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

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

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

$a \geq b$

$MCD(a,b) = MCD(b, a \bmod b)$ $\qquad MCD(a,0) = a$

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

$a \geq b$

$MCD(a,b) = MCD(b, a \bmod b)$ $\qquad MCD(a,0) = a$

$r_0 = a$ $\qquad r_{i-1}$

$r_1 = b$ $\qquad r_i$

$r_2 = a \bmod b$ $\qquad r_{i+1} = r_{i-1} \bmod r_i$

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

$a \geq b$

$MCD(a,b) = MCD(b, a \bmod b)$ $\qquad MCD(a,0) = a$

$r_0 = a$ $\qquad r_{i-1}$

$r_1 = b$ $\qquad r_i$

$r_2 = a \bmod b$ $\qquad r_{i+1} = r_{i-1} \bmod r_i$

r_{k-1}

$r_k = 0$

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

$a \geq b$

$MCD(a,b) = MCD(b, a \bmod b)$ $\qquad MCD(a,0) = a$

$r_0 = a = s_0 \cdot a + t_0 \cdot b$

$r_1 = b$

$r_2 = a \bmod b$

$r_{i-1} = s_{i-1} \cdot a + t_{i-1} \cdot b$

$r_i = s_i \cdot a + t_i \cdot b$

$r_{i+1} = r_{i-1} \bmod r_i$

r_{k-1}

$r_k = 0$

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

$a \geq b$

$MCD(a,b) = MCD(b, a \bmod b)$ $\qquad MCD(a,0) = a$

$r_0 = a = 1 \cdot a + 0 \cdot b$ $\qquad r_{i-1} = s_{i-1} \cdot a + t_{i-1} \cdot b$

$r_1 = b = 0 \cdot a + 1 \cdot b$ $\qquad r_i = s_i \cdot a + t_i \cdot b$

$r_2 = a \bmod b$ $\qquad r_{i+1} = r_{i-1} \bmod r_i$

r_{k-1}

$r_k = 0$

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

$a \geq b$

$MCD(a,b) = MCD(b, a \bmod b)$ $\qquad MCD(a,0) = a$

$r_0 = a = 1 \cdot a + 0 \cdot b$ $\qquad r_{i-1} = s_{i-1} \cdot a + t_{i-1} \cdot b$

$r_1 = b = 0 \cdot a + 1 \cdot b$ $\qquad r_i = s_i \cdot a + t_i \cdot b$

$r_2 = a \bmod b$ $\qquad r_{i+1} = r_{i-1} \bmod r_i$

r_{k-1}

$r_k = 0$

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

$MCD(a, 0) = a$

$r_0 = a = 1 \cdot a + 0 \cdot b$

$r_1 = b = 0 \cdot a + 1 \cdot b$

$r_2 = a \bmod b$

$r_{i-1} = s_{i-1} \cdot a + t_{i-1} \cdot b$

$r_i = s_i \cdot a + t_i \cdot b$

$r_{i+1} = r_{i-1} \bmod r_i$

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

$MCD(a, 0) = a$

$r_0 = a = 1 \cdot a + 0 \cdot b$

$r_1 = b = 0 \cdot a + 1 \cdot b$

$r_2 = a \bmod b$

$r_{i-1} = s_{i-1} \cdot a + t_{i-1} \cdot b$

$r_i = s_i \cdot a + t_i \cdot b$

$r_{i+1} = r_{i-1} \bmod r_i$

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

$$r_{i-1} = \alpha \cdot r_i + \beta$$

$$MCD(a, 0) = a$$

$$r_{i-1} = s_{i-1} \cdot a + t_{i-1} \cdot b$$

$$r_i = s_i \cdot a + t_i \cdot b$$

$$r_{i+1} = r_{i-1} \bmod r_i$$

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

$$r_{i-1} = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot r_i + \underbrace{r_{i-1} \bmod r_i}_{r_{i+1}} \ldots\ldots$$

$$MCD(a, 0) = a$$

$$\boxed{r_{i+1} = r_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot r_i}$$

$$r_{i-1} = s_{i-1} \cdot a + t_{i-1} \cdot b$$

$$r_i = s_i \cdot a + t_i \cdot b$$

$$r_{i+1} = r_{i-1} \bmod r_i$$

$$r_{i+1} = s_{i+1} \cdot a + t_{i+1} \cdot b$$

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

$$r_{i-1} = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot r_i + \underbrace{r_{i-1} \bmod r_i}_{r_{i+1}} \quad \ldots\ldots$$

$$MCD(a, 0) = a$$

$$\boxed{r_{i+1} = r_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot r_i}$$

$$r_{i-1} = s_{i-1} \cdot a + t_{i-1} \cdot b$$

$$r_i = s_i \cdot a + t_i \cdot b$$

$$r_{i+1} = r_{i-1} \bmod r_i$$

$$r_{i+1} = s_{i+1} \cdot a + t_{i+1} \cdot b$$

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

$$r_{i-1} = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot r_i + \underbrace{r_{i-1} \bmod r_i}_{r_{i+1}} \ldots\ldots$$

$$MCD(a, 0) = a$$

$$\boxed{r_{i+1} = r_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot r_i}$$

$$r_{i-1} = s_{i-1} \cdot a + t_{i-1} \cdot b$$

$$r_i = s_i \cdot a + t_i \cdot b$$

$$r_{i+1} = r_{i-1} \bmod r_i$$

$$r_{i+1} = s_{i+1} \cdot a + t_{i+1} \cdot b$$

$a = 60, \; b = 13$

$$\boxed{r_{i+1} = r_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot r_i}$$

$r_{i+1} = r_{i-1} \bmod r_i$

$r_{i+1} = s_{i+1} \cdot a + t_{i+1} \cdot b$

$a = 60, \; b = 13$

$1 = s \cdot 60 + t \cdot 13$

$$\boxed{r_{i+1} = r_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot r_i}$$

$r_i = \ldots$

$r_{i+1} = r_{i-1} \bmod r_i$

$r_{i+1} = s_{i+1} \cdot a + t_{i+1} \cdot b$

$a = 60, \; b = 13$

$1 = s \cdot 60 + t \cdot 13$

$r_0 = 60 = 1 \cdot 60 + 0 \cdot 13$

$r_1 = 13 = 0 \cdot 60 + 1 \cdot 13$

$r_2 =$

$a = 60, \; b = 13$

$1 = s \cdot 60 + t \cdot 13$

$r_0 = 60 = 1 \cdot 60 + 0 \cdot 13$

$r_1 = 13 = 0 \cdot 60 + 1 \cdot 13$

$r_2 = 8 =$

$a = 60, \; b = 13$

$1 = s \cdot 60 + t \cdot 13$

$r_0 = 60 = 1 \cdot 60 + 0 \cdot 13$

$r_1 = 13 = 0 \cdot 60 + 1 \cdot 13$

$r_2 = 8 = 60$

$s_2 = s_0 - \left\lfloor \frac{r_0}{r_1} \right\rfloor \cdot s_1$

$a = 60, \; b = 13$

$1 = s \cdot 60 + t \cdot 13$

$r_0 = 60 = 1 \cdot 60 + 0 \cdot 13$

$r_1 = 13 = 0 \cdot 60 + 1 \cdot 13$

$r_2 = 8 = 1 \cdot 60 + (-4) \cdot 13$

$s_2 = s_0 - \left\lfloor \frac{r_0}{r_1} \right\rfloor \cdot s_1$

$1 - 4 \cdot 0 = 1$

$t_2 = \cancel{t_0} - \left\lfloor \frac{r_0}{r_1} \right\rfloor \cancel{t_1} = -4$

$a = 60, \; b = 13$

$1 = s \cdot 60 + t \cdot 13$

$r_0 = 60 = 1 \cdot 60 + 0 \cdot 13$

$r_1 = 13 = 0 \cdot 60 + 1 \cdot 13$

$r_2 = 8 = 1 \cdot 60 + (-4) \cdot 13$

$s_2 = s_0 - \left\lfloor \frac{r_0}{r_1} \right\rfloor \cdot s_1$

$1 - 4 \cdot 0 = 1$

$t_2 = \underset{0}{\cancel{t_0}} - \left\lfloor \frac{r_0}{r_1} \right\rfloor \underset{1}{\cancel{t_1}} = -4$

$a = 60, \quad b = 13$

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

$r_0 = 60 = 1 \cdot 60 + 0 \cdot 13$

$r_1 = 13 = 0 \cdot 60 + 1 \cdot 13$

$r_2 = 8 = 1 \cdot 60 + (-4) \cdot 13$

$s_2 = s_0 - \left\lfloor \frac{r_0}{r_1} \right\rfloor \cdot s_1$

$1 - 4 \cdot 0 = 1$

$t_2 = \underset{0}{\cancel{t_0}} - \left\lfloor \frac{r_0}{r_1} \right\rfloor \underset{1}{\cancel{t_1}} = -4$

$a = 60, \quad b = 13$

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

$r_0 = 60 = 1 \cdot 60 + 0 \cdot 13 = a$

$r_1 = 13 = 0 \cdot 60 + 1 \cdot 13$

$r_2 = 8 = 1 \cdot 60 + (-4) \cdot 13$

$s_2 = s_0 - \left\lfloor \frac{r_0}{r_1} \right\rfloor \cdot s_1$

$1 - 4 \cdot 0 = 1$

$t_2 = \cancel{t_0} - \left\lfloor \frac{r_0}{r_1} \right\rfloor \cancel{t_1} = -4$

$a = 60, \quad b = 13$

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

$r_0 = 60 = 1 \cdot 60 + 0 \cdot 13$

$r_1 = 13 = 0 \cdot 60 + 1 \cdot 13$

$r_2 = 8 = 1 \cdot 60 + (-4) \cdot 13$

$s_2 = s_0 - \left\lfloor \frac{r_0}{r_1} \right\rfloor \cdot s_1$

$1 - 4 \cdot 0 = 1$

$t_2 = \cancel{t_0}^{\,0} - \left\lfloor \frac{r_0}{r_1} \right\rfloor \cancel{t_1}^{\,1} = -4$

$a = 60, \quad b = 13$

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

$r_0 = 60 = 1 \cdot 60 + 0 \cdot 13$

$r_1 = 13 = 0 \cdot 60 + 1 \cdot 13$

$r_2 = 8 = 1 \cdot 60 + (-4) \cdot 13$

$s_2 = s_0 - \left\lfloor \frac{r_0}{r_1} \right\rfloor \cdot s_1$

$1 - 4 \cdot 0 = 1$

$t_2 = \cancel{t_0}^{\,0} - \left\lfloor \frac{r_0}{r_1} \right\rfloor \cancel{t_1}^{\,1} = -4$

$a = 60$, $b = 13$

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

$r_0 = 60 = 1 \cdot 60 + 0 \cdot 13 = a$

$r_1 = 13 = 0 \cdot 60 + 1 \cdot 13$

$r_2 = 8 = 1 \cdot 60 + (-4) \cdot 13$

$s_2 = s_0 - \left\lfloor \frac{r_0}{r_1} \right\rfloor \cdot s_1$

$1 - 4 \cdot 0 = 1$

$t_2 = \cancel{t_0} - \left\lfloor \frac{r_0}{r_1} \right\rfloor \cancel{t_1} = -4$

$a = 60, \; b = 13$

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

$p = 7$

$a \in \{0, \ldots, 6\}$

$a^7 \equiv a \mod 7$

$2^7 = \boxed{128 \equiv 2 \mod 7}$

$126 =$

$1 - 4 \cdot 0 = 1$

$t_2 = \cancel{t_0}^{\,0} - \left\lfloor \frac{r_0}{r_1} \right\rfloor \cancel{t_1}^{\,1} = -4$

$a = 60, \; b = 13$

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

$p = 7$

$a \in \{0, \ldots, 6\}$

$a^7 \equiv a \mod 7$

$6^7 \mod 7$

$2^7 = \boxed{128 \equiv 2 \mod 7}$

$126 : 18$

$1 - 4 \cdot 0 = 1$

$t_2 = \cancel{t_0} - \left\lfloor \frac{r_0}{r_1} \right\rfloor \cancel{t_1} = -4$

$a = 60, \; b = 13$ $\qquad 1 = 5 \cdot 60 + (-23) \cdot 13$

$p = 7 \qquad 8^7 \equiv 8 \mod 7$

$a \in \{0, \ldots, 6\} \qquad a^7 \equiv a \mod 7$

$6^7 \mod 7 \qquad 6 \equiv -1 \mod 7 \qquad 2^7 = \boxed{128 \equiv 2 \mod 7}$

$= (-1)^7 \mod 7$

$\equiv -1 \mod 7$

$\equiv 6 \mod 7$

$126 : 18$

$1 - 4 \cdot 9 = 1$

$t_2 = \cancel{t_0} - \left\lfloor \frac{r_0}{r_1} \right\rfloor \cancel{t_1} = -4$

$a = 60$, $b = 13$ $\qquad 1 = 5 \cdot 60 + (-23) \cdot 13$

$p = 7$ $\qquad 8^7 \equiv 8 \mod 7$

$a \in \{1, \ldots, 6\}$ $\qquad a^6 \equiv 1 \mod 7$

$a = 60, \; b = 13$

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

$p = 7$

$8^7 \equiv 8 \mod 7$

$a \in \{1, \ldots, 6\}$

$\boxed{a^6 \equiv 1 \mod 7}$

$a^7 = a \; / \cdot \frac{1}{a}$

$a^6 = 1$

$a^7 \equiv a \mod 7$

$a \cdot b \equiv 1 \mod 7$

$a^7 \cdot b \equiv \cancel{a \cdot b}^{\,2} \mod 7$

$a^6 \cdot \underbrace{\cancel{a \cdot b}}_{1} \equiv 1 \mod 7$

$a = 60$, $b = 13$ $\qquad 1 = 5 \cdot 60 + (-23) \cdot 13$

$p = 7$ $\qquad 8^7 \equiv 8 \mod 7$

$a^7 = a \,/ \cdot \frac{1}{a}$

$a^6 = 1$

p es primo, $a \in \{1, \dots, p-1\}$

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

p no es primo, $a \in \{1, \dots, p-1\}$

$a = 60$, $b = 13$ $\qquad 1 = 5 \cdot 60 + (-23) \cdot 13$

$p = 7$ $\qquad 8^7 \equiv 8 \mod 7$

$a^7 = a \,/ \cdot \frac{1}{a}$

$a^6 = 1$

p es primo, $a \in \{1, \dots, p-1\}$

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

n no es primo, $a \in \{1, \dots, n-1\}$

$a^{n-1} \equiv 1 \mod n$

$a = 60$, $b = 13$ $\qquad 1 = 5 \cdot 60 + (-23) \cdot 13$

$p = 7 \qquad 8^7 \equiv 8 \mod 7$

$a^7 = a \,/ \cdot \frac{1}{a}$

$a^6 = 1$

p es primo, $a \in \{1, \dots, p-1\}$

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

n no es primo, $a \in \{1, \dots, n-1\}$

$a^{n-1} \equiv 1 \mod n$

$a = 60$, $b = 13$ $\qquad 1 = 5 \cdot 60 + (-23) \cdot 13$

$p = 7 \qquad 8^7 \equiv 8 \mod 7$

$a^7 = a \,/ \cdot \frac{1}{a}$

$a^6 = 1$

p es primo, $a \in \{1, \dots, p-1\}$

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

n no es primo, $a \in \{1, \dots, n-1\}$

$a^{n-1} \equiv 1 \mod n$

$a = 60$, $b = 13$ $\qquad 1 = 5 \cdot 60 + (-23) \cdot 13$

$p = 7 \qquad 8^7 \equiv 8 \mod 7$

$a^7 = a \,/ \cdot \frac{1}{a}$

$a^6 = 1$

p es primo, $a \in \{1, \dots, p-1\}$

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

n no es primo, $a \in \{1, \dots, n-1\}$

$n = 9 \qquad 1^8 \equiv 1 \mod 9 \qquad a^{n-1} \equiv 1 \mod n$

$8^8 \equiv 1 \mod 9$

$a = 60$, $b = 13$ $\qquad 1 = 5 \cdot 60 + (-23) \cdot 13$

$p = 7$ $\qquad 8^7 \equiv 8 \mod 7$

p es primo, $a \in \{1, \dots, p-1\}$

$a^7 = a \,/ \cdot \frac{1}{a}$ $\qquad a^{p-1} \equiv 1 \mod p$

$a^6 = 1$

n no es primo, $a \in \{1, \dots, n-1\}$

$d \mid n \quad 1 < d < n$ $\qquad n = d \cdot m$

$d^{n-1} \not\equiv 1 \mod n$

$a = 60$, $b = 13$ $\qquad 1 = 5 \cdot 60 + (-23) \cdot 13$

$p = 7$ $\qquad 8^7 \equiv 8 \mod 7$

p es primo, $a \in \{1, \dots, p-1\}$

$a^7 = a \,/ \cdot \frac{1}{a}$ $\qquad a^{p-1} \equiv 1 \mod p$

$a^6 = 1$

n no es primo, $a \in \{1, \dots, n-1\}$

$d \mid n \quad 1 < d < n$ $\qquad n = d \cdot m$

$d^{n-1} \not\equiv 1 \mod n$

$a = 60$, $b = 13$ $\qquad 1 = 5 \cdot 60 + (-23) \cdot 13$

$p = 7$ $\qquad 8^7 \equiv 8 \mod 7$

p es primo, $a \in \{1, \dots, p-1\}$

$a^7 = a \,/ \cdot \frac{1}{a}$

$a^6 = 1$

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

n no es primo, $a \in \{1, \dots, n-1\}$

$d \mid n \quad 1 < d < n$

$n = d \cdot m$

$d^{n-1} \equiv 1 \mod n \qquad d \, d^{n-2} \equiv 1 \mod n$

$n = 9$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a = 60, \; b = 13$

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

$p = 7$

$8^7 \equiv 8 \mod 7$

$a^7 = a \;/ \cdot \frac{1}{a}$

$a^6 = 1$

p es primo, $a \in \{1, \dots, p-1\}$

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

n no es primo, $a \in \{1, \dots, n-1\}$

$d \mid n \quad 1 < d < n$

$n = d \cdot m$

$d^{n-1} \equiv 1 \mod n \qquad d \, d^{n-2} \equiv 1 \mod n$

$n = 9$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a = 60, \; b = 13$

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

$p = 7$

$8^7 \equiv 8 \mod 7$

$a^7 = a \; / \cdot \frac{1}{a}$

$a^6 = 1$

p es primo, $a \in \{1, \dots, p-1\}$

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

n no es primo, $a \in \{1, \dots, n-1\}$

$d \mid n \quad 1 < d < n$

$n = d \cdot m$

$d^{n-1} \equiv 1 \mod n$

$d \, d^{n-2} \equiv 1 \mod n$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a^7 = a \quad / \cdot \frac{1}{a}$

$a^6 = 1$

$a = 60, \; b = 13$

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

$p = 7$

$8^7 \equiv 8 \mod 7$

p es primo, $a \in \{1, \dots, p-1\}$

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

n no es primo, $a \in \{1, \dots, n-1\}$

$d \mid n \quad 1 < d < n$

$n = d \cdot m$

$d^{n-1} \equiv 1 \mod n \qquad d \, d^{n-2} \equiv 1 \mod n$

$n = 9$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a = 60$, $b = 13$

$p = 7$

$d^{\ } - 1 \equiv 0 \mod n$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

$a^7 = a \,/ \cdot \frac{1}{a}$

$a^6 = 1$

p es primo, $a \in \{1, \ldots, p-1\}$

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

n no es primo, $a \in \{1, \ldots, n-1\}$

$d \mid n \quad 1 < d < n$

$n = d \cdot m$

$d^{n-1} \equiv 1 \mod n \qquad d \cdot d^{n-2} \equiv 1 \mod n$

$n = 9$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a^7 = a \,/ \cdot \frac{1}{a}$

$a^6 = 1$

$a = 60$, $b = 13$

$p = 7$

$d^{n-1} - 1 \equiv 0 \mod n$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

p es primo, $a \in \{1, \dots, p-1\}$

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

n no es primo, $a \in \{1, \dots, n-1\}$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a^7 = a \quad / \cdot \frac{1}{a}$

$a^6 = 1$

$a = 60, \; b = 13$

$p = 7$

$d^{\ } - 1 \equiv 0 \mod n$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \ldots, n-1\} : a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \ldots, n-1\} : a^{n-1} \not\equiv 1 \mod n$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a^7 = a \quad / \cdot \frac{1}{a}$

$a^6 = 1$

$a = 60, \; b = 13$

$p = 7$

$d^{\ } - 1 \equiv 0 \mod n$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \dots, n-1\} : a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\} : a^{n-1} \not\equiv 1 \mod n$

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

$\to \neq 1$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a^7 = a \quad / \cdot \frac{1}{a}$

$a^6 = 1$

$a = 60, \; b = 13$

$p = 7$

$d^{\ } - 1 \equiv 0 \mod n$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \dots, n-1\}: \; a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: \; a^{n-1} \not\equiv 1 \mod n$

$a \in \{1, \dots, n-1\}: \quad a^{n-1} \mod n \to 1$

$\searrow \neq 1$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a^7 = a \quad / \cdot \frac{1}{a}$

$a^6 = 1$

$a = 60, \; b = 13$

$p = 7$

$d^{n-1} - 1 \equiv 0 \mod n$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \dots, n-1\}: \; a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: \; a^{n-1} \not\equiv 1 \mod n$

$a \in \{1, \dots, n-1\} \qquad a^{n-1} \mod n \to 1$

$\qquad\qquad\qquad\qquad\qquad\qquad \to \neq 1$

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

$a^{n-1} \mod n = 1$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a^7 = a \,/ \cdot \frac{1}{a}$

$a^6 = 1$

$a = 60$, $b = 13$

$p = 7$

$d^{\ } - 1 \equiv 0 \mod n$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$a \in \{1, \dots, n-1\}$ $\quad a^{n-1} \mod n \to 1$, $\to \neq 1$

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

$a^{n-1} \mod n = 1$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a^7 = a \;/ \cdot \frac{1}{a}$

$a^6 = 1$

$a = 60$, $b = 13$

$p = 7$

$d^{\ } - 1 \equiv 0 \mod n$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

n compuesto $\quad \left| \{ a \in \{1, \dots, n-1\} \mid a^{n-1} \bmod n = 1 \} \right| = \sqrt{n}$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a^7 = a \;/ \cdot \frac{1}{a}$

$a^6 = 1$

$a = 60, \; b = 13$

$p = 7$

$d^{n-1} - 1 \equiv 0 \mod n$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \dots, n-1\} : a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\} : a^{n-1} \not\equiv 1 \mod n$

n compuesto $\quad \left| \{ a \in \{1, \dots, n-1\} \mid a^{n-1} \bmod n = 1 \} \right| = \sqrt{n}$

$$Pr(\text{error}) = \frac{\sqrt{n}}{n} = \frac{1}{\sqrt{n}}$$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a^7 = a \;/ \cdot \frac{1}{a}$

$a^6 = 1$

$a = 60, \; b = 13$

$p = 7$

$d^{\cdot} - 1 \equiv 0 \mod n$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \dots, n-1\} : a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\} : a^{n-1} \not\equiv 1 \mod n$

n compuesto $\quad \left| \{ a \in \{1, \dots, n-1\} \mid a^{n-1} \bmod n = 1 \} \right| = \sqrt{n}$

$$Pr(\text{error}) = \frac{\sqrt{n}}{n} = \frac{1}{\sqrt{n}}$$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a^7 = a \;/ \cdot \frac{1}{a}$

$a^6 = 1$

$a = 60, \; b = 13$

$p = 7$

$d^{n-1} - 1 \equiv 0 \mod n$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \dots, n-1\} : a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\} : a^{n-1} \not\equiv 1 \mod n$

n compuesto $\quad \left| \{ a \in \{1, \dots, n-1\} \mid a^{n-1} \bmod n = 1 \} \right| = \sqrt{n}$

$n \geq 10^{599}$

$$Pr(\text{error}) = \frac{\sqrt{n}}{n} = \frac{1}{\sqrt{n}} \to \frac{1}{10^{299.5}}$$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a^7 = a \;/ \cdot \frac{1}{a}$

$a^6 = 1$

$a = 60, \; b = 13$

$p = 7$

$d^{n-1} - 1 \equiv 0 \mod n$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \dots, n-1\} : a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\} : a^{n-1} \not\equiv 1 \mod n$

n compuesto $\quad \left| \{ a \in \{1, \dots, n-1\} \mid a^{n-1} \bmod n = 1 \} \right| \leq \frac{1}{2} \cdot n$

$n \geq 10^{599}$

$Pr(\text{error}) = \frac{\sqrt{n}}{n} = \frac{1}{\sqrt{n}} \quad \frac{1}{10^{299.5}}$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a^7 = a \;/ \cdot \frac{1}{a}$

$a^6 = 1$

$a = 60, \; b = 13$

$p = 7$

$d^{n-1} - 1 \equiv 0 \mod n$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \dots, n-1\} : a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\} : a^{n-1} \not\equiv 1 \mod n$

n compuesto

$$\left| \{ a \in \{1, \dots, n-1\} \mid a^{n-1} \bmod n = 1 \} \right| \leq \frac{1}{2} \cdot n$$

$$Pr(\text{error}) = \frac{\frac{1}{2} \cdot n}{n} = \frac{1}{2}$$

$n \geq 10^{599}$

$$\frac{1}{10^{299.5}}$$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a^7 = a \;/ \cdot \frac{1}{a}$

$a^6 = 1$

$a = 60, \; b = 13$

$p = 7$

$d^{n-1} - 1 \equiv 0 \mod n$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \dots, n-1\} : a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\} : a^{n-1} \not\equiv 1 \mod n$

n compuesto

$$\left| \{ a \in \{1, \dots, n-1\} \mid a^{n-1} \bmod n = 1 \} \right| \leq \frac{1}{2} \cdot n$$

$$Pr(\text{error}) = \frac{\frac{1}{2} \cdot n}{n} = \frac{1}{2}$$

$n \geq 10^{599}$

$$\frac{1}{10^{299.5}}$$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a^7 = a \;/ \cdot \frac{1}{a}$

$a^6 = 1$

$a = 60$, $b = 13$

$p = 7$

$d^{n-1} - 1 \equiv 0 \mod n$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \dots, n-1\} : a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\} : a^{n-1} \not\equiv 1 \mod n$

n compuesto $\quad \left| \{ a \in \{1, \dots, n-1\} \mid a^{n-1} \bmod n = 1 \} \right| \leq \frac{1}{2} \cdot n$

$n \geq 10^{519}$

$Pr(\text{error}) = \frac{\frac{1}{2} \cdot n}{n} = \frac{1}{2}$

$\frac{1}{10^{279.5}}$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a^7 = a \;/ \cdot \frac{1}{a}$

$a^6 = 1$

$a = 60$, $b = 13$

$p = 7$

$d^{n-1} - 1 \equiv 0 \mod n$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

n compuesto

$$\left| \{ a \in \{1, \dots, n-1\} \mid a^{n-1} \bmod n = 1 \} \right| \leq \frac{1}{2} \cdot n$$

$$Pr(\text{error}) = \frac{\frac{1}{2} \cdot n}{n} = \frac{1}{2}$$

$n \geq 10^{599}$

$$\frac{1}{10^{299.5}}$$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a^7 = a \;/ \cdot \frac{1}{a}$

$a^6 = 1$

$a = 60, \; b = 13$

$p = 7$

$d^{n-1} - 1 \equiv 0 \mod n$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

n compuesto

$$\left| \{ a \in \{1, \dots, n-1\} \mid a^{n-1} \bmod n = 1 \} \right| \leq \frac{1}{2} \cdot n$$

$$Pr(\text{error}) = \frac{\frac{1}{2} \cdot n}{n} = \frac{1}{2}$$

$n \geq 10^{519}$

$\frac{1}{19.5}$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a^7 = a \;/ \cdot \frac{1}{a}$

$a^6 = 1$

$a = 60$, $b = 13$

$p = 7$ $\quad N = P \cdot Q$

$d^{\ } - 1 \equiv 0 \mod n$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

n compuesto $\quad \left| \{ a \in \{1, \dots, n-1\} \mid a^{n-1} \equiv 1 \} \right| \leq \frac{1}{2} \cdot n$

$Pr(\text{error}) = \frac{\frac{1}{2} \cdot n}{n} = \frac{1}{2}$

$n \geq 10^{599}$

$\frac{1}{2^{199.5}}$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a^7 = a \,/ \cdot \frac{1}{a}$

$a^6 = 1$

$a = 60$, $b = 13$

$p = 7$ $\quad N = P \cdot Q$

$d^{\ } - 1 \equiv 0 \mod n$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

n compuesto

$\{a \in \{1, \dots, n-1\} \mid a^{n-1} \bmod n \neq 1\} \supseteq$

$\{a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1\}$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a^7 = a \,/ \cdot \frac{1}{a}$

$a^6 = 1$

$a = 60$, $b = 13$

$p = 7$ $\quad N = P \cdot Q$

$d^{\ } - 1 \equiv 0 \mod n$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

n compuesto

$\{a \in \{1, \dots, n-1\} \mid a^{n-1} \bmod n \neq 1\} \supseteq$

$\{a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1\}$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a^7 = a \,/ \cdot \frac{1}{a}$

$a^6 = 1$

$a = 60$, $b = 13$

$p = 7$ $\quad N = P \cdot Q$

$d^{n-1} - 1 \equiv 0 \mod n$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

n compuesto

$\{a \in \{1, \dots, n-1\} \mid a^{n-1} \bmod n \neq 1\} \supseteq$

$\{a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1\}$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a^7 = a \,/ \cdot \frac{1}{a}$

$a^6 = 1$

$a = 60$, $b = 13$

$p = 7$ $\quad N = P \cdot Q$

$d^{n-1} - 1 \equiv 0 \mod n$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

n compuesto

$\{a \in \{1, \dots, n-1\} \mid a^{n-1} \bmod n \neq 1\} \supseteq$

$\{a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1\}$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a = 60$, $b = 13$

$d^{\ } - 1 \equiv 0 \mod n$

$p = 7$ $\quad N = P \cdot Q$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$\{a \in \{1, \dots, n-1\} \mid a^{n-1} \mod n \neq 1\} \supseteq$

$\{a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1\}$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

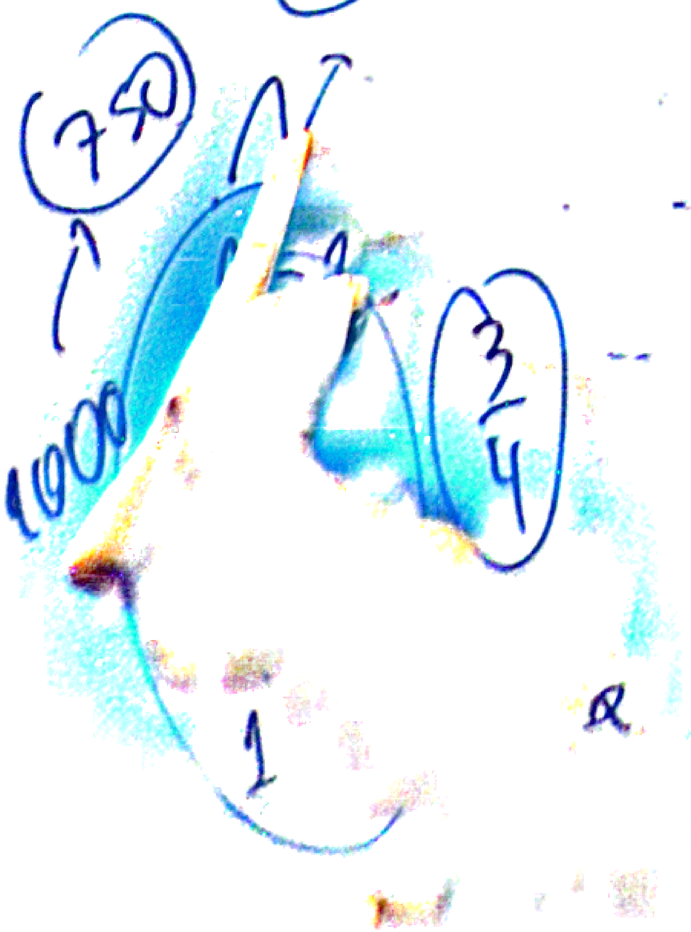
$a = 60$, $b = 13$

$d^{\ } - 1 \equiv 0 \mod n$

$p = 7$ $\quad N = P \cdot Q$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$



n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$\{a \in \{1, \dots, n-1\} \mid a^{n-1} \mod n \neq 1\} \supseteq$

$\{a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1\}$

$MCD(a, N)$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a = 60$, $b = 13$

$d^{\ } - 1 \equiv 0 \mod n$

$p = 7$ $\quad N = P \cdot Q$

$n \mid d^{n-1} - 1$

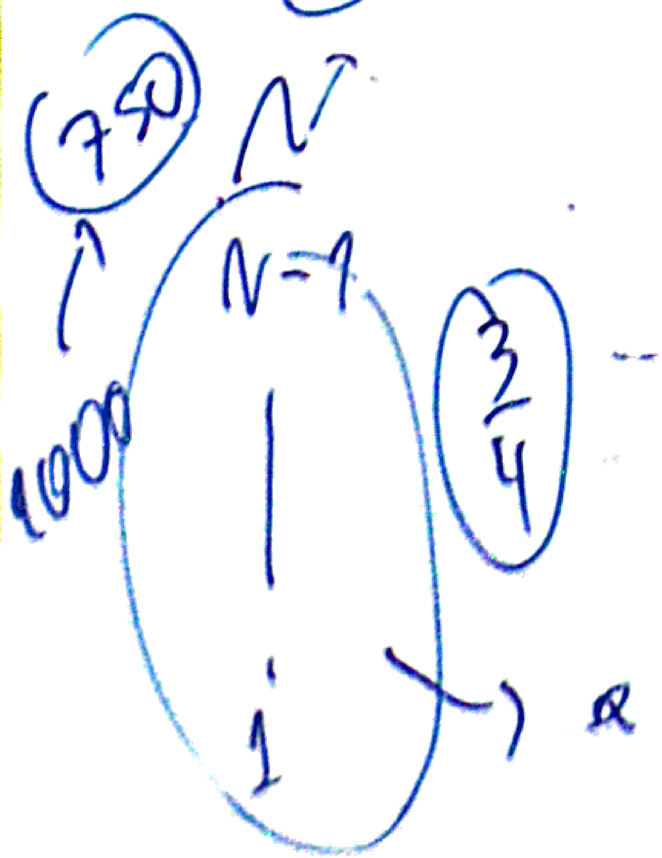
$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$\{a \in \{1, \dots, n-1\} \mid a^{n-1} \mod n \neq 1\} \supseteq$

$\{a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1\}$



$MCD(a, N)$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a = 60$, $b = 13$

$d^{\ } - 1 \equiv 0 \mod n$

$p = 7$ $\quad N = P \cdot Q$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$\{a \in \{1, \dots, n-1\} \mid a^{n-1} \bmod n \neq 1\} \supseteq$

$\{a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1\}$

$(7 \cdot 4)$ N

$N = 1$

1000

$\frac{3}{4}$

1

a

$MCD(a, N)$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a = 60$, $b = 13$

$d^{\ } - 1 \equiv 0 \mod n$

$p = 7$ $\quad N = P \cdot Q$

$n \mid d^{n-1} - 1$

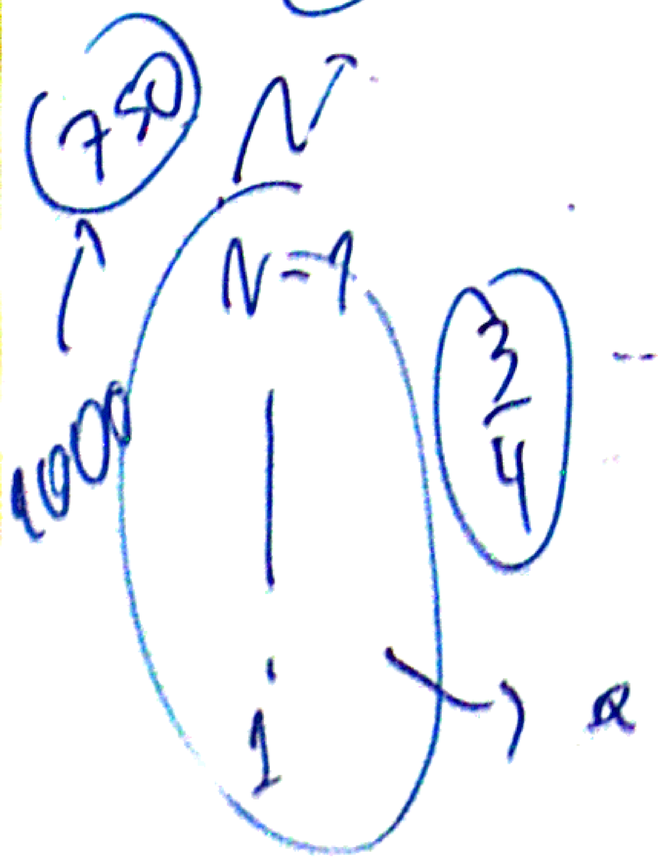
$n \cdot \alpha = d^{n-1} - 1$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$\{a \in \{1, \dots, n-1\} \mid a^{n-1} \bmod n \neq 1$

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



$MCD(a, N)$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a = 60$, $b = 13$

$d^{\ } - 1 \equiv 0 \mod n$

$p = 7$ $\quad N = P \cdot Q$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

$(7 \cdot 4)$ N

$N = 1$

1000

$\frac{3}{4}$

1

α

$MCD(a, N)$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$\{a \in \{1, \dots, n-1\} \mid a^{n-1} \mod n \neq 1\} \supseteq$

$\{a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1\}$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a = 60$, $b = 13$

$d^{\ } - 1 \equiv 0 \mod n$

$p = 7$ $\quad N = P \cdot Q$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

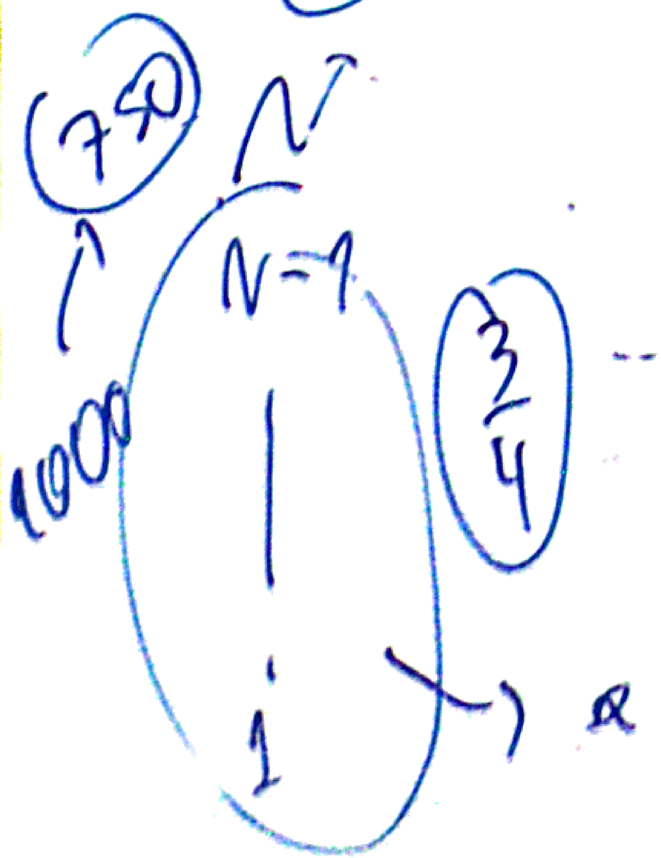
$\mathbb{Z}_n = \{0, \dots, n-1\}$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$\{a \in \{1, \dots, n-1\} \mid a^{n-1} \bmod n \neq 1\} \supseteq$

$\{a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1\}$



$MCD(a, N)$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a = 60$, $b = 13$

$d^{\ } - 1 \equiv 0 \mod n$

$p = 7$ $\quad N = P \cdot Q$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

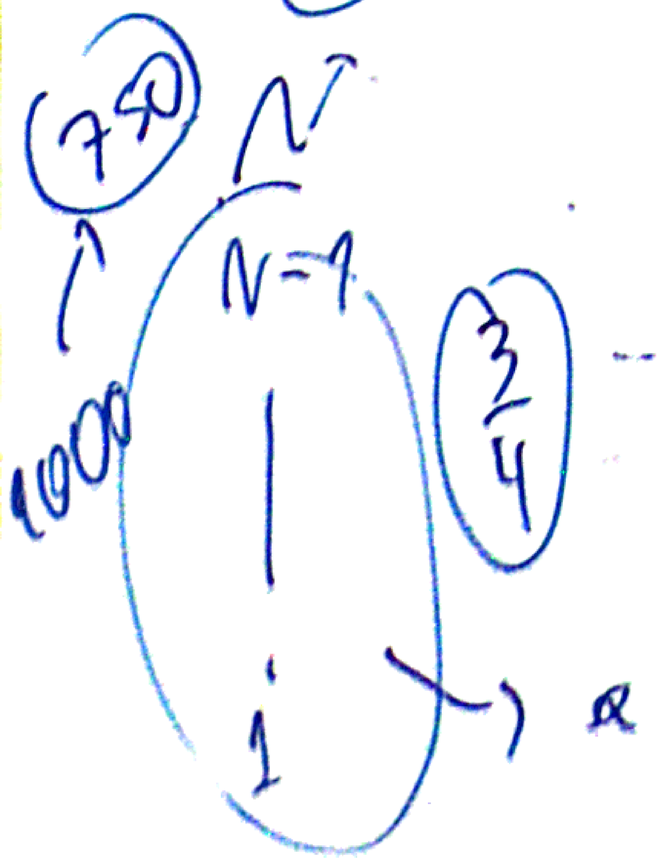
$\mathbb{Z}_n = \{0, \dots, n-1\}$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$\{a \in \{1, \dots, n-1\} \mid a^{n-1} \bmod n \neq 1\} \supseteq$

$\{a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1\}$



$MCD(a, N)$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a = 60$, $b = 13$

$d^{\ } - 1 \equiv 0 \mod n$

$p = 7$ $\quad N = P \cdot Q$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

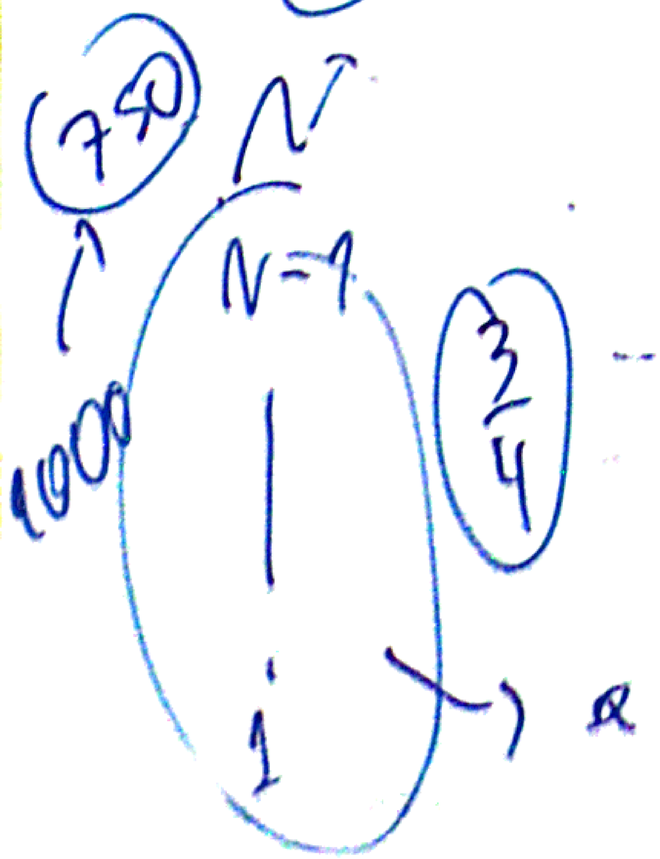
$\mathbb{Z}_n = \{0, \dots, n-1\}$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$\{a \in \{1, \dots, n-1\} \mid a^{n-1} \bmod n \neq 1\} \supseteq$

$\{a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1\}$



$MCD(a, N)$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a = 60$, $b = 13$

$d^{\ } - 1 \equiv 0 \mod n$

$p = 7$ $\quad N = P \cdot Q$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

$\mathbb{Z}_n = \{0, \dots, n-1\}$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$\{a \in \{1, \dots, n-1\} \mid a^{n-1} \mod n \neq 1\} \supseteq$

$\{a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1\}$

$(7 \cdot 9)$ N

$N = 1$

1000

$\frac{3}{4}$

1

a

$MCD(a, N)$

$n = 9$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a = 60$, $b = 13$

$a^{n-1} - 1 \equiv 0 \mod n$

$p = 7$ $\quad N = P \cdot Q$ $\quad n \mid a^{n-1} - 1$

$n \cdot \alpha = a^{n-1} - 1$

$\mathbb{Z}_n = \{0, \dots, n-1\}$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$\{a \in \{1, \dots, n-1\} \mid a^{n-1} \bmod n \neq 1\} \supseteq$

$\{a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1\}$

$(7 \cdot 4)$ N

$N = 9$

1000

$\frac{3}{4}$

1 $\to a$

$MCD(a, N)$

$n = 9$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a = 60$, $b = 13$

$a^{n-1} - 1 \equiv 0 \mod n$

$p = 7$ $\quad N = p \cdot q$ $\quad n \mid a^{n-1} - 1$

$n \cdot k = a^{n-1} - 1$

$\mathbb{Z}_n = \{0, \dots, n-1\}$

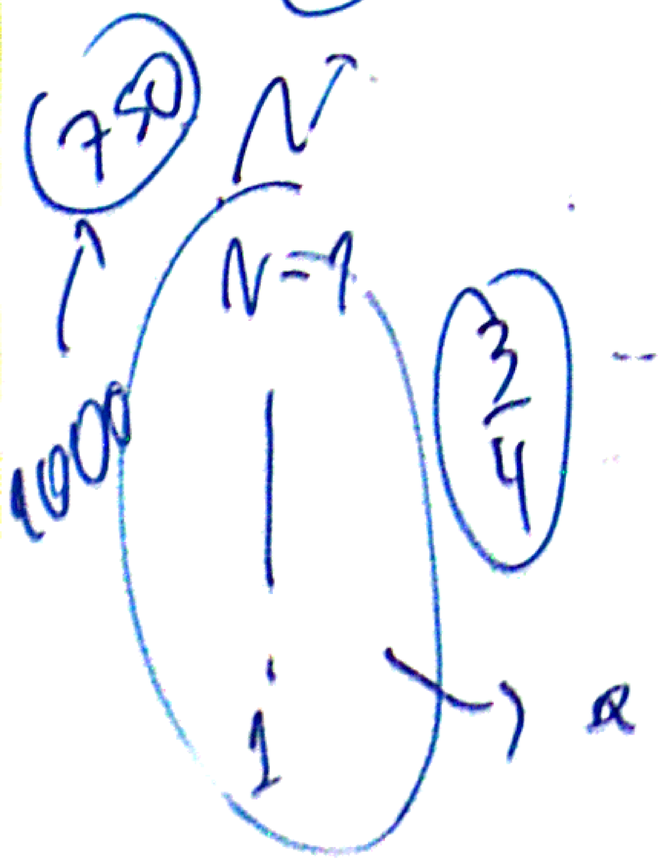
n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$\{a \in \{1, \dots, n-1\} \mid a^{n-1} \bmod n \neq 1\} \supseteq$

$\{a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1\}$

$MCD(a, N)$



$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a = 60$, $b = 13$

$d^{\ } - 1 \equiv 0 \mod n$

$p = 7$ $\quad N = P \cdot Q$

$n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

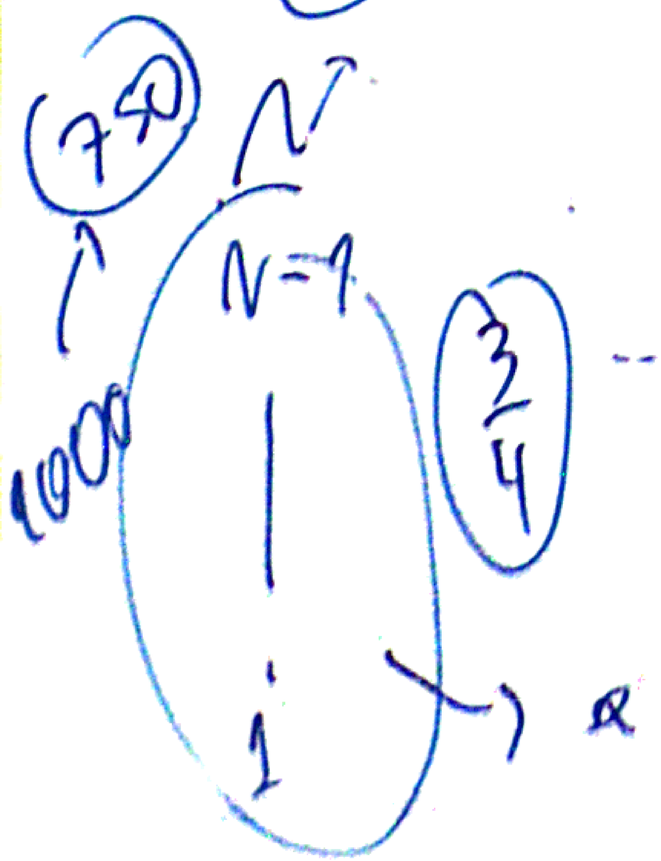
$\mathbb{Z}_n = \{0, \dots, n-1\}$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$\{a \in \{1, \dots, n-1\} \mid a^{n-1} \mod n \neq 1\} \supseteq$

$\{a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1\}$



$MCD(a, N)$

$n = 7$

$3^8 \equiv 1 \mod 9$

$3 \cdot 3^7 \equiv 1 \mod 9$

$a = 60$, $b = 13$

$a^{n-1} - 1 \equiv 0 \mod n$

$p = 7$ $\quad N = p \cdot q$ $\quad n \mid a^{n-1} - 1$

$n \cdot k = a^{n-1} - 1$

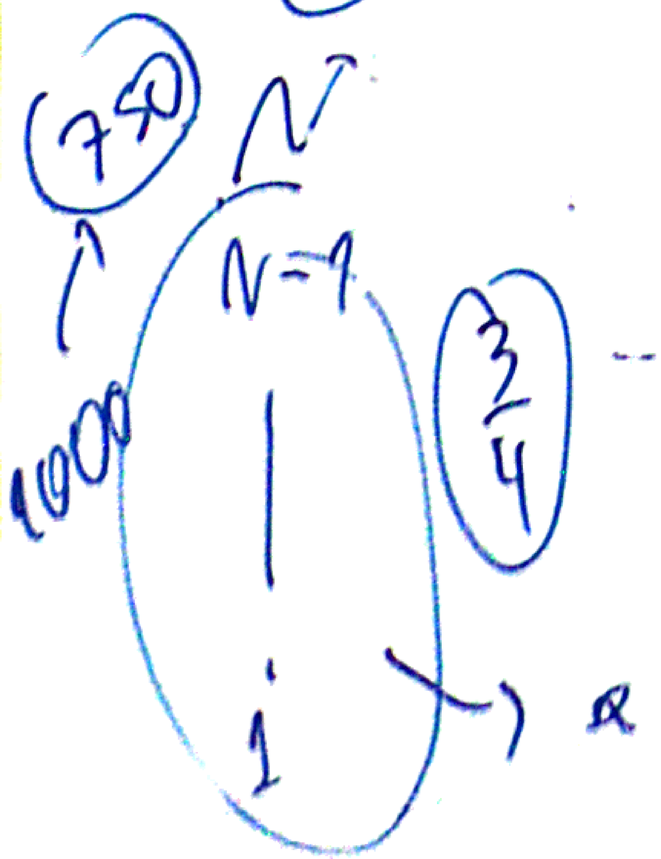
$\mathbb{Z}_n = \{0, \dots, n-1\}$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$\{a \in \{1, \dots, n-1\} \mid a^{n-1} \bmod n \neq 1\} \supseteq$

$\{a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1\}$



$MCD(a, N)$

$a = 60$, $b = 13$ $\quad d - 1 \equiv 0 \mod n$

$\phi(1) = 0$

$\phi(n) = |\mathbb{Z}_n^*|$

$p = 7 \quad N = P \cdot Q \quad n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

$\mathbb{Z}_n = \{0, \dots, n-1\}$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$\{a \in \{1, \dots, n-1\} \mid a^{n-1} \mod n \neq 1\} \supseteq$

$\{a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1\}$

$MCD(a, N)$

$a = 60$, $b = 13$ $\quad d^{\cdot} - 1 \equiv 0 \mod n$

$\phi(1) = 0$

$\phi(n) = |\mathbb{Z}_n^*|$

$p = 7 \quad N = P \cdot Q \quad n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

$\mathbb{Z}_n = \{0, \dots, n-1\}$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$\{a \in \{1, \dots, n-1\} \mid a^{n-1} \mod n \neq 1\} \supseteq$

$\{a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1\}$

$MCD(a, N)$

$a = 60$, $b = 13$ $\quad d - 1 \equiv 0 \mod n$

$\phi(1) = 0$

$\phi(n) = |\mathbb{Z}_n^*|$

$p = 7 \quad N = P \cdot Q \quad n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

$\mathbb{Z}_n = \{0, \dots, n-1\}$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$\{a \in \{1, \dots, n-1\} \mid a^{n-1} \mod n \neq 1\} \supseteq$

$\{a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1\}$

$MCD(a, N)$

$a = 60$, $b = 13$ $\qquad d - 1 \equiv 0 \mod n$

$\phi(1) = 0$ $\qquad p = 7$ $\qquad N = P \cdot Q$ $\qquad n \mid d^{n-1} - 1$

$\phi(n) = |\mathbb{Z}_n^*|$ $\qquad n \cdot \alpha = d^{n-1} - 1$

$\mathbb{Z}_n = \{0, \dots, n-1\}$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$FACT = \{(N, k) \mid$ existe $d: 1 < d \leq k$ y $d \mid N\}$

$a = 60$, $b = 13$ $\qquad d - 1 \equiv 0 \mod n$

$\phi(1) = 0$ $\qquad p = 7$ $\qquad N = P \cdot Q$ $\qquad n \mid d^{n-1} - 1$

$\phi(n) = |\mathbb{Z}_n^*|$ $\qquad n \cdot \alpha = d^{n-1} - 1$

$\mathbb{Z}_n = \{0, \dots, n-1\}$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$FACT = \{(N, k) \mid$ existe $d: 1 < d \leq k$ y $d \mid N\}$

$a = 60$, $b = 13$ $\qquad d - 1 \equiv 0 \mod n$

$\phi(1) = 0$

$\phi(n) = |\mathbb{Z}_n^*|$

$p = 7 \qquad N = p \cdot q \qquad n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

$\mathbb{Z}_n = \{0, \dots, n-1\}$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$FACT = \{(N, k) \mid \text{existe } d: 1 < d \leq k \text{ y } d \mid N\}$

$a = 60$, $b = 13$ $\quad d - 1 \equiv 0 \mod n$

$\phi(1) = 0$

$\phi(n) = |\mathbb{Z}_n^*|$

$p = 7 \quad N = P \cdot Q \quad n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

$\mathbb{Z}_n = \{0, \dots, n-1\}$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$FACT = \{(N, k) / \text{existe } d: 1 < d \leq k \text{ y } d \mid N\}$

(N, k) ✓

$a = 60$, $b = 13$ $\quad d - 1 \equiv 0 \mod n$

$\phi(1) = 0$

$\phi(n) = |\mathbb{Z}_n^*|$

$p = 7 \quad N = p \cdot q \quad n \mid d^{n-1} - 1$

$n \cdot \alpha = d^{n-1} - 1$

$\mathbb{Z}_n = \{0, \dots, n-1\}$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$FACT = \{(N, k) \mid$ existe $d: 1 < d \leq k$ y $d \mid N\}$

(N, k) ✓

$a = 60$, $b = 13$ $\qquad d - 1 \equiv 0 \mod n$

$\phi(1) = 0$ $\qquad p = 7$ $\qquad N = P \cdot Q$ $\qquad n \mid d^{n-1} - 1$

$\phi(n) = |\mathbb{Z}_n^*|$ $\qquad n \cdot \alpha = d^{n-1} - 1$

$\mathbb{Z}_n = \{0, \dots, n-1\}$

n es primo: $\forall a \in \{1, \dots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \dots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$FACT = \{(N, k) \mid$ existe $d: 1 < d \leq k$ y $d \mid N\}$

(N, k) ✓ $\qquad d$

$\phi(1) = 0$

$\phi(n) = |\mathbb{Z}_n^*|$

$N = p_1^{d_1} \cdots p_k^{d_k}$ $\quad (p_1, d_1) \cdots (p_k, d_k)$

n es primo: $\forall a \in \{1, \ldots, n-1\}: a^{n-1} \equiv 1 \bmod n$

n no es primo: $\exists a \in \{1, \ldots, n-1\}: a^{n-1} \not\equiv 1 \bmod n$

FACT $= \{(N, k)$ existe $d: 1 < d \leq k$ y $d \mid N\}$

(N, k) ✓

$\phi(1) = 0$

$\phi(n) = |\mathbb{Z}_n^*|$

$N = p_1^{d_1} \cdots p_k^{d_k}$ $\quad (p_1, d_1) \cdots (p_k, d_k)$

n es primo: $\forall a \in \{1, \ldots, n-1\}: a^{n-1} \equiv 1 \bmod n$

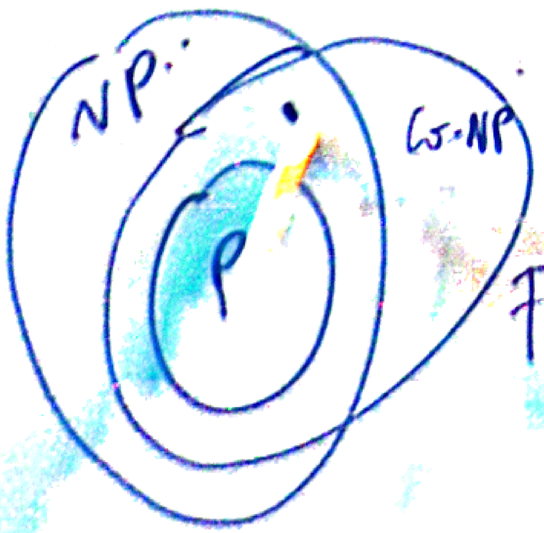
n no es primo: $\exists a \in \{1, \ldots, n-1\}: a^{n-1} \not\equiv 1 \bmod n$

$FACT := \{(N, k) \mid \text{existe } d: 1 < d \leq k \text{ y } d \mid N\}$

(N, k) ✓ $\quad d$

$\phi(1) = 0$

$\phi(n) = |\mathbb{Z}_n^*|$



$N = p_1^{d_1} \cdots p_k^{d_k}$ $\quad (p_1, d_1) \cdots (p_k, d_k)$

n es primo: $\forall a \in \{1, \ldots, n-1\}: a^{n-1} \equiv 1 \bmod n$

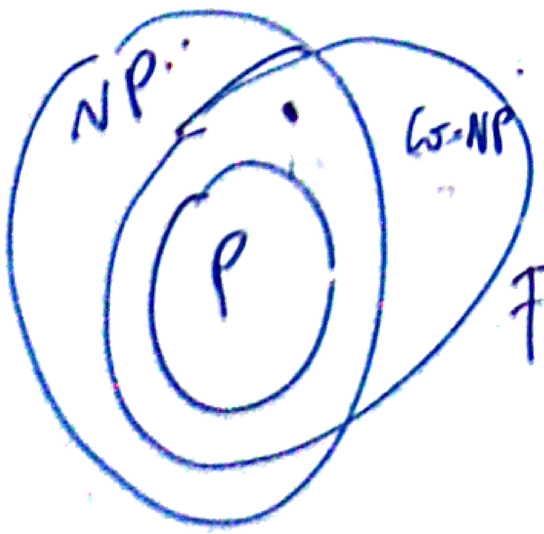
n no es primo: $\exists a \in \{1, \ldots, n-1\}: a^{n-1} \not\equiv 1 \bmod n$

$FACT = \{(N, k) \mid \text{existe } d: 1 < d \leq k \text{ y } d \mid N\}$

(N, k) ✓ $\quad d$

$\phi(1) = 0$

$\phi(n) = |\mathbb{Z}_n^*|$



$N = p_1^{d_1} \cdots p_k^{d_k}$ $\quad (p_1, d_1) \cdots (p_k, d_k)$

n es primo: $\forall a \in \{1, \ldots, n-1\}: a^{n-1} \equiv 1 \mod n$

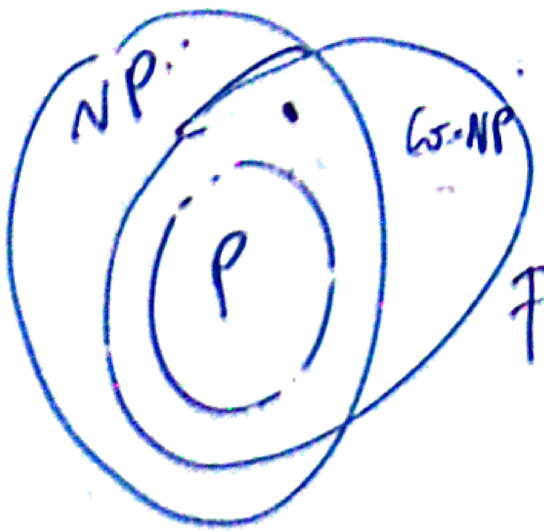
n no es primo: $\exists a \in \{1, \ldots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

FACT $:= \{(N, k) \mid$ existe $d: 1 < d \leq k$ y $d \mid N\}$

(N, k) ✓ $\quad d$

$\phi(1) = 0$

$\phi(n) = |\mathbb{Z}_n^*|$



$N = p_1^{d_1} \cdots p_k^{d_k}$ $\quad (p_1, d_1) \cdots (p_k, d_k)$

n es primo: $\forall a \in \{1, \ldots, n-1\}: a^{n-1} \equiv 1 \mod n$

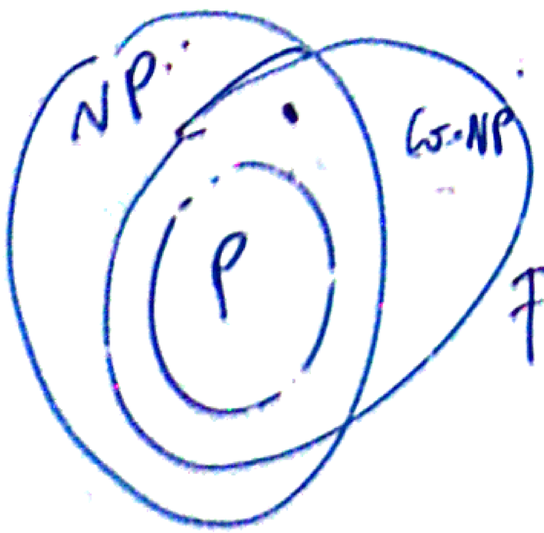
n no es primo: $\exists a \in \{1, \ldots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$FACT := \{(N, k) \mid \text{existe } d: 1 < d \leq k \text{ y } d \mid N\}$

(N, k) ✓ $\quad d$

$\phi(1) = 0$

$\phi(n) = |\mathbb{Z}_n^*|$



$N = p_1^{d_1} \cdots p_k^{d_k}$ $\quad (p_1, d_1) \cdots (p_k, d_k)$

n es primo: $\forall a \in \{1, \ldots, n-1\}: a^{n-1} \equiv 1 \bmod n$

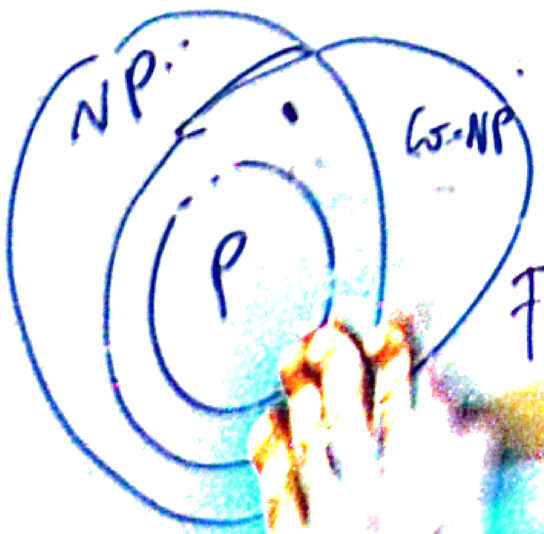
n no es primo: $\exists a \in \{1, \ldots, n-1\}: a^{n-1} \not\equiv 1 \bmod n$

$FACT = \{(N, k) \mid$ existe $d: 1 < d \leq k$ y $d \mid N\}$

(N, k) ✓ $\quad d$

$\phi(1) = 0$

$\phi(n) = |\mathbb{Z}_n^*|$



$N = p_1^{d_1} \cdots p_k^{d_k}$ $\quad (p_1, d_1) \cdots (p_k, d_k)$

n es primo: $\forall a \in \{1, \ldots, n-1\}: a^{n-1} \equiv 1 \bmod n$

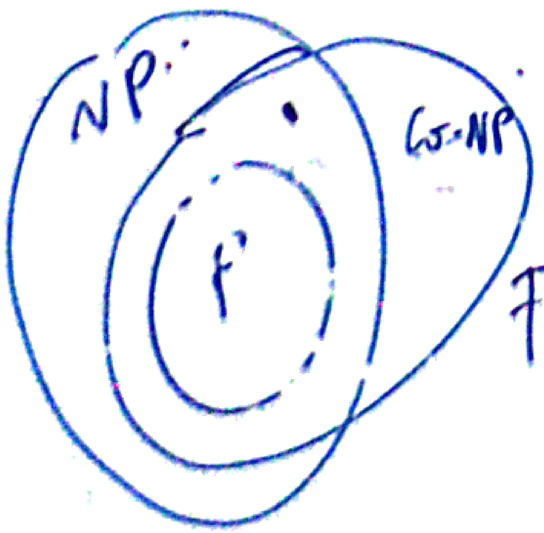
n no es primo: $\exists a \in \{1, \ldots, n-1\}: a^{n-1} \not\equiv 1 \bmod n$

$FACT := \{(N, k) \mid \text{existe } d: 1 < d \leq k \text{ y } d \mid N\}$

(N, k) ✓ $\quad d$

$\phi(1) = 0$

$\phi(n) = |\mathbb{Z}_n^*|$



$N = p_1^{d_1} \cdots p_k^{d_k}$ $\quad (p_1, d_1) \cdots (p_k, d_k)$

n es primo: $\forall a \in \{1, \ldots, n-1\}: a^{n-1} \equiv 1 \bmod n$

n no es primo: $\exists a \in \{1, \ldots, n-1\}: a^{n-1} \not\equiv 1 \bmod n$

$FACT := \{(N, k) \mid \text{existe } d: 1 < d \leq k \text{ y } d \mid N\}$

(N, k) ✓ $\quad d$

$\phi(1) = 0$

$\phi(n) = |\mathbb{Z}_n^*|$

$N = p_1^{d_1} \cdots p_k^{d_k}$ $\quad (p_1, d_1) \cdots (p_k, d_k)$

n es primo: $\forall a \in \{1, \ldots, n-1\}: a^{n-1} \equiv 1 \bmod n$

n no es primo: $\exists a \in \{1, \ldots, n-1\}: a^{n-1} \not\equiv 1 \bmod n$

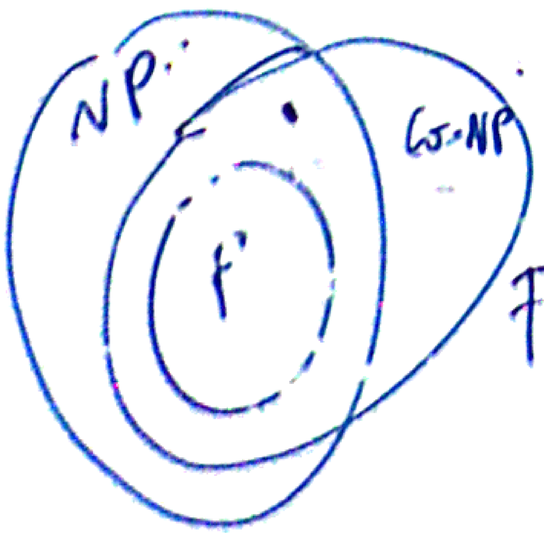
$FACT = \{(N, k) \mid$ existe $d: 1 < d \leq k$ y $d \mid N\}$

(N, k) ✓ $\quad d$

$N = p_1^{d_1} \cdots p_k^{d_k}$ $\quad (p_1, d_1) \cdots (p_k, d_k)$

$\phi(1) = 0$

$\phi(n) = |\mathbb{Z}_n^*|$



n es primo: $\forall a \in \{1, \ldots, n-1\}: a^{n-1} \equiv 1 \bmod n$

n no es primo: $\exists a \in \{1, \ldots, n-1\}: a^{n-1} \not\equiv 1 \bmod n$

$FACT := \{(N, k) \mid \text{existe } d: 1 < d \leq k \text{ y } d \mid N\}$

(N, k) ✓ $\quad d$

$\phi(1) = 0$

$\phi(n) = |\mathbb{Z}_n^*|$

$N = p_1^{d_1} \cdots p_k^{d_k}$ $\quad (p_1, d_1) \cdots (p_k, d_k)$

n es primo: $\forall a \in \{1, \ldots, n-1\}: a^{n-1} \equiv 1 \mod n$

n no es primo: $\exists a \in \{1, \ldots, n-1\}: a^{n-1} \not\equiv 1 \mod n$

$FACT := \{(N, k) \mid$ existe $d: 1 < d \leq k$ y $d \mid N\}$

(N, k) ✓ $\quad d$