Kyle Kloberdanz
17 January 2022

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

Proof. Recall that $a|b$ implies $b = xa, x \in \mathbb{Z}$ and $a|c$ implies $c = ya, y \in \mathbb{Z}$. Hence we can write $b + c = xa + ya$. We can see that $a|xa$ and $a|ya$, hence $a|(xa + ya)$, therefore $a|(b + c)$.

It is also true that $a|xam$ and $a|yan$, hence $a|(xam + yan)$, therefore $a|(mb + nc)$ □

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 $gcd(a, b) = m_0a + n_0b$ for $m_0, n_0 \in \mathbb{Z}$.

$gcd(130, 95)$
$130 = 95 \times q + r$
$130 = 95 \times 1 + 35$
$95 = 35 \times 2 + 25$
$35 = 25 \times 1 + 10$
$25 = 10 \times 2 + 5$
$10 = 5 \times 2 + 0$

Therefore, $gcd(130, 95) = 5$

$gcd(1295, 406)$
$1295 = 406 \times q + r$
$1295 = 406 \times 3 + 77$
$406 = 77 \times 5 + 21$
$77 = 21 \times 3 + 14$
$21 = 14 \times 1 + 7$
$14 = 7 \times 2 + 0$

Therefore, $gcd(1295, 406) = 7$

$gcd(1351, 165)$
$1351 = 165 \times q + r$
$1351 = 165 \times 8 + 31$
$165 = 31 \times 5 + 10$
$31 = 10 \times 3 + 1$
$10 = 3 \times 3 + 1$
$3 = 1 \times 3 + 0$

Therefore, $gcd(1351, 165) = 1$

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

Proof. Recall that $gcd(a, b) = 1$ implies $ma + nb = 1$ where $m, n \in \mathbb{Z}$. Also recall that $a|c$ implies $c = xa$ and $b|c$ implies $c = yb$ where $x, y \in \mathbb{Z}$.
Given the facts above, we can multiply $ma + nb = 1$ by c to find that $c = cma + cnb$. Substituting for c, we find $c = ybma + xanb$. Factoring out ab yields $c = ab(ym + xn)$, therefore $ab|c$ $\square$

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

$\times$	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 $\mathbb{Z}_{20}^\times$.

Recall Proposition 1.5.6. *For all $n \geq 1$, we have $\mathbb{Z}_n^\times = \{[a] \in \mathbb{Z}_n | gcd(a, n) = 1\}$*

$\mathbb{Z}_5^\times = \{[1], [2], [3], [4]\}$
$\mathbb{Z}_6^\times = \{[1], [5]\}$
$\mathbb{Z}_8^\times = \{[1], [3], [5], [7]\}$
$\mathbb{Z}_{20}^\times = \{[1], [3], [7], [9], [11], [13], [17], [19]]\}$

As an aside, this problem can be solved with a beautiful one-liner in Haskell.

```
Prelude> map (\n -> [[x] | x <- [1..n], gcd x n == 1]) [5, 6, 8, 20]
[[[1],[2],[3],[4]],[[1],[5]],[[1],[3],[5],[7]],[[1],[3],[7],[9],[11],[13],[17],[19]]]
```

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

Proof. Recall from the text that $\pi_{m,n}([a]_n) = [a]_m$. Recall that a function, f, is well-defined if $[x] = [y] \implies f(x) = f(y)$. Recall Proposition 1.4.2 (iv), which states if $a|b$ and $b|c$, then $a|c$

Therefore, we must show that:

If $m|n$ and $[x]_n = [y]_n$ where $x, y \in \mathbb{Z}$, then $\pi_{m,n}(x) = \pi_{m,n}(y)$ where $\pi_{m,n} : \mathbb{Z}_n \to \mathbb{Z}_m$ and therefore $[x]_m = [y]_m$.

$[x]_n = [y]_n$ implies $x \equiv y \pmod n$, hence $n|(x - y)$.

Because $m|n$ and $n|(x-y)$, then by Proposition 1.4.2 (iv), we see that $m|(x-y)$, hence $x \equiv y \pmod m$, hence $[x]_m = [y]_m$, therefore $\pi_{m,n}$ is well-defined.
$\square$