$3^1 \equiv 3 \pmod{12}$

$3^2 \equiv 9 \pmod{12}$

$3^3 \equiv 27 \equiv 3 \pmod{12}$

$3^4 \equiv 9 \pmod{12}$

$\vdots$

Is there always a repeating pattern when we look at

$a^i \pmod{n}$

$i = 1, 2, 3, 4, \ldots$?

<u>Ex</u>: $2^1 \equiv 2 \pmod{12}$

$2^2 \equiv 4 \pmod{12}$

$2^3 \equiv 8 \pmod{12}$

$2^4 \equiv 4 \pmod{12}$

$2^5 \equiv 8 \pmod{12}$

$\vdots$

<u>Ex</u>: $6^1 \equiv 6 \pmod{12}$

$6^2 \equiv 0 \pmod{12}$

$6^3 \equiv 0 \pmod{12}$

$6^4 \equiv 0 \pmod{12}$

$\vdots$

<u>Key idea of these exercises</u>: Any number, when working modulo n, can be replaced with a number between 0 and $n-1$.

3.3: $2^{50} \equiv k \pmod 7$, $0 \le k \le 6$

$2^2 \equiv 4 \pmod 7$

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

$2^4 \equiv 2 \pmod 7$

$50 = 3 \cdot 16 + 2$

$2^5 \equiv 4 \pmod 7$

$2^6 \equiv 1 \pmod 7$

$\vdots$

$2^{48} \equiv 1 \pmod 7$

$2^{49} \equiv 2 \pmod 7$

$\boxed{2^{50} \equiv 4 \pmod 7.}$

Thm 3.14: If a is any integer and $n \ge 1$, $a \equiv t \pmod n$ for some t in $\{0, 1, 2, \ldots, n-1\}$.

Def: The set $\{0, 1, 2, \ldots, n-1\}$ is the canonical complete residue system modulo n

More generally, a complete residue system modulo n is a set so that every integer a is congruent to exactly one t in the set modulo n.

Ex: $n=3$

CCRS: $\{0,1,2\}$

$a \equiv 0 \pmod 3 \iff a = 3k$ for some k

$a \equiv 1 \pmod 3 \iff a = 3k+1$ for some k

$a \equiv 2 \pmod 3 \iff a = 3k+2$ for some k

This encompasses all integers

a non-canonical CRS for $n=3$: $\{-1,0,1\}$

Because $2 \equiv -1 \pmod 3$,

so $a \equiv 2 \pmod 3$

$\iff a \equiv -1 \pmod 3$

Ex: $77^{381} \equiv (-1)^{381} \pmod 3$

$\equiv -1 \pmod 3$

$\equiv 2 \pmod 3.$

$77 = 75 + 2$

$= 78 - 1$