Exercise 1.4.2

If $a|b$ and $a|c$. that means there exist $p, q \in \mathbb{Z}$ such that $b = pa$ and $c = qa$. So, $mb + nc = mpa + nqa$ and thus $mb + nc = (mp + nq)a$ and $m, n, p, q \in \mathbb{Z}$ so $mp + nq \in \mathbb{Z}$. Thus $a|mb + nc$

Exercise 1.4.3

$\gcd(130, 95) = \gcd(35, 95) = \gcd(35, 25) = \gcd(10, 25) = \gcd(10, 5) = \gcd(0, 5) = 5 = 130$

$\gcd(130, 95) = -8 \cdot 130 + 11 \cdot 95$

$\gcd(1295, 406) = \gcd(77, 406) = \gcd(77, 21) = \gcd(14, 21) = \gcd(14, 7) = \gcd(0, 7) = 7$

$\gcd(1295, 406) = -21 \cdot 1295 + 406 \cdot 67$

$\gcd(1351, 165) = \gcd(31, 165) = \gcd(31, 10) = \gcd(1, 10) = \gcd(1, 0) = 1$

$\gcd(1351, 165) = 16 \cdot 1351 - 131 \cdot 165$

Exercise 1.4.4

Since $a|c$ and $b|c$, then $c = na$ and $c = mb$, $n, m \in \mathbb{Z}$ so that $na = mb$ and $a|mb$ According to **Proposition 1.4.10**, since a and b are relative prime ($\gcd(a, b) = 1$), $a|mb$, then $a|m$. Thus, there exists $q \in \mathbb{Z}$ that $m = qa$. Thus $c = mb = qab$ and $ab|c$.

Exercise 1.5.2

$$
\begin{array}{c|ccccc}
+ & [0] & [1] & [2] & [3] & [4] \\
\hline
[0] & [0] & [1] & [2] & [3] & [4] \\
[1] & [1] & [2] & [3] & [4] & [0] \\
[2] & [2] & [3] & [4] & [0] & [1] \\
[3] & [3] & [4] & [0] & [1] & [2] \\
[4] & [4] & [0] & [1] & [2] & [3]
\end{array}
\qquad
\begin{array}{c|ccccc}
\cdot & [0] & [1] & [2] & [3] & [4] \\
\hline
[0] & [0] & [0] & [0] & [0] & [0] \\
[1] & [0] & [1] & [2] & [3] & [4] \\
[2] & [0] & [2] & [4] & [1] & [3] \\
[3] & [0] & [3] & [1] & [4] & [2] \\
[4] & [0] & [4] & [3] & [2] & [1]
\end{array}
$$

Exercise 1.5.3

$\mathbb{Z}_5^\times = \{[1], [2], [3], [4]\}$

$\mathbb{Z}_6^\times = \{[1], [5]\}$

$\mathbb{Z}_8^\times = \{[1], [3], [5], [7]\}$

$\mathbb{Z}_{20}^\times = \{[1], [3], [7], [9], [11], [13], [17], [19]\}$

Exercise 1.5.4

From the definition, we know $\pi_{m,n}([a]_n) = [a]_m$

Suppose $[a]_n = [b]_n$, $[a]_n, [b]_n \in \mathbb{Z}_n$. Therefore, $a \equiv b \mod n$, and $n|a - b$. Since $m|n$. Thus $m|a - b$, and there exist $h \in \mathbb{Z}$ that $hm = (a - b)$. and thus

$[a]_m = \{a + mk|k \in \mathbb{Z}\} = \{hm + b + mk|k \in \mathbb{Z}\} = \{b + m(h + k)|h + k \in \mathbb{Z}\} = [b]_m$

Then

$$\pi_{m,n}([a]_n) = [a]_m = [b]_m = \pi_{m,n}([b]_n)$$

Thus, $\pi_{m,n}$ is well defined.