Ex: What is the remainder when $22 \cdot 19$ is divided by 3?

Recall: Remainder is the unique $r \in \mathbb{Z}$ such that $0 \le r \le 2$ and $22 \cdot 19 \equiv r \mod 3$.

$22 \equiv 1 \mod 3$, $\quad 19 \equiv 1 \mod 3$,

So $$\begin{aligned} 22 \cdot 19 &\equiv 1 \cdot 1 \mod 3 \\ &\equiv 1 \mod 3, \end{aligned}$$

meaning $22 \cdot 19$ leaves a remainder of 1 when divided by 3.

Ex: What is the remainder when

$$(754 + 1083) \cdot 17$$

is divided by 5?

$$\begin{aligned} (754 + 1083) \cdot 17 &\equiv (4 + 3) \cdot 2 \mod 5 \\ &\equiv 7 \cdot 2 \mod 5 \\ &\equiv 2 \cdot 2 \mod 5 \\ &\equiv 4 \mod 5 \end{aligned}$$

So the remainder is 4.

Ex: When $m=2$, every $a \in \mathbb{Z}$ satisfies exactly one of

- $a \equiv 0 \mod 2$ $\iff$ a is even
- $a \equiv 1 \mod 2$ $\iff$ a is odd

So when we do arithmetic mod 2, we can replace every integer by 0 or 1.

We have

$0+0=0$ $\qquad$ $0 \cdot 0 = 0$

$0+1=1$ $\qquad$ $0 \cdot 1 = 0$

$1+0=1$ $\qquad$ $1 \cdot 0 = 0$

$1+1=2 \equiv 0 \mod 2$ $\qquad$ $1 \cdot 1 = 1$

So we have the following $+$ and $\cdot$ tables:

$+$ mod 2	0	1
0	0	1
1	1	0

$\cdot$ mod 2	0	1
0	0	0
1	0	1

This recovers

+	even	odd
even	even	odd
odd	odd	even

$\cdot$	even	odd
even	even	even
odd	even	odd

<u>**Note**</u>: Can make similar tables for arithmetic modulo 3, 4, 5, ...

Thm: Let $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. If

$$a \equiv b \mod m$$

then

$$a^n \equiv b^n \mod m$$

for every $n \in \mathbb{N}$.

Proof: Let $P(n)$ be "$a^n \equiv b^n \mod m$."
We'll use induction.

Base Case: $P(1)$ is given.

Inductive Step: Let $n \in \mathbb{N}$ and suppose $P(n)$ is true. That is, $a^n \equiv b^n \mod m$.

Since $a \equiv b \mod m$, we get

$$a^n \cdot a \equiv b^n \cdot b \mod m,$$

i.e., $a^{n+1} \equiv b^{n+1} \mod m$. So $P(n+1)$ is true.

Thus, $P(n)$ is true for all $n \in \mathbb{N}$ by P.M.I. ∎

Ex: What is the remainder when 91^{100} is divided by 3?

Since $91 \equiv 1 \mod 3$, we have

$$91^{100} \equiv 1^{100} \mod 3$$
$$\equiv 1 \mod 3.$$

So the remainder is 1.

Ex: What is the remainder when 92^{100} is divided by 3?

Similarly, $92 \equiv 2 \mod 3$, so

$$92^{100} \equiv 2^{100} \mod 3.$$

Now, $2^2 \equiv 1 \mod 3$, so

$$2^{100} \equiv (2^2)^{50} \mod 3$$
$$\equiv 1^{50} \mod 3$$
$$\equiv 1 \mod 3.$$

Thus, the remainder is 1.

Ex: What is the remainder when 258^{50} is divided by 5?

Since $258 \equiv 3 \mod 5$, we have

$$258^{50} \equiv 3^{50} \mod 5.$$

Now, $3^4 = 81$, so $3^4 \equiv 1 \mod 5$.

Write

$$50 = 4 \cdot 12 + 2. \quad \text{(50 divided by 4)}$$

Then

$$3^{50} = 3^{4 \cdot 12 + 2} = (3^4)^{12} \cdot 3^2,$$

so

$$\begin{aligned} 258^{50} &\equiv 3^{50} \\ &\equiv (3^4)^{12} \cdot 3^2 \mod 5 \\ &\equiv 1^{12} \cdot 9 \mod 5 \\ &\equiv 4 \mod 5. \end{aligned}$$

The remainder is 4.