Divisibility in $\mathbb{Z}_n$.

We want to determine when $[a]$ divides $[b]$ in $\mathbb{Z}_n$, which means that there is some $[x] \in \mathbb{Z}_n$ such that $[a][x] = [b]$. This means that there is some $x \in \mathbb{Z}$ such that $ax \equiv b \pmod{n}$. The multiplication tables for $n = 7, 8, 9$ will be useful in the study of examples.

$\cdot$	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

$\cdot$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

$\cdot$	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

Definition 1. An element u of a number system (like $\mathbb{Z}_n$) is a ***unit*** if it divides 1. (This means that there is some v such that $uv = 1$.) An element z is a 0***-divisor*** if it divides 0 in a nontrivial way: there is a nonzero element w such that $zw = 0$.

Exercises.

1. For $n = 6, 7, 8, 9$, find the elements that are:

n	units	0-divisors	neither	both
6				
7				
8				
9				

2. Make some conjectures about the answers for other $\mathbb{Z}_n$. (How many of each kind are there? How do you find them?)

Finding units in $\mathbb{Z}_n$, testing for divisibility

To find if $[u]$ is a unit in $\mathbb{Z}_n$, we must find if $ux \equiv 1 \pmod{n}$ is solvable in $\mathbb{Z}$, equivalently whether there is a $y \in \mathbb{Z}$ such that $ux + ny = 1$. If we find such x and y, then $[x] = [u]^{-1}$ in $\mathbb{Z}_n$.

More generally, to find if $[a]$ divides $[c]$ in $\mathbb{Z}_n$ we must find if there is an $x \in \mathbb{Z}$ such that $ax \equiv c \pmod{n}$, equivalently whether there is a $y \in \mathbb{Z}$ such that $ax + ny = c$.

Theorem 2. *$ax \equiv c \pmod{n}$ is solvable iff $\gcd(a, n)$ divides c.*

Exercises.

1. How many units does $\mathbb{Z}_n$ have?

2. Find all units of $\mathbb{Z}_{20}$.

3. Find the inverse of each unit in $\mathbb{Z}_{20}$.

4. Find $[24]^{-1}$ in $\mathbb{Z}_{143}$.