- Problem DM-3.7-16(b) Problem DM-3.7-16(a) says that if we take two equivalence classes $[m]$ and $[n]$, then we can unambiguously define $[m]+[n]$ and $[m] \cdot[n]$. Pick any $m_{1} \in[m]$ and any $n_{1} \in[n]$, and define

$$
[m]+[n] \equiv\left[m_{1}+n_{1}\right]
$$

and

$$
[m] \cdot[n] \equiv\left[m_{1} \cdot n_{1}\right]
$$

The definition is unambiguous since it doesn't matter which $m_{1}$ and $n_{1}$ we pick. Find the addition and multiplication tables for the equivalence classes of $\equiv(\bmod 4)$ and $\equiv(\bmod 5)$. (Hint: for both $\equiv(\bmod 4)$ and $\equiv(\bmod 5)$, your answer should include

$$
[0]+[0] \equiv[0],[0]+[1] \equiv[1],[0] \cdot[0] \equiv[0]
$$

and

$$
[1] \cdot[1] \equiv[1]
$$

but, for $\equiv(\bmod 4)$,

$$
[2]+[2] \equiv[0]
$$

whereas, that will be false for $\equiv(\bmod 5)$.)

## Proof.

The addition and multiplication tables for the equivalence classes of $\equiv(\bmod 4)$

| + | $[0]$ | $[1]$ | $[2]$ | $[3]$ |
| :---: | :---: | :---: | :---: | :---: |
| $[0]$ | $[0]$ | $[1]$ | $[2]$ | $[3]$ |
| $[1]$ | $[1]$ | $[2]$ | $[3]$ | $[0]$ |
| $[2]$ | $[2]$ | $[3]$ | $[0]$ | $[1]$ |
| $[3]$ | $[3]$ | $[0]$ | $[1]$ | $[2]$ |


| $\cdot$ | $[0]$ | $[1]$ | $[2]$ | $[3]$ |
| :---: | :---: | :---: | :---: | :---: |
| $[0]$ | $[0]$ | $[0]$ | $[0]$ | $[0]$ |
| $[1]$ | $[0]$ | $[1]$ | $[2]$ | $[3]$ |
| $[2]$ | $[0]$ | $[2]$ | $[0]$ | $[2]$ |
| $[3]$ | $[0]$ | $[3]$ | $[2]$ | $[1]$ |

The addition and multiplication tables for the equivalence classes of $\equiv(\bmod 5)$

| + | $[0]$ | $[1]$ | $[2]$ | $[3]$ | $[4]$ |
| :---: | :---: | :---: | :---: | :---: | :---: |
| $[0]$ | $[0]$ | $[1]$ | $[2]$ | $[3]$ | $[4]$ |
| $[1]$ | $[1]$ | $[2]$ | $[3]$ | $[4]$ | $[0]$ |
| $[2]$ | $[2]$ | $[3]$ | $[4]$ | $[0]$ | $[1]$ |
| $[3]$ | $[3]$ | $[4]$ | $[0]$ | $[1]$ | $[2]$ |
| $[4]$ | $[4]$ | $[0]$ | $[1]$ | $[2]$ | $[3]$ |


| $\cdot$ | $[0]$ | $[1]$ | $[2]$ | $[3]$ | $[4]$ |
| :---: | :---: | :---: | :---: | :---: | :---: |
| $[0]$ | $[0]$ | $[0]$ | $[0]$ | $[0]$ | $[0]$ |
| $[1]$ | $[0]$ | $[1]$ | $[2]$ | $[3]$ | $[4]$ |
| $[2]$ | $[0]$ | $[2]$ | $[4]$ | $[1]$ | $[3]$ |
| $[3]$ | $[0]$ | $[3]$ | $[1]$ | $[4]$ | $[2]$ |
| $[4]$ | $[0]$ | $[4]$ | $[3]$ | $[2]$ | $[1]$ |

