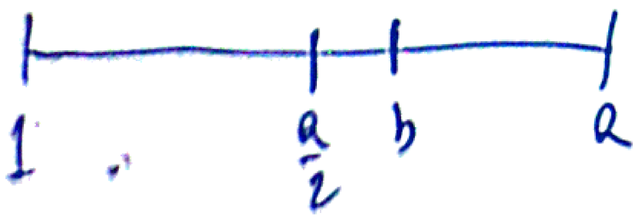
$b < \frac{a}{2}$ $\quad \boxed{a \bmod b < b} < \frac{a}{2}$ //

$b > \frac{a}{2}$ $\quad a \bmod b = a - b < a - \frac{a}{2} = \frac{a}{2}$

$3 \cdot 4 \equiv 1 \mod 11$

$3 \cdot 15 \equiv 1 \mod 11$

$\mod 10$

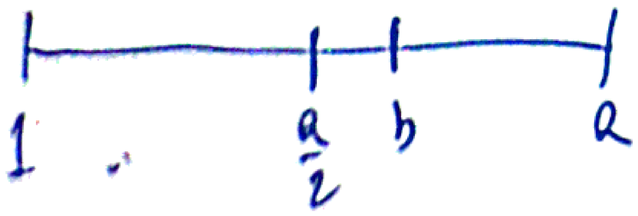


$b < \frac{a}{2}$ $\quad \boxed{a \bmod b < b} < \frac{a}{2}$ //

$b > \frac{a}{2}$ $\quad a \bmod b = a - b < a - \frac{a}{2} = \frac{a}{2}$

$3 \cdot 4 \equiv 1 \mod 11$

$3 \cdot 15 \equiv 1 \mod 11$



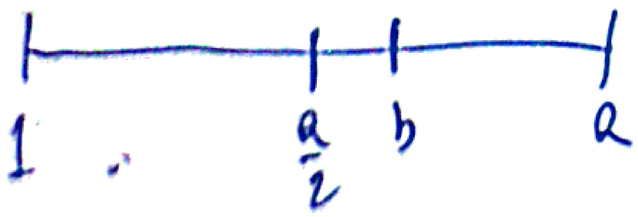
$2 \cdot x \equiv \square \mod 10$

$b < \frac{a}{2}$ $\quad \boxed{a \bmod b < b} < \frac{a}{2}$ //

$b > \frac{a}{2}$ $\quad a \bmod b = a - b < a - \frac{a}{2} = \frac{a}{2}$

$3 \cdot 4 \equiv 1 \mod 11$

$3 \cdot 15 \equiv 1 \mod 11$



$2 \cdot x \equiv \square \mod 10$

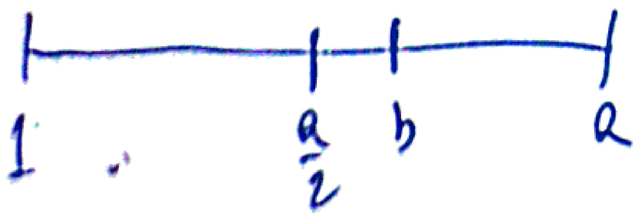
$b < \frac{a}{2}$ $\quad \boxed{a \bmod b < b} < \frac{a}{2}$ //

$b > \frac{a}{2}$ $\quad a \bmod b = a - b < a - \frac{a}{2} = \frac{a}{2}$

$3 \cdot 4 \equiv 1 \mod 11$

$3 \cdot 15 \equiv 1 \mod 11$

$2 \cdot \cancel{x \equiv 1} \mod 10$



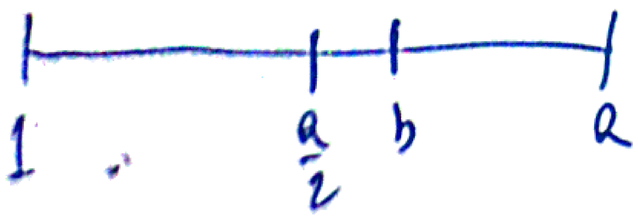
$b < \frac{a}{2}$ $\quad \boxed{a \bmod b < b} < \frac{a}{2}$ //

$b > \frac{a}{2}$ $\quad a \bmod b = a - b < a - \frac{a}{2} = \frac{a}{2}$

$3 \cdot 4 \equiv 1 \mod 11$

$3 \cdot 15 \equiv 1 \mod 11$

$2 \cdot \cancel{x \equiv 1} \mod 10$



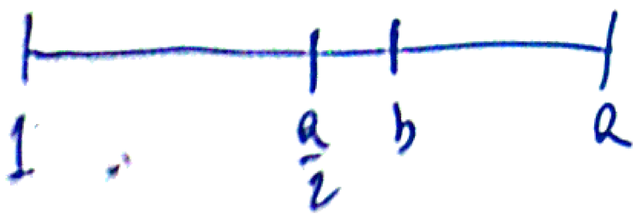
$b < \frac{a}{2}$ $\quad \boxed{a \bmod b < b} < \frac{a}{2}$ //

$b > \frac{a}{2}$ $\quad a \bmod b = a - b < a - \frac{a}{2} = \frac{a}{2}$

$3 \cdot 4 \equiv 1 \mod 11$

$3 \cdot 15 \equiv 1 \mod 11$

$2 \cdot \cancel{x \equiv 1} \mod 10$



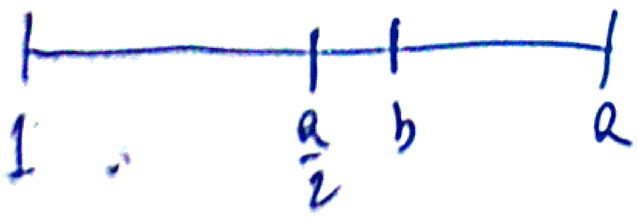
$b < \frac{a}{2}$ $\quad \boxed{a \bmod b < b} < \frac{a}{2}$ //

$b > \frac{a}{2}$ $\quad a \bmod b = a - b < a - \frac{a}{2} = \frac{a}{2}$

$3 \cdot 4 \equiv 1 \mod 11$

$3 \cdot 15 \equiv 1 \mod 11$

$2 \cdot \cancel{x \equiv 1} \mod 10$



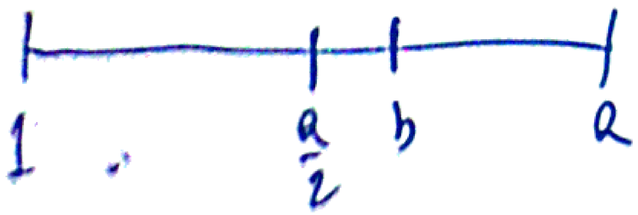
$b < \frac{a}{2}$ $\quad \boxed{a \bmod b < b} < \frac{a}{2}$ //

$b > \frac{a}{2}$ $\quad a \bmod b = a - b < a - \frac{a}{2} = \frac{a}{2}$

$3 \cdot 4 \equiv 1 \mod 11$

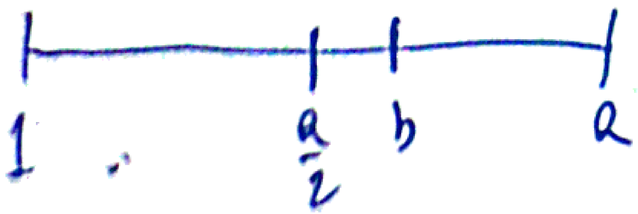
$3 \cdot 15 \equiv 1 \mod 11$

$2 \cdot \cancel{x \equiv 1} \mod 10$



$3 \cdot 4 \equiv 1 \mod 11$

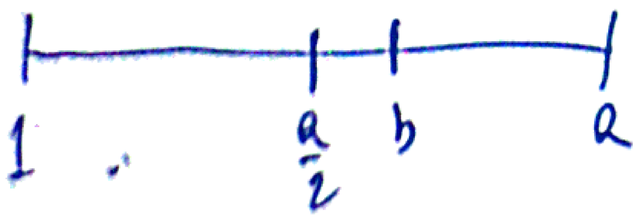
$3 \cdot 15 \equiv 1 \mod 11$



$MCD(a,b) = s \cdot a + t \cdot b$

$3 \cdot 4 \equiv 1 \mod 11$

$3 \cdot 15 \equiv 1 \mod 11$

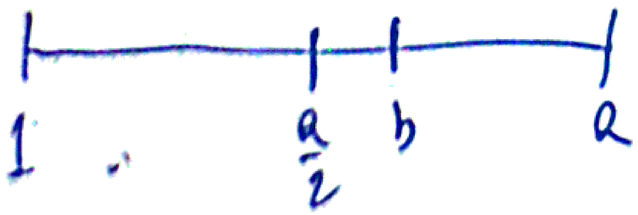


$MCD(a,b) = s \cdot a + t \cdot b$

$MCD(10,12) = 2 =$

$3 \cdot 4 \equiv 1 \mod 11$

$3 \cdot 15 \equiv 1 \mod 11$



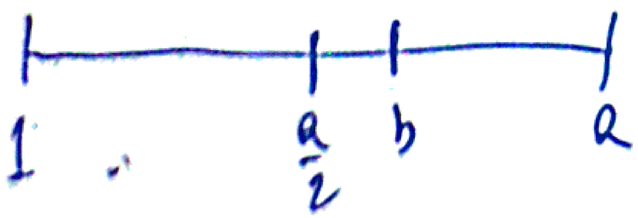
$MCD(a,b) = s \cdot a + t \cdot b$

$MCD(10,12) = \boxed{2 = s \cdot 10 + t \cdot 12}$

$-1 \cdot 10 +$

$3 \cdot 4 \equiv 1 \mod 11$

$3 \cdot 15 \equiv 1 \mod 11$



$MCD(a,b) = s \cdot a + t \cdot b$

$MCD(10,12) = \boxed{2 = s \cdot 10 + t \cdot 12}$

$-1 \cdot 10 + 1 \cdot 12$

$\Leftarrow$ / $MCD(a,n)=1$

$3 \cdot 4 \equiv 1 \mod 11$

$3 \cdot 15 \equiv 1 \mod 11$

$$\boxed{MCD(a,b) = s \cdot a + t \cdot b}$$

$$MCD(10,12) = \boxed{2 = s \cdot 10 + t \cdot 12}$$

$-1 \cdot 10 + 1 \cdot 12$

$\Leftarrow$ / $MCD(a,n)=1$

$3 \cdot 4 \equiv 1 \mod 11$

$3 \cdot 15 \equiv 1 \mod 11$

$$\boxed{MCD(a,b) = s \cdot a + t \cdot b}$$

$$MCD(10,12) = \boxed{2 = s \cdot 10 + t \cdot 12}$$

$-1 \cdot 10 + 1 \cdot 12$

$\Leftarrow$ / $MCD(a,n)=1$

$3 \cdot 4 \equiv 1 \mod 11$

$3 \cdot 15 \equiv 1 \mod 11$

$$\boxed{MCD(a,b) = s \cdot a + t \cdot b}$$

$MCD(10,12) = 2 = s \cdot 10 + t \cdot 12$

$-1 \cdot 10 + 1 \cdot 12$

$\Leftarrow$ $\underline{MCD(a,n)=1}$

$1 = s \cdot a + t \cdot n$

$5 \cdot 9 \equiv 1 \mod 11$

$3 \cdot 4 \equiv 1 \mod 11$

$3 \cdot 15 \equiv 1 \mod 11$

$\boxed{MCD(a,b) = s \cdot a + t \cdot b}$

$MCD(10,12) = \boxed{2 = s \cdot 10 + t \cdot 12}$

$-1 \cdot 10 + 1 \cdot 12$

$\Leftarrow$ $\underline{MCD(a,n)=1}$

$1 = s \cdot a + t \cdot n \;/ \bmod n$

$1 \equiv s \cdot a \bmod n$

$5 \cdot 9 \equiv 1 \bmod 11$

$3 \cdot 4 \equiv 1 \bmod 11$

$3 \cdot 15 \equiv 1 \bmod 11$

$\boxed{MCD(a,b) = s \cdot a + t \cdot b}$

$MCD(10,12) = \boxed{2 = s \cdot 10 + t \cdot 12}$

$-1 \cdot 10 + 1 \cdot 12$

$\Leftarrow$ $\underline{MCD(a,n)=1}$

$1 = s \cdot a + t \cdot n \;/ \bmod n$

$1 \equiv s \cdot a \bmod n$

$5 \cdot 9 \equiv 1 \bmod 11$

$3 \cdot 4 \equiv 1 \bmod 11$

$3 \cdot 15 \equiv 1 \bmod 11$

$\boxed{MCD(a,b) = s \cdot a + t \cdot b}$

$MCD(13,60) = 1 = s \cdot 13 + t \cdot 60$

$1 = (-23) \cdot 13 + 5 \cdot 60$

$\Leftarrow$ $\underline{MCD(a,n)=1}$

$1 = s\cdot a + t\cdot n \;/ \bmod n$

$1 \equiv s\cdot a \bmod n$

$-23 \cdot 13 \equiv 1 \bmod 60$

$37 \cdot 13 \equiv 1 \bmod 60$

$5\cdot 9 \equiv 1 \bmod 11$

$3\cdot 4 \equiv 1 \bmod 11$

$3\cdot 15 \equiv 1 \bmod 11$

$\boxed{MCD(a,b) = s\cdot a + t\cdot b}$

$MCD(13,60)=1 = s\cdot 13 + t\cdot 60$

$1 = (-23)\cdot 13 + 5\cdot 60$

$\Leftarrow$ $\underline{MCD(a,n)=1}$

$1 = s\cdot a + t\cdot n \;/ \bmod n$

$1 \equiv s\cdot a \bmod n$

$-23\cdot 13 \equiv 1 \bmod 60$

$37\cdot 13 \equiv 1 \bmod 60$

$5\cdot 9 \equiv 1 \bmod 11$

$3\cdot 4 \equiv 1 \bmod 11$

$3\cdot 15 \equiv 1 \bmod 11$

$\boxed{MCD(a,b) = s\cdot a + t\cdot b}$

$MCD(13,60)=1 = s\cdot 13 + t\cdot 60$

$1 = (-23)\cdot 13 + 5\cdot 60$

$\Leftarrow$ $\underline{MCD(a,n)=1}$

$\Rightarrow$ hay existe b tal que

$a \cdot b \equiv 1 \mod n$

$1 = s \cdot a + t \cdot n \;/ \mod n$

$1 \equiv s \cdot a \mod n$

$-23 \cdot 13 \equiv 1 \mod 60$

$37 \cdot 13 \equiv 1 \mod 60$

$\Leftarrow$ $\underline{MCD(a,n)=1}$

$1 = s\cdot a + t\cdot n \;/ \bmod n$

$1 \equiv s\cdot a \bmod n$

$-23\cdot 13 \equiv 1 \bmod 60$

$37\cdot 13 \equiv 1 \bmod 60$

$\Rightarrow$ hi existe b tal que

$a\cdot b \equiv 1 \bmod n$

$\Rightarrow n \mid (a\cdot b - 1)$ p.d. $MCD(a,n)=1$

$\Rightarrow \alpha\cdot n = a\cdot b - 1$

$\Rightarrow \boxed{1 = a\cdot b - \alpha\cdot n}$

$\Leftarrow$ $\underline{MCD(a,n)=1}$

$1 = s\cdot a + t\cdot n \;/ \bmod n$

$1 \equiv s\cdot a \bmod n$

$-23\cdot 13 \equiv 1 \bmod 60$

$37\cdot 13 \equiv 1 \bmod 60$

$\Rightarrow$ h. existe b tal que

$a\cdot b \equiv 1 \bmod n$

$\Rightarrow n \mid (a\cdot b - 1)$

p.d. $MCD(a,n)=1$

$\Rightarrow \alpha\cdot n = a\cdot b - 1$

$\Rightarrow \boxed{1 = a\cdot b - \alpha\cdot n}$

$\Leftarrow$ / $\underline{MCD(a,n)=1}$

$1 = s\cdot a + t\cdot n \;/ \bmod n$

$1 \equiv s\cdot a \bmod n$

$-23\cdot 13 \equiv 1 \bmod 60$

$37\cdot 13 \equiv 1 \bmod 60$

$\Rightarrow$ / Si existe b tal que

$a\cdot b \equiv 1 \bmod n$

$\Rightarrow n \mid (a\cdot b - 1)$

$\Rightarrow \alpha\cdot n = a\cdot b - 1$

$\Rightarrow \boxed{1 = a\cdot b - \alpha\cdot n}$

p.d. / si $c \mid a$ y $c \mid n$, entonces $c=1$

$\Leftarrow$ / $\underline{MCD(a,n)=1}$

$1 = s\cdot a + t\cdot n \;/ \bmod n$

$1 \equiv s\cdot a \bmod n$

$-23\cdot 13 \equiv 1 \bmod 60$

$37\cdot 13 \equiv 1 \bmod 60$

$\Rightarrow$ / Si existe b tal que

$a\cdot b \equiv 1 \bmod n$

$\Rightarrow n \mid (a\cdot b - 1)$

$\Rightarrow \alpha\cdot n = a\cdot b - 1$

$\Rightarrow \boxed{1 = a\cdot b - \alpha\cdot n}$

p.d./ si $c \mid a$ y $c \mid n$, entonces $c=1$

$c|a \Rightarrow c|a\cdot b$

$c|n$

$\Rightarrow$ / hi existe b tal que

$a\cdot b \equiv 1 \mod n$

$\Rightarrow n|(a\cdot b - 1)$

$\Rightarrow \alpha\cdot n = a\cdot b - 1$

$\Rightarrow \boxed{1 = a\cdot b - \alpha\cdot n}$.

p.d./ si $c|a$ y $c|n$, entonces $c=1$

$c \mid a \Rightarrow c \mid a \cdot b$

$c \mid n \Rightarrow c \mid (-\alpha) n$

$\Rightarrow c \mid a \cdot b - \alpha \cdot n$

$\Rightarrow c \mid 1$

$\Rightarrow c = 1$

propiedad: $c \mid a \Rightarrow c \mid a \cdot k$

$c \mid a$ y $c \mid b \Rightarrow c \mid (a+b)$

$\Rightarrow$ / hi existe b tal que

$a \cdot b \equiv 1 \mod n$

$\Rightarrow n \mid (a \cdot b - 1)$

$\Rightarrow \alpha \cdot n = a \cdot b - 1$

$\Rightarrow \boxed{1 = a \cdot b - \alpha \cdot n}$.

p.d./ si $c \mid a$ y $c \mid n$, entonces $c = 1$

$c \mid a \Rightarrow c \mid a \cdot b$

$c \mid n \Rightarrow c \mid (-\alpha) n$

$\Rightarrow c \mid a \cdot b - \alpha \cdot n$

$\Rightarrow c \mid 1$

$\Rightarrow c = 1$

Prop: $c \mid a \Rightarrow c \mid a \cdot k$

$c \mid a$ y $c \mid b \Rightarrow c \mid (a+b)$

$\Rightarrow$) Si existe b tal que

$a \cdot b \equiv 1 \mod n$

$\Rightarrow n \mid (a \cdot b - 1)$

$\Rightarrow \alpha \cdot n = a \cdot b - 1$

$\Rightarrow \boxed{1 = a \cdot b - \alpha \cdot n}$.

p.d.) si $c \mid a$ y $c \mid n$, entonces $c = 1$

$c \mid a \Rightarrow c \mid a \cdot b$

$c \mid n \Rightarrow c \mid (-\alpha) n$

$\Rightarrow c \mid a \cdot b - \alpha \cdot n$

$\Rightarrow c \mid 1$

$\Rightarrow c = 1$

Porque: $c \mid a \Rightarrow c \mid a \cdot k$

$c \mid a$ y $c \mid b \Rightarrow c \mid (a+b)$

$\Rightarrow$) Si existe b tal que

$a \cdot b \equiv 1 \mod n$

$\Rightarrow n \mid (a \cdot b - 1)$

$\Rightarrow \alpha \cdot n = a \cdot b - 1$

$\Rightarrow \boxed{1 = a \cdot b - \alpha \cdot n}$.

p.d.) Si $c \mid a$ y $c \mid n$, entonces $c = 1$

$c \mid a \Rightarrow c \mid a \cdot b$

$c \mid n \Rightarrow c \mid (-\alpha) n$

$\Rightarrow c \mid a \cdot b - \alpha \cdot n$

$\Rightarrow c \mid 1$

$\Rightarrow c = 1$

Prop: $c \mid a \Rightarrow c \mid a \cdot k$

$c \mid a$ y $c \mid b \Rightarrow c \mid (a+b)$

$\Rightarrow$) Si existe b tal que

$a \cdot b \equiv 1 \mod n$

$\Rightarrow n \mid (a \cdot b - 1)$

$\Rightarrow \alpha \cdot n = a \cdot b - 1$

$\Rightarrow \boxed{1 = a \cdot b - \alpha \cdot n}$.

p.d.) Si $c \mid a$ y $c \mid n$, entonces $c = 1$

$c \mid a \Rightarrow c \mid a \cdot b$

$c \mid n \Rightarrow c \mid (-\alpha) n$

$\Rightarrow c \mid a \cdot b - \alpha \cdot n$

$\Rightarrow c \mid 1$

$\Rightarrow c = 1$

Prop: $c \mid a \Rightarrow c \mid a \cdot k$

$c \mid a$ y $c \mid b \Rightarrow c \mid (a+b)$

$\Rightarrow$) Si existe b tal que

$a \cdot b \equiv 1 \mod n$

$\Rightarrow n \mid (a \cdot b - 1)$

$\Rightarrow \alpha \cdot n = a \cdot b - 1$

$\Rightarrow \boxed{1 = a \cdot b - \alpha \cdot n}$.

p.d.) Si $c \mid a$ y $c \mid n$, entonces $c = 1$