Exercise. @
Prove $a-1 \mid a^n - 1$ $(n \geq 1, a \neq 0)$.
Hint: $((a-1)+1)^n$ with binomial theorem.
(Useful for assignment.)

Recall last time:
$a \equiv b \pmod n \Leftrightarrow$ same remainder when divided by n.
$\Leftrightarrow n \mid a-b$.

Proposition.
Congruence mod n is an equivalence relation.
proof.
(1) $a \equiv a \pmod n$ since $a-a=0$ so $n \mid a-a$. (anything divides 0).
(2) If $a \equiv b \pmod n$ then $n \mid a-b$ so $n \mid b-a$ so $b \equiv a \pmod n$.
(3) If $a \equiv b$, $b \equiv c \pmod n$ then $n \mid a-b$ and $n \mid b-c$.
Hence, $a-b = ns$, $b-c = nt$ some $s, t \in \mathbb{Z}$.
So, $nt + ns = b-c+a-b$
$n(t+s) = a-c$.
So $n \mid a-c$. Thus $a \equiv c \pmod n$. □

Notation: Equivalence class of x mod n is denoted
$[x]_n = \{y \in \mathbb{Z} \mid x \equiv y \pmod n\}$
$= \{y \in \mathbb{Z} \mid n \mid x-y\}$.

ex. $[0]_5 = \{\ldots, -10, -5, 0, 5, 10, 15, \ldots\}$
$[1]_5 = \{\ldots, -4, 1, 6, 11, 16, \ldots\}$

In fact, $[x]_n = \{x + nt \mid t \in \mathbb{Z}\}$.

def. Any element of $[x]_n$ is called a representative of that class.

ex. 2, 7, −3 are all representative of $[2]_5$ and $[2]_5 = [7]_5 = [-3]_5$ etc.

Usually, we choose representations in range $0, 1, \ldots, n-1$ so there are exactly n equivalence classes mod n, $[0], [1], \ldots, [n-1]$.

def. The integers mod n, denoted $\mathbb{Z}/n\mathbb{Z}$, is the set of these classes.
$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$.

Note: $|\mathbb{Z}/n\mathbb{Z}| = n$, finite set.
$[n]_n = [0]_n$.

Alison Li

Operations on $\mathbb{Z}/n\mathbb{Z}$

We define addition/multiplication as functions:
$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $[a]+[b] = [a+b]$
$[a][b] = [ab]$
i.e. it is usual addition/multiplication using using representatives.

ex. In $\mathbb{Z}/5\mathbb{Z}$:
$[2]+[1] = [3]$
$[2]+[3] = [5] = [0]$
$[2]+[4] = [6] = [1]$
$[2][3] = [6] = [1]$
$[2][4] = [8] = [3]$

Issue.
If you use different representatives to carry out the operation, is the result the same?
ex. $[2]+[1] = [7]+[11] = [18] = [3]$.
$[2][3] = [-3][8] = [-24] = 1$.
That is, are the operations well-defined? Yes, need to prove.

Lemma.
If $a \equiv c \pmod n$, $b \equiv d \pmod n$, then
(1) $a+b \equiv c+d \pmod n$
(2) $ab \equiv cd \pmod n$.
Hence,
$[a]+[b] = [c]+[d]$
$[a][b] = [c][d]$
i.e. the operations are well-defined.
proof.
We know $n|a-c$ so $a-c = ns$ and $n|b-d$ so $b-d = nt$ some $s,t \in \mathbb{Z}$
(1) $ns+nt = (a-c)+(b-d) = (a+b)-(c+d)$ so $n|(a+b)-(c+d)$.
so $a+b \equiv c+d \pmod n$.
(2) Have $a-c = ns$. (Want to show $ab-cd = n$).
$ba-bc = bns$
$cb-cd = cnt$
$(ab-bc)+(cb-cd) = ab-cd = n(bs+ct)$
So, $n|ab-cd$ so $ab \equiv cd \pmod n$. □

ex. Write down addition/multiplication tables for $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$.

$\mathbb{Z}/4\mathbb{Z}$:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}/2\mathbb{Z}$:

+	0	1
0	0	1
1	1	0

XOR

·	0	1
0	0	0
1	0	1

AND

def. Subtraction is defined by
$[a]-[b] = [a]+[-1][b]$
$= [a]+[-b]$.

Properties of addition/multiplication
Most usual properties are true.
For example,
$[1][a] = [a]$
$[0]+[a] = [a]$
$[0][a] = [0]$
$[a]([b]+[c]) = [a][b]+[a][c]$
Interestingly,
$[a]^n = [a][a]\cdots[a]$ (n times)
proof. Exercise ☺ by induction, $n \geq 0$.

Caution: If $[a][b] = [0]$, this does not imply $[a] = [0]$ or $[b] = [0]$.
e.g. $[2]_4[2]_4 = [4]_4 = [0]_4$.

Inverses and Division

def. $[m] \in \mathbb{Z}/n\mathbb{Z}$ is invertible if $\exists\, [x] \in \mathbb{Z}/n\mathbb{Z}$ such that $[m][x] = [1]$.

ex. $[2]_5[3]_5 = [6]_5 = [1]_5$
So $[2]_5, [3]_5$ are invertible.

ex. $[2]_4$ is not invertible since
$[2][0] = [0]$
$[2][1] = [2]$
$[2][2] = [0]$
$[2][3] = [2]$
None of the possible choices for $[x]$ work.

Lemma.
If $[m][x] = [1]$ and $[m][y] = [1]$ then $[x] = [y]$. (Inverse is unique).
proof #1.
We have $[mx] = [1]$. Hence, n divides $1-mx$, so $ns = 1-mx$ for some integer s. Similarly $nt = 1-my$ for some integer t. Then $yns = y-ymx$, and substituting $ym = 1-nt$ gives $yns = y-(1-nt)x$. Rearrange this to $n(ys-tx) = y-x$. Hence, $n \mid y-x$ and so y is equivalent to $x \pmod n$, hence $[x] = [y]$. □
proof #2.
We have $[m][x] = [1]$, $[m][y] = [1]$.
Multiply $[m][x] = [1]$ by $[y]$.
Then $[y][m][x] = [y][1]$
$([m][y])[x] = [y \cdot 1]$
$[1][x] = [y]$
So $[x] = [y]$. □

def. The inverse of $[m]$ is denoted $[m]^{-1}$ (if it exists).

Caution: $[m^{-1}]$ (i.e. $[\frac{1}{m}]$) is undefined since $\frac{1}{m} \notin \mathbb{Z}$.

Proposition.
$[m]$ in $\mathbb{Z}/n\mathbb{Z}$ invertible $\Leftrightarrow$ $\gcd(m,n) = 1$
Further, if $1 = mx + ny$ for $x, y \in \mathbb{Z}$ then $[m]^{-1} = [x]$.

proof.
($\Rightarrow$) Assume $[m][x] = [1]$ some $[x]$. (i.e $[m]^{-1} = [x]$)
Then $mx \equiv 1 \pmod n$ so $n \mid 1 - mx$ so $ny = 1 - mx$, some $y \in \mathbb{Z}$.
So $1 = mx + ny$. Hence, $\gcd(n, m) = 1$.
($\Leftarrow$) Assume $\gcd(m,n) = 1$.
Then $1 = mx + ny$ some x, y. (Bézout's identity)
So $1 - mx = ny$, so $n \mid 1 - mx$.
So $1 \equiv mx \pmod n$ so $[1] = [mx] = [m][x]$ so $[m]$ invertible where $[m]^{-1} = [x]$.
Further, if $1 = mx + ny$, so $[1] = [mx + ny]$
$[1] = [m][x] + [n][y]$
$[1] = [m][x] + [0][y] = [m][x]$. □

def. If $[m]$ invertible, then division by $[m]$ defined by
$$\frac{[k]}{[m]} = [k][m]^{-1}.$$

ex. Find $[17]^{-1}$ in $\mathbb{Z}/20\mathbb{Z}$, compute $\frac{[4]}{[17]}$.

Run Euclid:
$\gcd(20,17)$: $20 = 1(17) + 3$ ↑ $1 = -17 + 6(20 - 17) = 6 \cdot 20 - 7 \cdot 17$
$\gcd(17,3)$: $17 = 3(5) + 2$ ↑ $1 = 3 - (17 - 5 \cdot 3) = -17 + 6 \cdot 3$
$\gcd(3,2)$: $3 = 2 + 1$ ↑ $1 = 3 - 2$

So $[17]^{-1} = [-7]$.
Verify:
$[17][-7] = [-3][-7] = [21] = [1]$.
Then divide:
$$\frac{[4]}{[17]} = [4][17]^{-1} = [4][-7] = [-28] = [12].$$