Modular Arithmetic

Usually, when we perform division, we focus on the quotient and the remainder is an afterthought.
Modular arithmetic: Only care about the remainder.

Definition (mod as an operator):
Given $n \in \mathbb{N}$ and $x \in \mathbb{Z}$, if $x = q \cdot n + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r \leq n-1$ then we say that $x \bmod n = r$.

Examples:

$11 \bmod 4 = 3$ as $11 = 2 \cdot 4 + 3$

$77 \bmod 3 = 2$ as $77 = 25 \cdot 3 + 2$

$957 \bmod 10 = 7$ as $957 = 95 \cdot 10 + 7$

Modular Arithmetic

Definition (Congruence modulo n):
We say that $x \equiv y \bmod n$ if $n \mid (y-x)$
i.e. $\exists q \in \mathbb{Z}\ (y = x + qn)$.
Note: We can also write $x \equiv_n y$.
Examples:
$24 \equiv 4 \bmod 5$ as $5 \mid (24-4)$.
$31 \equiv 19 \bmod 6$ as $6 \mid (31-19)$.
$100 \equiv 16 \bmod 21$ as $100 - 16 = 84$ and $21 \mid 84$.
Note: mod n and congruence mod n are closely related but not the same thing!

Correct:
$20 \bmod 7 = 6$
$30 \equiv 19 \bmod 11$

Incorrect:
$20 \bmod 7 \equiv 6$
$30 = 19 \bmod 11$
$30 \bmod 11 = 19$
$19 \bmod 11 = 8$
$30 \bmod 11 = 8$

Consistency of Addition and Multiplication Mod n

Important fact about arithmetic modulo n: If we replace x by x' where $x' \equiv x \bmod n$ then we will get the same answer.

Lemma: If $x' \equiv x \bmod n$ and $y' \equiv y \bmod n$ then $x'+y' \equiv x+y \bmod n$ and $x'y' \equiv xy \bmod n$.

Proof: If $x' \equiv x \bmod n$ and $y' \equiv y \bmod n$ then

$\exists q_1, q_2 \in \mathbb{Z}\ (x' = x + q_1 n \wedge y' = y + q_2 n)$

$x' + y' = x + q_1 n + y + q_2 n = (x+y) + (q_1+q_2)n$

So $x'+y' \equiv x+y \bmod n$

$x'y' = (x+q_1 n)(y+q_2 n) = xy + xq_2 n + q_1 n y + q_1 q_2 n^2$

$= xy + (xq_2 + q_1 y + q_1 q_2 n)n$

$x'y' \equiv xy \bmod n$

The Ring Z_n

A ring is a set together with + and × operations (which have the usual properties)

Example: $\mathbb{Z}$

Definition: The ring $\mathbb{Z}_n$ consists of the elements $\{0, 1, \ldots, n-1\}$ where $\forall x, y \in \mathbb{Z}_n$, $x+y = (x+y) \bmod n$ and $xy = xy \bmod n$.

Example: Times table for $\mathbb{Z}_7$:

	×0	×1	×2	×3	×4	×5	×6
×0	0	0	0	0	0	0	0
×1	0	1	2	3	4	5	6
×2	0	2	4	6	1	3	5
×3	0	3	6	2	5	1	4
×4	0	4	1	5	2	6	3
×5	0	5	3	1	6	4	2
×6	0	6	5	4	3	2	1

Note: When working in $\mathbb{Z}_n$, we should note this.

Example: In $\mathbb{Z}_7$, $4 \cdot 3 = 5$.

In $\mathbb{Z}_n$, $x' = x \iff x' \equiv x \bmod n$

Note: $\mathbb{Z}_n$ can also be written as $\mathbb{Z}/n\mathbb{Z}$.