Examples: Find the remainder of 2^{31415} divided by 7.

$2^2 \equiv 4 \pmod 7$

$2^3 \equiv 8 \equiv 1 \pmod 7$

$(2^3)^k \equiv 1^k \equiv 1 \pmod 7$

$31415 = 3 \cdot 10471 + 2$

$2^{31415} \equiv 2^{3 \cdot 10471 + 2} \equiv (2^3)^{10471} \cdot 2^2 \pmod 7$

$\equiv 1 \cdot 4 \pmod 7$

$\equiv 4 \pmod 7$

So the remainder is 4.

Example: Find remainder of 20^{31415} divided by 9.

$20 \equiv 2 \pmod 9$

So $20^{31415} \equiv 2^{31415} \pmod 9$

$2^2 \equiv 4 \pmod 9$

$2^3 \equiv 8 \equiv -1 \pmod 9$

$2^{31415} \equiv (2^3)^{10471} \cdot 2^2$

$\equiv -1 \cdot 4$

$\equiv -4 \pmod 9$

$\equiv 5 \pmod 9$

remainder is 5.

Note: Every int is congruent to exactly one of $0, 1, 2, \ldots, m-1 \pmod m$.

Modular Arithmetic

Definition: The congruence class modulo m of an integer a is the set $[a] = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$.

The set of <u>integers modulo m</u> is

$$\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$$

Example: $m = 5$ $\quad \mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$.

$$[0] = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{5}\} = \{5n \mid n \in \mathbb{Z}\}$$

$$[1] = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{5}\} = \{5n+1 \mid n \in \mathbb{Z}\}$$

$$[2] = \ldots\ldots 2 \ldots\ldots 2 \ldots$$

$$[3] = \ldots\ldots 3 \ldots\ldots 3 \ldots$$

$$[4] = \ldots\ldots 4 \ldots\ldots 4 \ldots$$

Note: $[5] = \{x \in \mathbb{Z} \mid x \equiv 5 \pmod{5}\} = [0]$

$\quad [6] = [1] \ldots\ldots\ldots$

Definitions of operations: For $a, b \in \mathbb{Z}$,

define $[a] + [b] = [a+b]$

$\qquad [a] \cdot [b] = [ab]$

Examples: $m = 5$ $\quad [2] + [3] = [5] = [0]$

$\qquad [2] \cdot [3] = [6] = [1]$

	[0]	[1]	[2]	[3]	[4]
[0]	[0]	--	--	--	--
[1]		[1]			
[2]		|	[4]	[1]	|
[3]		|	[1]	.	|
[4]		.		[2]	[1]

$$[2] + [3] = \{a + b \mid a \in [2], b \in [3]\}$$

$$a \equiv 2 \pmod{5}$$

$$b \equiv 3 \pmod{5}$$

$$a + b \equiv 2 + 3 \equiv 0 \pmod{5} = [0]$$

$[0] = [5] = [10] = [-100] = \cdots$

Proposition: $[a] = [b]$ if and only if $a \equiv b \pmod{m}$

Proof: excersice.

Additive Identity: $[0]$ in $\mathbb{Z}_m$ $\quad [a] + [0] = [a]$

Additive Inverse: Additive Inverse of $[3]$ is $[2]$,
since $[3] + [2] = 0$ [Add. Id.].

Multiplicative Identity: $[1]$ in $\mathbb{Z}_m$. Since $[a] \cdot [1] = [a]$.

Multiplicative Inverse: $[a]^{-1}$ is the element in $\mathbb{Z}_m$ such that $[a] \cdot [a]^{-1} = [1]$.

Example: $\mathbb{Z}_5$

$[1]^{-1} = [1]$

$[2]^{-1} = [3]$ $\quad ([2] \cdot [3] = [1])$

$[3]^{-1} = [2]$

$[4]^{-1} = [4]$

$[0]^{-1} = ???$ $\quad$ no inverse

Example: $\mathbb{Z}_6$

$[5]^{-1} = [5]$ $\quad ([5] \cdot [5] = [25] = [1])$

$[3]^{-1} = \times$ does not exist $\quad [3] \cdot [x] = [3x]$

$3x \not\equiv 1 \pmod{6}$

Not all elements in $\mathbb{Z}_m$ have inverses.