Solution for Homework 2

Xiangcan Li

March 22, 2021

Exercise 1.4.2 Prove that if $a, b, c, m, n \in \mathbb{Z}$, $a \mid b$, and $a \mid c$, then $a \mid (mb + nc)$.

$a \mid b \implies$ There exists $\alpha \in \mathbb{Z}$ such that $b = \alpha a$.
$a \mid c \implies$ There exists $\beta \in \mathbb{Z}$ such that $c = \beta a$.
Hence, $mb + nc = m(\alpha a) + n(\beta a) = (m\alpha + n\beta)a$.
Since $m, n, \alpha, \beta \in \mathbb{Z}$, then there exists $(m\alpha + n\beta) \in \mathbb{Z}$ such that $mb + nc = (m\alpha + n\beta)a$.
We conclude that $a \mid (mb + nc)$.

Exercise 1.4.3 For each of the pairs $(a, b) = (130, 95), (1295, 406), (1351, 165)$,
find $\gcd(a, b)$ using the Euclidean Algorithm and express it in the form $\gcd(a, b) = m_0 a + n_0 b$ for $m_0, n_0 \in \mathbb{Z}$.

- $(a, b) = (130, 95)$

$$
\begin{aligned}
130 &= 1(95) + 35 \\
95 &= 2(35) + 25 \\
35 &= 1(25) + 10 \\
25 &= 2(10) + 5 \\
10 &= 2(5)
\end{aligned}
$$

$$
\begin{aligned}
5 &= 25 - 2(10) \\
&= \big(95 - 2(35)\big) - 2\big(35 - 1(25)\big) \\
&= \Big(95 - 2\big(130 - 1(95)\big)\Big) - 2\Big(35 - 1\big(95 - 2(35)\big)\Big) \\
&= \big(3(95) - 2(130)\big) + \big(2(95) - 6(35)\big) \\
&= \big(3(95) - 2(130)\big) + \Big(2(95) - 6\big(130 - 1(95)\big)\Big) \\
&= \big(3(95) - 2(130)\big) + \big(8(95) - 6(130)\big) \\
&= -8(130) + 11(95)
\end{aligned}
$$

  $\gcd(130, 95) = 5$ and $5 = -8(130) + 11(95)$.

- $(a, b) = (1295, 406)$

$$
\begin{aligned}
1295 &= 3(406) + 77 \\
406 &= 5(77) + 21 \\
77 &= 3(21) + 14 \\
21 &= 1(14) + 7 \\
14 &= 2(7)
\end{aligned}
$$

$$\begin{aligned}
7 &= 21 - 1(14) \\
&= \big(406 - 5(77)\big) - 1\big(77 - 3(21)\big) \\
&= 406 - 6(77) + 3(21) \\
&= 406 - 6(77) + 3\big(406 - 5(77)\big) \\
&= 4(406) - 21(77) \\
&= 4(406) - 21\big(1295 - 3(406)\big) \\
&= -21(1295) + 67(406)
\end{aligned}$$

$\gcd(1295, 406) = 7$ and $7 = -21(1295) + 67(406)$.

- $(a, b) = (1351, 165)$

$$\begin{aligned}
1351 &= 8(165) + 31 \\
165 &= 5(31) + 10 \\
31 &= 3(10) + 1 \\
10 &= 10(1)
\end{aligned}$$

$$\begin{aligned}
1 &= 31 - 3(10) \\
&= \big(1351 - 8(165)\big) - 3\big(165 - 5(31)\big) \\
&= 1351 - 11(165) + 15(31) \\
&= 1351 - 11(165) + 15\big(1351 - 8(165)\big) \\
&= 16(1351) - 131(165)
\end{aligned}$$

$\gcd(1351, 165) = 1$ and $1 = 16(1351) - 131(165)$.

Exercise 1.4.4 Suppose $a, b, c \in \mathbb{Z}$. Prove that if $\gcd(a, b) = 1$, $a \mid c$, $b \mid c$, then $ab \mid c$.

Since $a \mid c$, there exists $m \in \mathbb{Z}$ so that $c = ma$. Then $b \mid ma$. By **Proposition 1.4.10**, since $\gcd(a, b) = 1$, which means a and b are relatively prime, and $b \mid ma$, then $b \mid m$. Hence, there exists $n \in \mathbb{Z}$ so that $m = nb$. Hence, $c = nba$. Then $ab \mid c$.

We conclude that if $\gcd(a, b) = 1$, $a \mid c$, $b \mid c$, then $ab \mid c$.

Exercise 1.5.2 Write down the addition and multiplication tables for $\mathbb{Z}_5$.

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

Exercise 1.5.3 List all elements of $\mathbb{Z}_5^\times.\mathbb{Z}_6^\times, \mathbb{Z}_8^\times$ and $\mathbb{Z}_{20}^\times$.

Note that 5 is a prime. Then $\mathbb{Z}_5^\times = \{[1], [2], [3], [4]\}$.
$\gcd(1, 6) = 1$,$\gcd(5, 6) = 1$. Then $\mathbb{Z}_6^\times = \{[1], [5]\}$.
$\gcd(1, 8) = 1$,$\gcd(3, 8) = 1$,$\gcd(5, 8) = 1$,$\gcd(7, 8) = 1$. Then $\mathbb{Z}_8^\times = \{[1], [3], [5], [7]\}$.
$\gcd(1, 20) = 1$,$\gcd(3, 20) = 1$,$\gcd(7, 20) = 1$,$\gcd(9, 20) = 1$,
$\gcd(11, 20) = 1$,$\gcd(13, 20) = 1$,$\gcd(17, 20) = 1$,$\gcd(19, 20) = 1$
Then $\mathbb{Z}_{20}^\times = \{[1], [3], [7], [9], [11], [13], [17], [19]\}$.

Exercise 1.5.4 Prove that if $m \mid n$, then $\pi_{m,n} : \mathbb{Z}_n \to \mathbb{Z}_m$ is well-defined.

Let $[a]_n, [b]_n \in \mathbb{Z}_n$, where $a, b \in \mathbb{Z}$.
Assume $[a]_n = [b]_n$. Then $a \equiv b \mod n$. Hence, $n \mid (a - b)$.
Since $m \mid n$, $m \mid (a - b)$. Then we have $a \equiv b \mod m$, which implies $[a]_m = [b]_m$.
We conclude that $\pi_{m,n}$ is well-defined.