Fact: the modulus gives an equivalence relation. We will not prove this fact, but if you have never checked the three properties, you should!

Lemma: (equivalences) For $m, n \in \mathbb{Z}$,

the following are equivalent:

1) $m \equiv n \mod k$ for $k \in \mathbb{N}$

2) $[m] = [n]$ $(\text{mod } k)$

3) The remainders upon division by k of m and n are the same.

4) $[m] \cap [n] \neq \emptyset$ $(\text{mod } k)$

proof: $1) \Rightarrow 2)$ Since $m \equiv n \mod k$,

we know $k \mid (m-n)$.

Then $\exists\ a \in \mathbb{Z}$,

$ak = m - n$, and so

$m = n + ak$

$\Rightarrow m \in [n]$.

Similarly, since $n - m = -ak$,

$n \in [m]$.

Therefore, $[n] = [m]$.

2) $\Rightarrow$ 3) Suppose $[n]=[m]$.

Then this means that if

$b \in \{0,1,2,\ldots,k-1\}$ is

the remainder upon dividing

n by k, then

$[n]=[b]$. But

$[n]=[m]$, so

$[m]=[b]$. By

definition of the remainder,

b is the remainder upon

dividing m by k.

3) $\Rightarrow$ 4) Suppose the remainders, upon division by k, of m and n are equal to b.

Then

$$b \in [n] \text{ and } b \in [m]$$

$$\Rightarrow [n] \cap [m] \neq \emptyset.$$

4) $\Rightarrow$ 1) Suppose $[n] \cap [m] \neq \emptyset$.

Let $c \in [n] \cap [m]$.

Then $n \equiv c \bmod k$ and $m \equiv c \bmod k \Rightarrow$

$$n \equiv m \bmod k.$$

$\square$

Observation: any two equivalence classes are either disjoint (have empty intersection) or equal!

Corollary: (residue classes) For $k \in \mathbb{N}$, $k \geq 2$, $\exists$ exactly k equivalence classes, modulo k:

$$[0], [1], [2], \ldots, [k-2], [k-1].$$

Proof: Immediate from the previous proposition: any $n \in \mathbb{Z}$ has $[n] = [b]$ where b is the remainder upon division of n by k, and there are exactly k choices for $b \in \mathbb{Z}$, $0 \leq b < k$.

$\square$

Lemma: (addition and multiplication)

Let $k \in \mathbb{N}$, $k \geq 2$. Then if $m, n \in \mathbb{Z}$ and $m', n' \in \mathbb{Z}$ with $m = m' \bmod k$ and $n = n' \bmod k$, then

$$m + n \equiv (n' + m') \bmod k \quad \text{and}$$

$$m \cdot n \equiv (n' \cdot m') \bmod k, \text{ i.e.},$$

addition and multiplication of equivalence classes is well-defined:

$$[m+n] = [m'+n']$$

$$[m \cdot m] = [m' \cdot n']$$

proof:

$$(m+n)-(m'+n')$$

$$=(m-m')+(n-n').$$

Since $m \equiv m' \bmod k$, $n \equiv n' \bmod k$,

then $\exists$ $a, b \in \mathbb{Z}$ with

$$m-m' = ak, \quad n-n' = bk.$$

Then

$$(m+n)-(m'+n') = ak+bk = (a+b)k$$

$$\Rightarrow \quad m+n \equiv (m'+n') \bmod k.$$

$$m\cdot n - m'n' = mn \underbrace{-(mn') + (mn')}_{=0} - m'n'$$

$$m\cdot n - m'\cdot n' = m(n-n') + (m-m')n'$$

With a and b as above,

$$m\cdot n - m'\cdot n' = m(bk) + (ak)n'$$

$$= (mb + an')k$$

$$\Rightarrow \quad m\cdot n = m'\cdot n' \mod k.$$

$\square$

Definition: ($\mathbb{Z}_n$) Denote by $\mathbb{Z}_n$ the collection of all equivalence classes of $\mathbb{Z}$, modulo n.

Then we may define two operations on $\mathbb{Z}_n$, "+" and "$\cdot$", by, for $[m], [k] \in \mathbb{Z}_n$,

$$\boxed{\begin{aligned} [m]+[k] &= [m+k] \\ [m]\cdot[k] &= [m\cdot k]. \end{aligned}}$$

Observations: (ring properties)

$\mathbb{Z}_n$, with "$+$" and "$\cdot$" as defined previously, satisfies

1) "$+$" is commutative on $\mathbb{Z}_n$

2) "$+$" is associative on $\mathbb{Z}_n$

3) $\forall [m] \in \mathbb{Z}_n$, $[m]+[0]=[m]$,

so zero is a neutral element for "$+$".

4) If $m \in \mathbb{Z}$, then

$$[m]+[-m]=[0]$$

So $[-m]$ is the "inverse" of $[m]$ with respect to "$+$".

5) "$\cdot$" is commutative on $\mathbb{Z}_n$

6) "$\cdot$" is associative on $\mathbb{Z}_n$

7) "$\cdot$" distributes over "$+$":

if $m, k, l \in \mathbb{Z}$,

$$[m] \cdot ([k] + [l]) = [m] \cdot [k] + [m] \cdot [l]$$

8) If $m \in \mathbb{Z}$, $[1] \cdot [m] = [m]$,

so $[1]$ is a neutral element for "$\cdot$" on $\mathbb{Z}_n$.

Example 2: (calculation in $\mathbb{Z}_n$)

Let $n=3$.

Then

$$[74]+[49] \pmod 3$$

$$= [2]+[1] = [3)$$

$$= [0]$$

$$[74]\cdot[49] \pmod 3$$

$$= [2]\cdot[1]$$

$$= [2]$$

Theorem: (Chinese remainder) Suppose $m, n \in \mathbb{N}$, $m, n \geq 2$, and $\gcd(m, n) = 1$. Then if $a, b \in \mathbb{Z}$, $\exists$ $s \in \mathbb{Z}$ such that

$$s \equiv a \bmod m$$

and

$$s \equiv b \bmod n.$$

s is unique up to equivalence modulo mn.

proof: Since $\gcd(m,n)=1$, $\exists$ $k,t \in \mathbb{Z}$ with

$$1 = km + tn.$$

Let $s_1 = 1 - km = tn$.

Let $s_2 = 1 - tn = km$.

Let $s = as_1 + bs_2$.

$$[s]_m = [as_1]_m + [bs_2]_m$$

$$[s]_m = [a]_m [s_1]_m + [b]_m [s_2]_m$$

But $[s_2]_m = [km]_m = [0]_m$.

Also,

$$[s_1]_m = [1-km]_m$$
$$= [1]_m + [-km]_m$$
$$= [1]_m + [0]_m$$
$$= [1]_m$$

So $[s]_m = [a]_m [s_1]_m + [b]_m [s_2]_m$
$$= [a]_m [1]_m + [b]_m [0]_m$$
$$= [a]_m$$

$\Rightarrow s \equiv a \mod m$.

Similarly, $s \equiv b \bmod n$.

Now suppose $\exists\, s' \in \mathbb{Z}$,

$$s' \equiv b \bmod n$$

$$s' \equiv a \bmod m$$

Then

$s - s'$ is divisible by both

n and m, so

$$[s - s']_{nm} = [0]_{nm}.$$

$\square$