$(S, *)$

Def. The identity element e for an operation $*$ is the element such that $e * a = a = a * e$ $\forall$ a in the set.

Def. The inverse element a^{-1} of a for an operator $*$ is the element such that $a^{-1} * a = e = a * a^{-1}$.

0: additive identity in $\mathbb{Z}_n$.

$$w + 0 \equiv 0 + w \equiv w \pmod{n} \ \forall w \in \mathbb{Z}_n.$$

Additive inverse: for each $w \in \mathbb{Z}_n$, there exists $z \in \mathbb{Z}_n$ such that $w + z \equiv 0 \pmod{n}$

$$z \equiv -w \pmod{n}$$
$$\equiv n - w \pmod{n}.$$

$$a - b \stackrel{\wedge}{\equiv} a + (-b) \pmod{n}.$$

$$a - b \triangleq a + (-b) \pmod{n}$$

4. If $(a+b) \equiv (a+c) \pmod{n}$,

then $b \equiv c \pmod{n}$.

$$(-a) + (a+b) \equiv (-a) + (a+c) \pmod{n}.$$

$$\Rightarrow b \equiv c \pmod{n}.$$

1: multiplicative identity in $\mathbb{Z}_n$.

Multiplicative inverse of a : a^{-1}

such that $a \cdot a^{-1} = 1 = a^{-1} \cdot a$.

However not all integers modulo n have a multiplicative inverse.

$\Rightarrow$ division is not necessarily well-defined.

Lemma. If $\gcd(a, n) = 1$, then there exists the multiplicative inverse of a modulo n, a^{-1}, such that $(a^{-1}) \cdot a \equiv 1 \pmod{n}$.

constructive Proof by Extended Euclidean Algorithm

5. Suppose $\gcd(a, n) = 1$.

If $a \times b \equiv a \times c \pmod{n}$,

then $b \equiv c \pmod{n}$.

$\gcd(a, n) = 1 \Rightarrow a^{-1}$ exists

$\underline{(a^{-1}) \times a} \times b \equiv (a^{-1}) \times a \times c \pmod{n}$.

$\Rightarrow b \equiv c \pmod{n}$.

Extended Euclidean Algorithm

Lemma. For $a, b \in \mathbb{Z}$, there exist $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$.

For $\gcd(a, n) = 1$, there exist $x, y \in \mathbb{Z}$ such that $ax + ny = 1$.

$$\Rightarrow \quad ax \equiv 1 \pmod n.$$
$$\Rightarrow \quad x \equiv a^{-1} \pmod n.$$

Proof.

$a = q_1 b + r_1 \Rightarrow r_1 = a - q_1 b. \quad x_1 = 1, \; y_1 = -q_1$

$\qquad = a x_1 + b y_1.$

$b = q_2 r_1 + r_2 \Rightarrow r_2 = b - q_2 r_1$

$r_1 = q_3 r_2 + r_3$

$\qquad = b - q_2 a + q_2 q_1 b$

$\qquad = a(-q_2) + b(1 + q_2 q_1)$

$x_2 = -q_2, \; y_2 = 1 + q_2 q_1$

$\qquad = a x_2 + b y_2.$

$\vdots$

$r_{n-2} = q_n r_n + r_{n-1}$

$ax_n + by_n = r_n$

$= \gcd(a, b)$

#

$r_{n-1} = q_{n+1} r_n + 0$

$r_n = a x_n + b y_n.$

$\boxed{r_n = \gcd(a, b)}$

$r_{i-2} = a x_{i-2} + b y_{i-2}.$

$r_{i-1} = a x_{i-1} + b y_{i-1}$

$\boxed{\begin{aligned} x_i &= x_{i-2} - q_i x_{i-1} \\ y_i &= y_{i-2} - q_i y_{i-1} \end{aligned}}$

$r_i = r_{i-2} - q_i r_{i-1}$

$\quad = a\underbrace{(x_{i-2} - q_i x_{i-1})}_{x_i} + b\underbrace{(y_{i-2} - q_i y_{i-1})}_{y_i}$