② For a linear congruential generator, we know that,

$$X_{i+1} = (aX_i + c) \bmod (m)$$

If $c = 0$,

$$X_{i+1} = (aX_i) \bmod (m)$$

$$X_{i+2} = (aX_{i+1}) \bmod (m)$$

$$= \Big(a\big(aX_i \bmod (m)\big)\Big) \bmod (m)$$

If $u = (aX_i) \bmod (m)$, then, $u = aX_i \pm mk_1,\ k \in \mathbb{Z}$

Therefore, $X_{i+2} = \big(a(aX_i \pm mk_1)\big) \bmod (m)$

$$= (a^2X_i \pm mk_1) \bmod (m)$$

$$X_{i+2} = a^2X_i \pm mk_1 \pm mk_2$$

$$= a^2X_i \pm mk$$

$$\Rightarrow X_{i+2} = (a^2X_i) \bmod (m)$$

As we increase the value of "n" in X_{i+n}, we

As we increase
get a pattern of,

$$X_{i+n} = (a^n X_n) \bmod (m).$$

We get the above result by inductive property.
For a more formal inductive proof, replace two with "k+1."

(b) We need to prove,

$$(a^n X_i) \bmod (m) = ((a^n \bmod (m)) X_i) \bmod (m)$$

$$u = (a^n X_i) \bmod (m)$$

$$\Rightarrow u = a^n X_i \pm mk$$

$$= a^n X_i \pm m(k_1 + k_2)$$

$$= a^n X_i \pm mk_1 \pm mk_2$$

$$= ((a^n X_i) \bmod (m)) \bmod (m)$$

(Integers can be represented as an addition or subtraction of multiple integers
(6=3+3, 6=4+2, 6=7-1))

$$u = (a^n X_i) \bmod (m)$$

$$= a^n X_i \pm mk$$

$$= X_i \left(a^n \pm \frac{mk}{X_i}\right)$$

Since "X_i" is an integer, $\frac{mk}{X_i}$ is also an integer.

$$\therefore u = X_i\left(\left(a^n\right) \bmod (m)\right)$$

Inserting this in the previous equation obtained, we get,

$$u = \left(\left(a^n \bmod (m)\right) X_i\right) \bmod (m)$$

ⓒ Given $X_{i+1} = (19 X_i) \bmod (100)$, $X_0 = 63$.

$$X_1 = (19 X_0) \bmod (100)$$
$$= (19 \times 63) \bmod (100)$$
$$= (1197) \bmod (100)$$
$$= 97$$

$$X_2 = (19 \times X_1) \bmod (100)$$

$X_2 = (19 \times X_1) \bmod (100)$

$= (19 \times 97) \bmod (100)$

$= (1843) \bmod (100)$

$= 43$

$X_3 = (19 \times 43) \bmod (100)$

$= (817) \bmod (100)$

$= 17$

$X_4 = (19 \times 17) \bmod (100)$

$= (323) \bmod (100)$

$= 23$

$X_5 = (19 \times 23) \bmod (100)$

$= (437) \bmod (100)$

$= 37$

Now, calculating using the result from part b,

$X_1 = (19^1 X_0) \bmod (100)$

$a = 19$

$$X_5 = \left(19^5 \bmod (100) \times X_0\right) \bmod (100)$$

$$= (99 \times X_0) \bmod (100)$$

$$= (99 \times 63) \bmod (100)$$

$$= (6237) \bmod (100)$$

$$= 37$$

We get the same value for X_5 using both the methods.