Chapter 1.3. Modular Arithmetic

Def. Let $m \geq 1$ be an integer.

The integer a and b are congruent modulo m if $a-b$ is divisible by m.

We write $a \equiv b \pmod{m}$.

modulus

Ex. $17 \equiv 7 \pmod{5}$

$18 \not\equiv 6 \pmod{11}$

Thm. Let $m \geq 1$ be an integer.

i) If $a_1 \equiv a_2 \pmod{m}$ and $b_1 \equiv b_2 \pmod{m}$,

then $a_1 \pm b_1 \equiv a_2 \pm b_2 \pmod{m}$

$a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{m}$

ii) Let a be an integer.

Then, $ab \equiv 1 \pmod{m}$ for some integer b iff $\gcd(a, m) = 1$.

multiplicative inverse of a modulo m.

Ex. Since $2 \cdot 3 \equiv 1 \pmod{5}$, 3 is the inverse of 2 modulo 5. and $\gcd(2,5) = \gcd(3,5) = 1$

Since $7 \cdot 8 \equiv 1 \pmod{11}$, $5/7 \equiv 5 \cdot 8 \equiv 7 \pmod{11}$.

Def. i) $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m = \{0, 1, 2, \cdots, m-1\}$

ring of integers modulo m.

ii) $(\mathbb{Z}/m\mathbb{Z})^* = \mathbb{Z}_m^* = \{a \in \mathbb{Z}_m : \gcd(a, m) = 1\}$

group of units modulo m

iii) $\phi(m) = \#(\mathbb{Z}/m\mathbb{Z})^* = |\{0 \leq a < m : \gcd(a, m) = 1\}|$

Ex. $\mathbb{Z}/7\mathbb{Z} = \{0, 1, 2, \cdots, 6\}$ and $(\mathbb{Z}/7\mathbb{Z})^* = \{1, 2, \cdots, 6\}$

$\phi(7) = 6$