4.1: $2^i \pmod 7$ CCRS $= \{0, 1, \ldots, 6\}$

$2^0 = 1 \equiv 1 \pmod 7$

$2^1 = 2 \equiv 2 \pmod 7$

$2^2 = 4 \equiv 4 \pmod 7$

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

$2^4 = 16 \equiv 2 \pmod 7$ → $2^4 = 2 \cdot 2^3 \equiv 2 \cdot 1 \pmod 7$

$2^5 = 32 \equiv 4 \pmod 7$

$2^6 = 64 \equiv 1 \pmod 7$

$3^i \pmod 7$

$3^0 \equiv 1 \pmod 7$

$27 = 21 + 6$

$3^1 \equiv 3 \pmod 7$

$3^2 = 9 \equiv 2 \pmod 7$

$3^3 = 3^2 \cdot 3 \equiv 2 \cdot 3 \equiv 6 \pmod 7$

$3^4 = 81 = 77 + 4$

$3^4 = 3^2 \cdot 3^2 \equiv 2 \cdot 2 \equiv 4 \pmod 7$

$3^5 = 3 \cdot 3^4 \equiv 3 \cdot 4 \equiv 12 \equiv 5 \pmod 7$

$3^6 = 3 \cdot 3^5 \equiv 3 \cdot 5 \equiv 15 \equiv 1 \pmod 7$

You'll prove (4.6): If $(a, n) = 1$, then

$$a^k \equiv 1 \pmod{n}$$

for some natural number $k \geq 1$

The smallest such k is the order of a modulo n.

is $\text{ord}_n(a)$

$2^1 \not\equiv 1 \pmod 7$
$2^2 \not\equiv 1 \pmod 7$ $\longrightarrow$ $\text{ord}_7(2) = 3$
$2^3 \equiv 1 \pmod 7$

$3^1 \not\equiv 1 \pmod 7$
$3^2 \not\equiv 1 \pmod 7$ $\longrightarrow$ $\text{ord}_7(3) = 6$
$\vdots$
$3^5 \not\equiv 1 \pmod 7$
$3^6 \equiv 1 \pmod 7$

$(a, n) \neq 1$

$2^i \pmod 6$:

$2^0 \equiv 1 \pmod 6$
$2^1 \equiv 2 \pmod 6$
$2^2 \equiv 4 \pmod 6$
$2^3 \equiv 2 \pmod 6$
$2^4 \equiv 4 \pmod 6$
$\vdots$

$\text{ord}_6(2)$ is NOT Defined

Thm 4.5 = Thm 1.45 will be useful.