Homework 12

Mark Petersen

Sections 22 and 23

22. Equivalence Relations

Exercise 22.1. Let $A = \{1, 2, 3, 4\}$. List one partition of A with one part, seven partitions of A with two parts, six partitions of A with three parts, and one partition of A with four parts. This gives a total of fifteen partitions.

a) One partition of A with one part.
   $P = \{\{1, 2, 3, 4\}\}$
b) Seven partitions of A with two parts.
   $P_1 = \{\{1\}, \{2, 3, 4\}\}$
   $P_2 = \{\{1, 2\}, \{3, 4\}\}$
   $P_3 = \{\{1, 2, 3\}, \{4\}\}$
   $P_4 = \{\{2\}, \{1, 3, 4\}\}$
   $P_5 = \{\{2, 3\}, \{1, 4\}\}$
   $P_6 = \{\{2, 4\}, \{1, 3\}\}$
   $P_7 = \{\{3\}, \{1, 2, 4\}\}$
c) Six partitions of A with three parts.
   $P_1 = \{\{1, 2\}, \{3\}, \{4\}\}$
   $P_2 = \{\{1\}, \{2, 3\}, \{4\}\}$
   $P_3 = \{\{1\}, \{3\}, \{2, 4\}\}$
   $P_4 = \{\{2\}, \{1, 3\}, \{4\}\}$
   $P_5 = \{\{2\}, \{3\}, \{1, 4\}\}$
   $P_6 = \{\{1\}, \{2\}, \{3, 4\}\}$
d) One partition of A with four parts.
   $P = \{\{1\}, \{2\}, \{3\}, \{4\}\}$

Exercise 22.2. Let A be a set with $|A| = 10$, and let $\sim$ be an equivalence relation on A. Denote the equivalence classes of $\sim$ by $[x]$ for $x \in A$. Suppose that we have elements $a, b, c \in A$ with $|[a]| = 3$, $|[b]| = 5$, and $|[c]| = 1$.

a) Are any of a, b, and c related by $\sim$?.
   No, according to theorem 22.1 in the book, if $x \sim y$ then $[x] = [y]$ for any $x, y \in A$. And if $[x] = [y]$ then they must have the same cardinality. Since the cardinality of the equivalence classes of a, b, and c are different, they cannot be the same equivalence class, and hence not related.
b) How many equivalence classes for $\sim$ are there in A?
   Since the cardinality of A is 10, the sum of the cardinality of the elements of its partition by $\sim$ must equal 10. That is $|[a]| + |[b]| + |[c]| + \cdots = 10$. Since, $|[a]| + |[b]| + |[c]| = 9$ there can only be one other equivalence class of the relation $\sim$ on A whose cardinality is 1.

Exercise 22.3. Define a relation $\sim$ on $\mathbb{R}^2$ by $(a, b) \sim (c, d)$ if $a^2 + b^2 = c^2 + d^2$. We saw in Example 21.6 that $\sim$ is an equivalence relation.

a) Describe the equivalence class $[(3, 4)]$, both as a set and geometrically.
   $[(3, 4)] = \left\{(a, b) \in \mathbb{R}^2 : a^2 + b^2 = 28\right\}$. It is the set of points in $\mathbb{R}^2$ that are a distance of $\sqrt{28}$ from the origin. In other words, this set forms a circle around the origin with a radius of $\sqrt{28}$.

b) For an arbitrary element $(a, b) \in \mathbb{R}^2$, describe $[(a, b)]$.

$[(a, b)]$ is the set of points in $\mathbb{R}^2$ that are a distance of $\sqrt{a^2 + b^2}$ from the origin. (I think this is what the question is asking)

c) Prove that the set $[0, \infty) \times \{0\}$ is a transversal of $\sim$.

Proof: In order to show that $T = [0, \infty) \times \{0\}$ is a transversal of $\sim$, we need to show that every element of $\mathbb{R}^2$ is related to at least one element T, and we need to show that every element of $\mathbb{R}^2$ is related to at most one element of T. I will separate this into show existence and uniqueness.

Existence: Suppose directly that $(a, b) \in \mathbb{R}^2$, then $(a, b) \sim \big(a^2 + b^2, 0\big) \in T$. Hence there exists at least one element of T that is related to (a, b).

Uniqueness: Suppose by contradiction that $t_1 \sim (a, b)$ and $t_2 \sim (a, b)$ such that $t_1 \neq t_2$, then $t_1 = \big(a^2 + b^2, 0\big)$ and $t_2 = \big(a^2 + b^2, 0\big)$. This is a contradiction since $t_1 = t_2$. Therefore, every element of $\mathbb{R}^2$ is related to only one element of T. Hence T is a traversal of $\sim$. ■

Exercise 22.4. Let W be the set of all the words in the English language. Define a relation of W by $\alpha \approx \beta$ if α and β have the same first letter.

a) Prove that $\approx$ is an equivalence relation.

Proof: We want to show that $\approx$ is an equivalence relation on A. We do this by showing that $\approx$ is reflexive, symmetric, and transitive.

Reflexive: Suppose directly $a \in A$. Then a starts with some letter γ, which is the same letter that a starts with since its the same word. Hence $a \approx a$. Therefore, $\approx$ is reflexive.

Symmetric: Suppose directly $a, b \in A$ and $a \approx b$. Then the first letter of b is the same as the first letter of a. Well, if they have the same first letter, then the first letter of a is the first letter of b. Hence $a \approx b$. Therefore $\approx$ is symmetric.

Transitive: Suppose directly that $a, b, c \in A$ and $(a \approx b \wedge b \approx c)$. Then a and b start with the same letter, and b and c start with the same letter. Hence a and c must start with the same letter, so that $a \approx b$. Therefore $\approx$ is transitive.

Since $\approx$ is reflexive, symmetric, and transitive, it is an equivalence relation. ■

b) Let $[\alpha]$ be the equivalence class of $\alpha \in W$. For $\alpha =$ "cat", list six elements of $[\alpha]$.

call, calling, calls, caller, car, cars

c) How may equivalence classes are there in W for $\approx$?

Since there are 26 letters in the English alphabet, there are 26 equivalence classes.

d) Describe a transversal of $\approx$.

A transversal of $\approx$ would contain for every letter of the alphabet one word that starts with a letter of the alphabet.

Exercise 22.5. Let A be a set with n elements. Define a relation $\sim$ on $\mathcal{P}(A)$ by $X \sim A$ if $|X| = |Y|$, for any $X, Y \in \mathcal{P}(A)$.

a) Prove that $\sim$ is an equivalence relation.

Proof: We want to show that $\sim$ is an equivalence relation on $\mathcal{P}(A)$. We do this by showing that $\sim$ is reflexive, symmetric, and transitive.

Reflexive: Suppose directly $a \in \mathcal{P}(A)$. Then $|a| = x$ for some $x \in \mathbb{Z} \geq 0$. So $|a| = x = |a|$, which shows that $|a| \, R \, |a|$, thus $\sim$ is reflexive.

Symmetric: Suppose directly $a, b \in \mathcal{P}(A)$ and $a \sim b$. Then $|a| = x$ and $|b| = x$ for some $x \in \mathbb{Z} \geq 0$. Thus $|b| = |a|$, which shows that $|b| \, R \, |a|$, thus $\sim$ is symmetric.

Transitive: Suppose directly that $a, b, c \in \mathcal{P}(A)$ and $(a \sim b \wedge b \sim c)$. hen $|a| = x$, $|b| = x$, and $|c| = x$ for some $x \in \mathbb{Z} \geq 0$. So $|a| = |c|$, which shows that $|a| \, R \, |c|$, thus $\sim$ is reflexive.
Since $\sim$ is reflexive, symmetric, and transitive, it is an equivalence relation.

■

b) Describe the equivalence classes for $\sim$.

The equivalence classes for $\sim$, contains the subsets of $\mathcal{P}(A)$ with the same cardinality. Hence, there are $n+1$ equivalence classes, since one equivalence class contains just the empty set.

c) How many equivalence classes are there for $\sim$.

As stated earlier, there are $n+1$ equivalence classes, since one equivalence class contains just the empty set.

d) Describe a transversal of $\sim$.

The transversal of $\sim$ would contain one element of $\mathcal{P}(A)$ for every distinct cardinality.

e) How many elements of $\mathcal{P}(A)$ are in each equivalence class?

Let $[m]$ denote the equivalence class for $\sim$ that contains all the elements of $\mathcal{P}(A)$ with cardinality m, them $|[m]| = \binom{n}{m}$.

Exercise 22.6. Let $A = \{1, 2, \ldots, 10\}$. For $i \in A$, define

$$S_i = \{X \in \mathcal{P}(A) \, : \, i \, \text{is the least element of X}\}$$

Let $P = \{\{\emptyset\}, S_1, \ldots, S_{10}\}$.

a) Prove that P is a partition of $\mathcal{P}(A)$.

Proof: To show that P is a partition of $\mathcal{P}(\mathcal{A})$, we need to show that no set in P is empty, every element of $\mathcal{P}(A)$ is a member of some element of P, and that any two distinct elements of P are disjoint. We will prove each property separately.
(Nonempty pieces): We suppose directly that

$$S_i = \{X \in \mathcal{P}(A) \, : \, i \, \text{is the least element of X}\},$$

since $\mathcal{P}(A)$ contains all of the possible subsets of A, the sets $\{1\}, \{2\}, \ldots, \{10\}$ must be elements of $\mathcal{P}(A)$, and thus the set $\{i\}$ must be an element of S_i for $i \in A$. This shows that none of the sets S_i are empty, and since the set $\{\emptyset\}$ is clearly not empty, none of the sets in P are empty.
(Covering): We suppose directly that

$$S_i = \{X \in \mathcal{P}(A) \, : \, i \, \text{is the least element of X}\},$$

since each element of $\mathcal{P}(A)$ has a least element $i \in A$ except for the empty set, then each element of $\mathcal{P}(A)$, except for the empty set, must be an element of one of the sets S_i. And since an element of P contains the empty set, P is a covering of $\mathcal{P}(A)$.
(Disjoint Pieces): We suppose by contradiction that $S_k, S_m \in P$, with $k, m \in A$ and $k \neq m$, and that $S_k \cap S_m \neq \emptyset$. Since $S_k = \{X \in \mathcal{P}(A) \, : \, k \, \text{is the least element of X}\}$ and $S_m = \{X \in \mathcal{P}(A) \, : \, m \, \text{is the least element of X}\}$, then S_m and S_k must have an element $Y \in \mathcal{P}(A)$ in common. Since Y cannot contain two different least elements, the only way for $Y \in S_k$ and $Y \in S_m$ would be for $S_k = S_m$. But this is a contradiction. Thus, every element of P is disjoint. We quickly state that the element $\{\emptyset\}$ of P is disjoint from all other sets since $\emptyset \notin A$, therefore $\emptyset \notin S_i$ for $i \in A$.
We have shown that P contains no empty pieces, is a covering of $\mathcal{P}(A)$, and that its pieces are disjoint. Therefore, P is a covering of $\mathcal{P}(A)$. ■

b) Let $\sim$ be the equivalence relation of $\mathcal{P}(A)$ corresponding to P. How many equivalence classes does $\sim$ have?

Since P contains 11 disjoint elements, then there are 11 equivalence classes according to Theorem 22.9.

c) Write down a transversal of $\sim$.

$T = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}, \{7\}, \{8\}, \{9\}, \{10\}\}$.

d) Determine the equivalence class $[\{8, 9, 10\}]$ by listing its elements.

$[\{8, 9, 10\}] = \{\{8\}, \{8, 9\}, \{8, 10\}, \{8, 9, 10\}\}$

e) How large is the equivalence class $[\{2, 3, 4\}]$?

Its huge! $|[\{2, 3, 4\}]| = 1 + \binom{8}{1} + \binom{8}{2} + \binom{8}{3} + \binom{8}{4} + \binom{8}{5} + \binom{8}{6} + \binom{8}{7} + \binom{8}{8} = 256$.

Exercise 22.7. Give another proof of Theorem 22.1, by proving that (1) implies (2), that (2) implies (3), and that (3) implies (1). Note that your proof should not use any theorems after or including Theorem 22.1; it should only use basic properties of equivalence relations and equivalence classes.

Proof: We prove the equivalence by proving three implications: $(1) \implies (2)$, $(2) \implies (3)$, and $(3) \implies (1)$.

$(1) \implies (2)$: We suppose directly that $x \sim y$. Since an equivalence relation is reflexive we know that $x, y \in [x]$ and $y \in [y]$. Since it is symmetric, we know that $y \sim x$, thus $x \in [y]$. Thus the intersection $[x] \cap [y]$ must contain at least the elements x, y and therefore cannot be empty.

$(2) \implies (3)$: Assume $[x] \cap [y] \neq \emptyset$. We wish to show $[x] = [y]$. We will prove this equality by showing both inclusions.

We first show $[x] \subseteq [y]$. Let $z \in [x]$, then $x \sim z$. Since $[x] \cap [y] \neq \emptyset$ there is an element m that is in both $[x]$ and $[y]$ so that $x \sim m$ and $y \sim m$. Using the symmetric property and transitive properties of equivalence relations we get $z \sim m$. Using the same properties again we get $y \sim z$. Thus $z \in [y]$.

We now show $[y] \subseteq [x]$. This is similar to the proof of $[x] \subseteq [y]$.

$(3) \implies (2)$. We assume directly that $[x] = [y]$. This meas that $x, y \in [x]$, thus $x \sim y$.

Since all three implications hold, the theorem 22.1 is true. ∎

Exercise 22.8. It is claimed above that every equivalence relation corresponds uniquely to a partition. Prove the final piece of that claim, by showing the following: Let A be a set. Let $\sim$ and $\approx$ be two equivalence relations. Show that if their equivalence classes are the same, then the relations are the same. (In other words, conclude that for all $a, b \in A$, we have $a \sim b$ if and only if $a \approx b$.) For ease of notation, we will write the equivalence classes for $\sim$ using $[a]$, and the equivalence classes for $\approx$ using $\bar{a}$.

Proof: We suppose directly that the equivalence relations $\sim$ and $\approx$ on A have the same equivalence classes, i.e., $[a] = \bar{a}$ for all $a \in A$. Using the definition of equivalence classes, for all $x \in [a]$ and $a \in A$, $(a, x) \in \sim$, and for all $x \in \bar{a}$ and $a \in A$, $(a, x) \in \approx$. Since $[a] = \bar{a}$ for all $a \in A$, $\sim$ must have the same elements as $\approx$. Thus they are equal. ∎

23. Integers modulo n

Exercise 23.1. Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. Prove that $0 \in \bar{a}$ if and only if $n \mid a$.

Proof: We wish to show that $0 \in \bar{a}$ if and only if $n \mid a$. This is a biconditional statement, so we will show both implications.

$(\implies)$: We assume directly that $0 \in \bar{a}$, then $a \equiv 0 \pmod{n}$. In other words $n \mid a - 0$ which is equivalent to $n \mid a$.

$(\impliedby)$: We assume directly that $n \mid a$. This can be written as $n \mid (a-0)$, which is equivalent to $a \equiv 0 \pmod{n}$, hence $0 \in \bar{a}$.

Since both implications hold, the statement that $0 \in \bar{a}$ if and only if $n \mid a$ is true. ■

Exercise 23.2. Compute the following. Write the results as $\bar{r}$, with $r \in \mathbb{Z}$ non-negative and as small as possible. For this problem let % denote modulus

a) $\bar{6} + \bar{7}$ in $\mathbb{Z}_9$.
   $(6+7)\,\%9 = 4$. Thus $\bar{4}$.
b) $\bar{6} \cdot \bar{7}$ in $\mathbb{Z}_9$.
   $(6 \cdot 7)\,\%9 = 6$. Thus $\bar{6}$.
c) $\overline{59} \cdot \overline{119}$ in $\mathbb{Z}_{30}$.
   $(59 \cdot 119)\,\%30 = 1$. Thus $\bar{1}$
d) $\bar{6} \cdot \bar{5} + \overline{85}$ in $\mathbb{Z}_7$.
   $(6 \cdot 5 + 85)\,\%7 = 3$. Thus $\bar{3}$.
e) $\bar{2}^{10}$ in $\mathbb{Z}_5$
   $\left(2^{10}\right)\%5 = \left(2^4 \cdot 2^4 \cdot 2^2\right)\%5 = 4$. Thus $\bar{4}$.

Exercise 23.3. Create addition and multiplication tables for $\mathbb{Z}_5$. Be sure to write each entry of the tables as one of $\bar{0}, \bar{1}, \bar{2}, \bar{3}$ or $\bar{4}$

+	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

*	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 23.4. Let $n \in \mathbb{N}$. Prove the following facts about addition and multiplication in $\mathbb{Z}_n$.

a) For all $X, Y \in \mathbb{Z}_n$, $X + Y = Y + X$
   Proof: We suppose directly that $X, Y \in \mathbb{Z}_n$. Then $X = \bar{x}$ and $Y = \bar{y}$. According to Theorem 23.4, $\bar{x} = \{x + kn \,:\, k \in \mathbb{Z}\}$ and $\bar{y} = \{y + \ell n \,:\, \ell \in \mathbb{Z}\}$. Adding the two together gives me

$$\begin{aligned}\overline{x+y} &= \{x + kn + y + \ell n \,:\, k, \ell \in \mathbb{Z}\}\\ &= \{y + \ell n + x + kn \,:\, k, \ell \in \mathbb{Z}\}\\ &= \overline{y+x}\\ &= \bar{y} + \bar{x}\\ &= Y + X\end{aligned}$$

■

b) For all $X, Y \in \mathbb{Z}_n$, $X \cdot Y = Y \cdot X$

Proof: We assume directly that $X, Y \in \mathbb{Z}_n$. Then $X = \bar{x}$ and $Y = \bar{y}$. According to Theorem 23.4, $\bar{x} = \{x + kn \,:\, k \in \mathbb{Z}\}$ and $\bar{y} = \{y + \ell n \,:\, \ell \in \mathbb{Z}\}$. Multiplying the two together gives

$$\begin{aligned}
\overline{x \cdot y} &= \{(x + kn)(y + \ell n) \,:\, k, \ell \in \mathbb{Z}\} \\
&= \{(y + \ell n)(x + kn) \,:\, k, \ell \in \mathbb{Z}\} \\
&= \overline{y \cdot x} \\
&= \bar{y} \cdot \bar{x} \\
&= Y \cdot X
\end{aligned}$$

■

c) For all $X \in \mathbb{Z}_n$, $X \cdot \bar{0} = \bar{0}$.
Proof: We assume directly that $X, \bar{0} \in \mathbb{Z}_n$. Then $X = \bar{x}$. According to Theorem 23.4, $\bar{x} = \{x + kn \,:\, k \in \mathbb{Z}\}$ and $\bar{0} = \{0 + \ell n \,:\, \ell \in \mathbb{Z}\}$. Multiplying the two together gives

$$\begin{aligned}
\overline{x \cdot 0} &= \{(x + kn)(0 + \ell n) \,:\, k, \ell \in \mathbb{Z}\} \\
&= \{(x + kn)\,\ell n \,:\, k, \ell \in \mathbb{Z}\} \\
&= \{0 + mn \,:\, m \in \mathbb{Z}\} \\
&= \bar{0}
\end{aligned}$$

■

d) For all $X \in \mathbb{Z}_n$, $X \cdot \bar{1} = X$.
Proof: We assume directly that $X, \bar{1} \in \mathbb{Z}_n$. Then $X = \bar{x}$. According to Theorem 23.4, $\bar{x} = \{x + kn \,:\, k \in \mathbb{Z}\}$ and $\bar{1} = \{1 + \ell n \,:\, \ell \in \mathbb{Z}\}$. Multiplying the two together gives

$$\begin{aligned}
\overline{x \cdot 0} &= \{(x + kn)(1 + \ell n) \,:\, k, \ell \in \mathbb{Z}\} \\
&= \{x + kn + x\ell n + kn\ell n \,:\, k, \ell \in \mathbb{Z}\} \\
&= \{x + mn \,:\, m \in \mathbb{Z}\} \\
&= \bar{x}
\end{aligned}$$

■

e) For all $X \in \mathbb{Z}_n$, $X \cdot \bar{2} = X + X$.
Proof: We assume directly that $X, \bar{2} \in \mathbb{Z}_n$. Then $X = \bar{x}$. According to Theorem 23.4, $\bar{x} = \{x + kn \,:\, k \in \mathbb{Z}\}$ and $\bar{2} = \{2 + \ell n \,:\, \ell \in \mathbb{Z}\}$. Multiplying the two together gives

$$\begin{aligned}
\overline{x \cdot 0} &= \{(x + kn)(2 + \ell n) \,:\, k, \ell \in \mathbb{Z}\} \\
&= \{x2 + 2kn + x\ell n + kn\ell n \,:\, k, \ell \in \mathbb{Z}\} \\
&= \{x + (2k)\,n + x + (x\ell + kn\ell)\,n \,:\, k, \ell \in \mathbb{Z}\} \\
&= \{(x + mn) + (x + pn) \,:\, m, p \in \mathbb{Z}\} \\
&= \bar{x} + \bar{x}
\end{aligned}$$

■

f) For all $X \in \mathbb{Z}_n$, there is some $Y \in \mathbb{Z}_n$ such that $X + Y = \bar{0}$.
Proof: We assume directly that $X, Y \in \mathbb{Z}_n$. Then $X = \bar{x}$ and $Y = \bar{y}$. According to Theorem 23.4, $\bar{x} = \{x + kn \,:\, k \in \mathbb{Z}\}$ and $\bar{y} = \{y + \ell n \,:\, \ell \in \mathbb{Z}\}$. Adding the two together gives

$$\begin{aligned}
\bar{x} + \bar{y} &= \{x + kn + y + \ell n \,:\, k, \ell \in \mathbb{Z}\} \\
&= \{x + y + kn + \ell n \,:\, k, \ell \in \mathbb{Z}\}\,.
\end{aligned}$$

We can choose y such that $n \mid x+y$. In other words $x+y=nm$ for some $m \in \mathbb{Z}$. Then

$$\begin{aligned}\{x+y+kn+\ell n \,:\, k,\ell \in \mathbb{Z}\} &= \{mn+kn+\ell n \,:\, k,\ell,m \in \mathbb{Z}\} \\ &= \{(m+k+\ell)\,n \,:\, k,\ell,m \in \mathbb{Z}\} \\ &= \{0+(m+k+\ell)\,n \,:\, k,\ell,m \in \mathbb{Z}\} \\ &= \bar{0}\end{aligned}$$

■

g) For all $X, Y, Z \in \mathbb{Z}_n$, $(X+Y)\cdot Z = (X\cdot Z)+(Y\cdot Z)$.
Proof: We assume directly that $X, Y, Z \in \mathbb{Z}_n$. Then $X=\bar{x}$, $Y=\bar{y}$, and $Z=\bar{z}$. According to Theorem 23.4, $\bar{x}=\{x+kn : k\in\mathbb{Z}\}$, $\bar{y}=\{y+\ell n : \ell \in \mathbb{Z}\}$ and $\bar{z}=\{z+hn \,:\, h\in\mathbb{Z}\}$. Then we can write

$$\begin{aligned}(\bar{x}+\bar{y})\cdot\bar{z} &= \{(x+kn+y+\ell n)\cdot(z+hn) \,:\, k,\ell,h\in\mathbb{Z}\} \\ &= \{(x+kn)\cdot(z+hn)+(y+\ell n)\,(z+hn) \,:\, k,\ell,h\in\mathbb{Z}\} \\ &= \bar{x}\cdot\bar{z}+\bar{y}\cdot\bar{z}\end{aligned}$$

■

Exercise 23.5. Demonstrate that for each $X \neq \bar{0}$ in $\mathbb{Z}_5$, there is some $Y \in \mathbb{Z}_5$ such that $X\cdot Y=\bar{1}$.

According to the multiplication table in exercise 23.3, we see that $\bar{1}\cdot\bar{1}=1$, $\bar{2}\cdot\bar{3}=1$, $\bar{3}\cdot\bar{2}=1$, and $\bar{4}\cdot\bar{4}=1$.

Exercise 23.6. Is it true that for each $X \neq \bar{0}$ in $\mathbb{Z}_6$, there is some $Y \in \mathbb{Z}_6$ such that $X\cdot Y=\bar{1}$?

No, consider the simple multiplication table below which shows $\bar{2}\cdot Y$ for all $Y \in \mathbb{Z}$.

*	0	1	2	3	4	5
2	0	2	4	0	2	4

The table shows that there is not $Y \in \mathbb{Z}$ such that $\bar{2}\cdot Y=\bar{1}$.

Exercise 23.7. In this exercise we generalize what was done in the previous two exercises.

a) If $n \in \mathbb{N}$ is composite, prove that there are elements $\bar{a}, \bar{b} \in \mathbb{Z}_n$ with $\bar{a}\cdot\bar{b}=\bar{0}$ even though $\bar{a}, \bar{b} \neq \bar{0}$.
Proof: We assume directly that n is composite. Then, according to theorem 19.3, there exists two integers $x, y \in \mathbb{Z}$ such that $1 < x, y < n$ such that $x\cdot y=n$. The integers x and y are elements of their respective equivalence classes $\bar{x}$ and $\bar{y}$ which can be written as $\bar{x}=\{x+kn : k\in\mathbb{Z}\}$ and $\bar{y}=\{y+\ell n : \ell\in\mathbb{Z}\}$. Multiplying them together yields

$$\begin{aligned}\overline{x\cdot y} &= \{(x+kn)\,(y+\ell n) \,:\, k,\ell\in\mathbb{Z}\} \\ &= \{xy+ykn+x\ell n+kn\ell n \,:\, k,\ell\in\mathbb{Z}\} \\ &= \{n+ykn+x\ell n+kn\ell n \,:\, k,\ell\in\mathbb{Z}\} \\ &= \{0+mn \,:\, m\in\mathbb{Z}\} \\ &= \bar{0}\end{aligned}$$

■

b) If $n \in \mathbb{N}$ is prime, prove that given $\bar{a}, \bar{b} \in \mathbb{Z}_n$, if $\bar{a}\cdot\bar{b}=\bar{0}$, then $\bar{a}=\bar{0}$ or $\bar{b}=\bar{0}$.

Proof: We assume directly that n is prime and that for $\bar{a}, \bar{b} \in \mathbb{Z}_n$, $\bar{a} \cdot \bar{b} = \bar{0}$. The equivalence classes $\bar{a}$ and $\bar{b}$ are $\bar{a} = \{a + kn \,:\, k \in \mathbb{Z}\}$ and $\bar{b} = \{b + \ell n \,:\, \ell \in \mathbb{Z}\}$. Multiplying them together we get

$$\begin{aligned} \bar{a} \cdot \bar{b} &= \{(a + kn)(b + \ell n) \,:\, m, k \in \mathbb{Z}\} \\ &= \{(ab + a\ell n + bkn + kn\ell n), : m, k \in \mathbb{Z}\}. \end{aligned}$$

Since $\bar{a} \cdot \bar{b} = \bar{0}$, $(ab + a\ell n + bkn + kn\ell n) = mn$ for some $m \in \mathbb{Z}$. This would require that $n \mid ab$. According to Euclid's lemma, since $n \mid ab$ and n is prime, we know that $n \mid a$ or $n \mid b$. thus $a = ng$ or $b = nh$ for some $g, h \in \mathbb{Z}$. Thus $\bar{a} = \{gn + kn \,:\, k, g \in \mathbb{Z}\}$ or $\bar{b} = \{hn + \ell n \,:\, \ell, g \in \mathbb{Z}\}$. Therefore, $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$. ∎

c) If $n \in \mathbb{N}$ is prime, prove that for any nonzero $\bar{a} \in \mathbb{Z}_n$, there exists $\bar{b} \in \mathbb{Z}$ with $\bar{a} \cdot \bar{b} = \bar{1}$.

Proof: We suppose directly that n is prime, $\bar{a} \in \mathbb{Z}_n$ and that $\bar{a} \neq \bar{0}$. Then $\bar{a} = \{a + kn \,:\, k \in \mathbb{Z}\}$. Since n is prime, then GCD $(a, n) = 1$. This allows us to write 1 as a linear combination of a and n. Let $x, y \in \mathbb{Z}$ then $1 = ax + ny$. This can be written as $n(-y) = ax - 1$ which is equivalent to $n \mid ax - 1$ or $ax \equiv 1 \bmod n$. Let $x \in \bar{b}$ so that $x = b + pn$ for some $p \in \mathbb{Z}$. This means that $x \equiv b \bmod n$.. Thus we can substitute in b for x to get $ab \equiv 1 \bmod n$. Therefore $\bar{a} \cdot \bar{b} = \bar{1}$. ∎