

Chapter 6

Relations

6.1 Introduction to Relations

Definition 6.1. An **ordered pair** is an object of the form (x, y) . Two ordered pairs (x, y) and (a, b) are **equal** iff $x = a$ and $y = b$.

Definition 6.2. An **n -tuple** is an object of the form (x_1, x_2, \dots, x_n) . Each x_i is referred to as the **i th component**.

Note that an ordered pair is just a 2-tuple.

Definition 6.3. If X and Y are sets, the **Cartesian product** of X and Y is defined by

$$X \times Y = \{(x, y) \mid x \in X, y \in Y\}.$$

That is, $X \times Y$ is the set of all ordered pairs where the first element is from X and the second element is from Y . The set $X \times X$ is sometimes denoted by X^2 . We similarly define the Cartesian product of n sets, say X_1, \dots, X_n , by

$$\prod_{i=1}^n X_i = X_1 \times \dots \times X_n = \{(x_1, \dots, x_n) \mid \text{each } x_i \in X_i\}.$$

Example 6.4. Let $A = \{a, b, c\}$ and $B = \{\odot, \ominus\}$. Then

$$A \times B = \{(a, \odot), (a, \ominus), (b, \odot), (b, \ominus), (c, \odot), (c, \ominus)\}.$$

Exercise 6.5. Using the sets A and B from the previous example, find $B \times A$.

Exercise 6.6. Using the set B from the previous examples, find $B \times B$.

Exercise 6.7. What general conclusion can you make about $X \times Y$ versus $Y \times X$? When will they be equal?

Exercise 6.8. If X and Y are both finite sets, then how many elements will $X \times Y$ have? Be as specific as possible.

Exercise 6.9. Let $A = \{1, 2, 3\}$, $B = \{1, 2\}$, and $C = \{1, 3\}$. List the elements of the set $A \times B \times C$.

Exercise 6.10. Let $A = \mathbb{N}$ and $B = \mathbb{R}$. Describe the elements of the set $A \times B$.

Exercise 6.11. Let A be the set of all differentiable functions on the open interval $(0, 1)$, and let B equal the set of all derivatives of functions in A evaluated at $x = \frac{1}{2}$. Describe the elements of the set $A \times B$.

Exercise 6.12. Three space, \mathbb{R}^3 , is a Cartesian product. Unpack the meaning of \mathbb{R}^3 using the Cartesian product, and write the complete set notation version.

Exercise 6.13. Let $X = [0, 1]$ and let $Y = \{1\}$. Describe geometrically what $X \times Y$, $Y \times X$, $X \times X$, and $Y \times Y$ look like.

Definition 6.14. Let X and Y be sets. A **relation** from a set X to a set Y is a subset of $X \times Y$. A relation on X is a subset of $X \times X$.

Example 6.15. You may not realize it, but you are familiar with many relations. For example, on the real numbers, we have the relation \leq . We could say that $(3, \pi)$ is in the relation \leq since $3 \leq \pi$. However, $(1, -1)$ is not in the relation since $1 \not\leq -1$. (Order matters!)

Remark 6.16. Different notations for relations are used in different contexts. When talking about relations in the abstract, we indicate that a pair (a, b) is in the relation by some notation like $a \sim b$, which is read “ a is related to b .”

Example 6.17. Let P_f denote the set of all people with accounts on Facebook. Define F via $x F y$ iff x is friends with y . Then F is a relation on P_f .

We can often represent relations using graphs or digraphs. Given a finite set X and a relation \sim on X , a **digraph** (short for *directed graph*) is a discrete graph having the members of X as vertices and a directed edge from x to y iff $x \sim y$.

Example 6.18. Figure 6.1 depicts a digraph that represents a relation R given by

$$R = \{(a, b), (a, c), (b, b), (b, c), (c, d), (c, e), (d, d), (d, a), (e, a)\}.$$

Exercise 6.19. Let $A = \{a, b, c\}$ and define $\sim = \{(a, a), (a, b), (b, c), (c, b), (c, a)\}$. Draw the digraph for \sim .

Exercise 6.20. Let $A = \{1, 2, 3, 4, 5, 6\}$. Define $|$ on A via $x|y$ iff x divides y . Draw the digraph for $|$ on A .

When X or Y is infinite, it is not practical to draw a digraph. However, you are familiar with the graphs of some relations involving infinite sets.

Example 6.21. When we write $x^2 + y^2 = 1$, we are implicitly defining a relation. In particular, the relation is the set of ordered pairs (x, y) satisfying $x^2 + y^2 = 1$. In set notation:

$$\{(x, y) \mid x^2 + y^2 = 1\}$$

The graph of this relation in \mathbb{R}^2 is the standard unit circle.

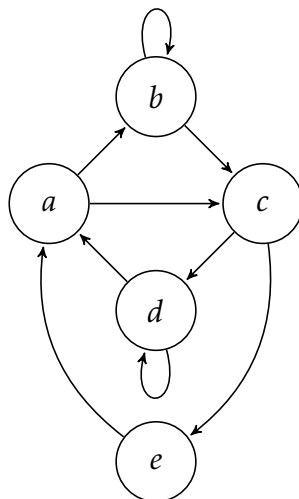


Figure 6.1: An example of a digraph for a relation.

Exercise 6.22. Define \sim on \mathbb{R} via $x \sim y$ iff $x \leq y$. Draw a picture of this relation in \mathbb{R}^2 . In other words, draw all points (x, y) where $x \sim y$.

Definition 6.23. Let \sim be a relation on a set A .

- (a) \sim is **reflexive** if for all $x \in A$, $x \sim x$ (every element is related to itself).
- (b) \sim is **symmetric** if for all $x, y \in A$, if $x \sim y$, then $y \sim x$.
- (c) \sim is **transitive** if for all $x, y, z \in A$, if $x \sim y$ and $y \sim z$, then $x \sim z$.

Example 6.24.

- (a) \leq on \mathbb{R} is reflexive and transitive, but not symmetric. $<$ on \mathbb{R} is transitive, but not symmetric and not reflexive.
- (b) If S is a set, then \subseteq on $\mathcal{P}(S)$ is reflexive and transitive, but not symmetric.
- (c) $=$ on \mathbb{R} is reflexive, symmetric, and transitive.

Exercise 6.25. Given a finite set A and a relation \sim , describe what each of reflexive, symmetric, and transitive look like in terms of a digraph.

Exercise 6.26. Let P be the set of people at a party and define N via $(x, y) \in N$ iff x knows the name of y . Describe what it would mean for N to be reflexive, symmetric, and transitive.

Exercise 6.27. Determine whether each of the following relations is reflexive, symmetric, or transitive.

- (a) Let P_f denote the set of all people with accounts on Facebook. Define F via xFy iff x is friends with y .

- (b) Let P be the set of all people and define H via xHy iff x and y have the same height.
- (c) Let P be the set of all people and define T via xTy iff x is taller than y .
- (d) Consider the relation “divides” on \mathbb{N} .
- (e) Let L be the set of lines and define \parallel via $l_1 \parallel l_2$ iff l_1 is parallel to l_2 .
- (f) Let $C[0, 1]$ be the set of continuous functions on $[0, 1]$. Define $f \sim g$ iff

$$\int_0^1 |f(x)| dx = \int_0^1 |g(x)| dx.$$

- (g) Define \sim on \mathbb{N} via $n \sim m$ iff $n + m$ is even.
- (h) Define D on \mathbb{R} via $(x, y) \in D$ iff $x = 2y$.

6.2 Equivalence Relations

Let \sim be a relation on a set A . Recall the following definitions:

- (a) \sim is **reflexive** if for all $x \in A$, $x \sim x$ (every element is related to itself).
- (b) \sim is **symmetric** if for all $x, y \in A$, if $x \sim y$, then $y \sim x$.
- (c) \sim is **transitive** if for all $x, y, z \in A$, if $x \sim y$ and $y \sim z$, then $x \sim z$.

As we’ve seen in the previous section of notes, these conditions are independent. That is, a relation may have some combination of these properties, but not necessarily all of them. However, we have a special name for when a relation does satisfy all three.

Definition 6.28. Let \sim be a relation on a set A . Then \sim is called an **equivalence relation** iff \sim is reflexive, symmetric, and transitive.

Exercise 6.29. Given a finite set A and a relation \sim on A , describe what the corresponding digraph would have to look like in order for \sim to be an equivalence relation.

Exercise 6.30. Let $A = \{a, b, c, d, e\}$. Make up an equivalence relation on A by drawing a digraph such that a is not related to b and c is not related to b .

Exercise 6.31. Let $S = \{1, 2, 3, 4, 5, 6\}$ and define

$$\sim = \{(1, 1), (1, 6), (2, 2), (2, 3), (2, 4), (3, 3), (3, 2), (3, 4), (4, 4), (4, 2), (4, 3), (5, 5), (6, 6), (6, 1)\}.$$

Justify that this is an equivalence relation.

Exercise 6.32. Determine which of the following are equivalence relations. Some of these occurred in the last section of notes and you are welcome to use your answers from those problems.

- (a) Let P_f denote the set of all people with accounts on Facebook. Define F via xFy iff x is friends with y .
- (b) Let P be the set of all people and define H via xHy iff x and y have the same height.
- (c) Let P be the set of all people and define T via xTy iff x is taller than y .
- (d) Consider the relation “divides” on \mathbb{N} .
- (e) Let L be the set of lines and define \parallel via $l_1 \parallel l_2$ iff l_1 is parallel to l_2 .
- (f) Let $C[0,1]$ be the set of continuous functions on $[0,1]$. Define $f \sim g$ iff

$$\int_0^1 |f(x)| dx = \int_0^1 |g(x)| dx.$$

- (g) Define \sim on \mathbb{N} via $n \sim m$ iff $n + m$ is even.
- (h) Define D on \mathbb{R} via $(x, y) \in D$ iff $x = 2y$.
- (i) Define \sim on \mathbb{Z} via $a \sim b$ iff $a - b$ is a multiple of 5.
- (j) Define \sim on \mathbb{R}^2 via $(x_1, y_1) \sim (x_2, y_2)$ iff $x_1^2 + y_1^2 = x_2^2 + y_2^2$.
- (k) Define \sim on \mathbb{R} via $x \sim y$ iff $\lfloor x \rfloor = \lfloor y \rfloor$, where $\lfloor x \rfloor$ is the greatest integer less than or equal to x (e.g., $\lfloor \pi \rfloor = 3$, $\lfloor -1.5 \rfloor = -2$, and $\lfloor 4 \rfloor = 4$).
- (l) Define \sim on \mathbb{R} via $x \sim y$ iff $|x - y| < 1$.

Definition 6.33. Let \sim be a relation on a set A (not necessarily an equivalence relation) and let $x \in A$. Then we define the **set of relatives of x** via

$$[x] = \{y \in A \mid x \sim y\}.$$

Also, define

$$\Omega_{\sim} = \{[x] \mid x \in A\}.$$

Notice that Ω_{\sim} is a set of sets. In particular, an element in Ω_{\sim} is a subset of A (equivalently, an element of $\mathcal{P}(A)$). Other common notations for $[x]$ include \bar{x} and R_x .

Exercise 6.34. Let P_f and F be as in part (a) of Exercise 6.32. Describe $[\text{Bob}]$ (assume you know which Bob we’re talking about). What is Ω_F ?

Exercise 6.35. Using your digraph in Exercise 6.30, find Ω_{\sim} .

Exercise 6.36. Consider the relation \leq on \mathbb{R} . If $x \in \mathbb{R}$, what is $[x]$?

Exercise 6.37. Find $[1]$ and $[2]$ for the relation given in part (i) of Exercise 6.32. How many different sets of relatives are there? What are they?

Exercise 6.38. Find $[x]$ for all $x \in S$ for S and \sim from Exercise 6.31. Any observations?

Theorem 6.39. Suppose \sim is an equivalence relation on a set A and let $a, b \in A$. Then $[a] = [b]$ iff $a \sim b$.

Theorem 6.40. Suppose \sim is an equivalence relation on a set A . Then

- (a) $\bigcup_{x \in A} [x] = A$, and
- (b) For all $x, y \in A$, either $[x] = [y]$ or $[x] \cap [y] = \emptyset$.

Definition 6.41. In light of Theorem 6.40, if \sim is an equivalence relation on a set A , then we refer to each $[x]$ as the **equivalence class** of x . In this case, Ω_{\sim} is the set of equivalence classes determined by \sim .

The upshot of Theorem 6.40 is that given an equivalence relation, every element lives in exactly one equivalence class. We'll see in the next section of notes that we can run this in reverse. That is, if we separate out the elements of a set so that every element is an element of exactly one subset (like the bins of my kid's toys), then this determines an equivalence relation. More on this later.

Example 6.42. The set of relatives that you found in part (i) of Exercise 6.32 is the set of equivalence classes modulo 5.

Exercise 6.43. If \sim is an equivalence relation on a finite set A , then what is the connection between the equivalence classes and the corresponding digraph?

Exercise 6.44. For each of the equivalence relations in Exercise 6.32, describe the equivalence classes as best as you can.

6.3 Partitions

Theorems 6.39 and 6.40 imply that if \sim is an equivalence relation on a set A , then \sim breaks A up into pairwise disjoint chunks, where each chunk is some $[a]$ for $a \in A$. Furthermore, each pair of elements in the same set of relatives are related via \sim .

As you've probably already noticed, equivalence relations are intimately related to the following concept.

Definition 6.45. A collection Ω of subsets of a set A is said to be a **partition** of A if the elements of Ω satisfy:

- (a) Each $X \in \Omega$ is nonempty,
- (b) Given $X, Y \in \Omega$, either $X = Y$ or $X \cap Y = \emptyset$, and
- (c) $\bigcup_{X \in \Omega} X = A$.

That is, the elements of Ω are pairwise disjoint and their union is all of A .

Notice that in the second condition of Definition 6.45, we cannot have both $X = Y$ and $X \cap Y = \emptyset$ at the same time.

Example 6.46. The following are all examples of partitions of the given set. Perhaps you can find exceptions in these examples, but please take them at face value.

- (a) Democrat, Republican, Independent, Green Party, Libertarian, etc. (set of registered voters)
- (b) freshman, sophomore, junior, senior (set of high school students)
- (c) evens, odds (set of integers)
- (d) rationals, irrationals (set of real numbers)

Example 6.47. Let $A = \{a, b, c, d, e, f\}$ and $\Omega = \{X_1, X_2, X_3\}$, where $X_1 = \{a\}$, $X_2 = \{b, c, d\}$, and $X_3 = \{e, f\}$. Then Ω is a partition of A since the elements of Ω are nonempty subsets of A , pairwise disjoint, and their union is all of A .

Exercise 6.48. Consider the set A from Example 6.47.

- (a) Find a partition of A that has 4 subsets in the partition.
- (b) Find a collection of subsets of A that does *not* form a partition.

Exercise 6.49. Find a partition of \mathbb{N} that consists of 3 subsets, where one of the sets is finite and the remaining two sets are infinite.

Exercise 6.50. Let P be the set of prime numbers, N be the set of odd natural numbers that are not prime, and E be the set of even natural numbers. Explain why this is not a partition of \mathbb{N} .

The next theorem spells out half of the close connection between partitions and equivalence relations. Hopefully you were anticipating this.

Theorem 6.51. Let \sim be an equivalence relation on a set A . Then Ω_{\sim} forms a partition of A .

Exercise 6.52. Consider the equivalence relation

$$\sim = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4), (4, 5), (5, 4), (5, 5), (6, 6), (5, 6), (6, 5), (4, 6), (6, 4)\}$$

on the set $A = \{1, 2, 3, 4, 5, 6\}$. Find the partition determined by Ω_{\sim} .

It turns out that we can reverse the situation, as well. That is, given a partition, we can form an equivalence relation. Before proving this, we need a definition.

Definition 6.53. Let A be a set and Ω any collection of subsets of A (not necessarily a partition). If $a, b \in A$, we will define a to be Ω -related to b if there exists an $R \in \Omega$ that contains both a and b . This relation is denoted by \sim_{Ω} and is called the **relation on A associated to Ω** .

This definition may look more awkward than the actual underlying concept. The idea is that if two elements are in the same subset, then they are related. For example, when my kids pick up all their toys and put them in the appropriate toy bins, we say that two toys are related if they are in the same bin.

Notice that we have two notations that look similar: Ω_{\sim} and \sim_{Ω} .

- (a) Ω_{\sim} is the collection of subsets of A determined by the relation \sim .
- (b) \sim_{Ω} is the relation determined by the collection of subsets Ω .

Exercise 6.54. Let $A = \{a, b, c, d, e, f\}$ and let $\Omega = \{X_1, X_2, X_3\}$, where $X_1 = \{a, c\}$, $X_2 = \{b, c\}$, and $X_3 = \{d, f\}$. List the elements of \sim_{Ω} by listing ordered pairs or drawing a digraph.

Exercise 6.55. Let A and Ω be as in Example 6.47. List the elements of \sim_{Ω} by listing ordered pairs or drawing a digraph.

Theorem 6.56. Let A be a set and let Ω be a collection of subsets of A (not necessarily a partition). Then \sim_{Ω} is symmetric.

Exercise 6.57. Give an example of a set A and a collection Ω from $\mathcal{P}(A)$ such that the relation \sim_{Ω} is not reflexive.

Theorem 6.58. Let A be a set and let Ω be a collection of subsets of A (not necessarily a partition). If

$$\bigcup_{R \in \Omega} R = A,$$

then \sim_{Ω} is reflexive.

Theorem 6.59. Let A be a set and let Ω be a collection of subsets of A (not necessarily a partition). If the elements of Ω are pairwise disjoint, then \sim_{Ω} is transitive.

Corollary 6.60. Let A be a set and let Ω be a partition of A . Then \sim_{Ω} is an equivalence relation.

The previous corollary says that every partition determines a natural equivalence relation. Namely, two elements are related iff they are elements of the same set in the partition.

Exercise 6.61. Let $A = \{\circ, \triangle, \blacktriangle, \square, \blacksquare, \star, \odot, \ominus\}$. Make up a partition Ω on A and then draw the digraph corresponding to \sim_{Ω} .

6.4 Modular Arithmetic

In this section, we look at a particular family of equivalence relations on the integers and explore the way in which arithmetic interacts with them.

Definition 6.62. For each $m \in \mathbb{N}$, define $m\mathbb{Z}$ to be the set of all integers that are divisible by m ; in set-builder notation, we have $m\mathbb{Z} = \{n \in \mathbb{Z} \mid n = mk \text{ for some } k \in \mathbb{Z}\}$.

For example, $5\mathbb{Z} = \{\dots, -10, -5, 0, 5, 10, \dots\}$ (the integers divisible by 5), and $2\mathbb{Z}$ is the set of even integers. What is $3\mathbb{Z}$? What about $1\mathbb{Z}$?

Exercise 6.63. Consider the sets $3\mathbb{Z}$, $5\mathbb{Z}$, $15\mathbb{Z}$, and $20\mathbb{Z}$.

- Make a partial list of the elements in each of four sets. Include at least five elements in each list.
- Notice that $3\mathbb{Z} \cap 5\mathbb{Z} = m\mathbb{Z}$ for some m ; what is m ? Describe $15\mathbb{Z} \cap 20\mathbb{Z}$ a similar way.
- Draw a Venn diagram illustrating how the sets $3\mathbb{Z}$, $5\mathbb{Z}$, and $15\mathbb{Z}$ intersect.
- Draw a Venn diagram illustrating how the sets $5\mathbb{Z}$, $15\mathbb{Z}$, and $20\mathbb{Z}$ intersect.

Theorem 6.64. Let $m \in \mathbb{N}$. If $a, b \in m\mathbb{Z}$, then $-a$, $a + b$, and ab are also in $m\mathbb{Z}$.¹

Definition 6.65. For each $m \in \mathbb{N}$, define a relation on \mathbb{Z} via $a \equiv_m b$ iff $(a - b) \in m\mathbb{Z}$. We read $a \equiv_m b$ as “ a is congruent to b modulo m .”

Theorem 6.66. For $m \in \mathbb{N}$, the relation \equiv_m is an equivalence relation on \mathbb{Z} .

Since we know that \equiv_m is an equivalence relation, we introduce some more notation.

Definition 6.67. For $m \in \mathbb{N}$, let $[a]_m$ denote the equivalence class of a with respect to \equiv_m . The class $[a]_m$ is called the **class of a modulo m** . The set of all equivalence classes determined by \equiv_m is denoted $\mathbb{Z}/m\mathbb{Z}$.

Example 6.68. Notice that you computed $[1]_5$ and $[2]_5$ in Exercise 6.37. For fun, let’s compute $[2]_7$. Tracing back through the definitions, we find that

$$n \in [2]_7 \iff n \equiv_7 2 \iff (n - 2) \in 7\mathbb{Z} \iff n - 2 = 7k \text{ for some } k \in \mathbb{Z}.$$

Thus, $n \in [2]_7 \iff n = 7k + 2$ for some $k \in \mathbb{Z}$, which is to say that the elements of $[2]_7$ are precisely those numbers that have a remainder of 2 when divided by 7. Thus, $[2]_7 = \{\dots, -12, -5, 2, 9, 16, \dots\}$. Also, by Theorem 6.39, $[2]_7 = [-12]_7 = [-5]_7 = [9]_7 = \dots$

Theorem 6.69. For $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, $[a]_m = [b]_m$ iff $(a - b)$ is divisible by m .²

Theorem 6.70. For $m \in \mathbb{N}$ and $a \in \mathbb{Z}$, $[a]_m = [0]_m$ iff a is divisible by m .

Exercise 6.71. Find $[0]_3$, $[1]_3$, $[2]_3$, $[4]_3$, and $[-2]_3$. How many elements are in $\mathbb{Z}/3\mathbb{Z}$?

Theorem 6.72. Let $m \in \mathbb{N}$, and let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. If $[a_1]_m = [a_2]_m$ and $[b_1]_m = [b_2]_m$, then $[a_1 + b_1]_m = [a_2 + b_2]_m$.³

Theorem 6.73. Let $m \in \mathbb{N}$, and let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. If $[a_1]_m = [a_2]_m$ and $[b_1]_m = [b_2]_m$, then $[a_1 \cdot b_1]_m = [a_2 \cdot b_2]_m$.⁴

¹You are encouraged to make use of what you proved in Chapter 2.

²Theorem 6.39 may be helpful.

³Consider using Theorem 6.69.

⁴Hint: note that $a_1 b_1 - a_2 b_2 = a_1 b_1 - a_2 b_1 + a_2 b_1 - a_2 b_2$.

The previous two theorems allows us to define addition and multiplication for $\mathbb{Z}/m\mathbb{Z}$.

Definition 6.74. Let $m \in \mathbb{N}$. For $[a]_m, [b]_m \in \mathbb{Z}/m\mathbb{Z}$, define the sum $[a]_m + [b]_m$ to be $[a + b]_m$ and the product $[a]_m \cdot [b]_m$ to be $[a \cdot b]_m$.

Remark 6.75. Addition and multiplication for $\mathbb{Z}/m\mathbb{Z}$ has many familiar (and some not so familiar) properties. For example, addition and multiplication are both associative and commutative. But, it is possible for $[a]_m \cdot [b]_m = [0]_m$ even when $[a]_m \neq [0]_m$ and $[b]_m \neq [0]_m$.

Theorem 6.76. Let $m \in \mathbb{N}$. Then addition for $\mathbb{Z}/m\mathbb{Z}$ is associative and commutative.⁵

Theorem 6.77. Let $m \in \mathbb{N}$. Then multiplication for $\mathbb{Z}/m\mathbb{Z}$ is associative and commutative.

Exercise 6.78. Find a and b such that $[a]_6 \cdot [b]_6 = [0]_6$ but $[a]_6 \neq [0]_6$ and $[b]_6 \neq [0]_6$. Do the same in $\mathbb{Z}/15\mathbb{Z}$: find a and b such that $[a]_{15} \cdot [b]_{15} = [0]_{15}$ but $[a]_{15} \neq [0]_{15}$ and $[b]_{15} \neq [0]_{15}$.

Theorem 6.79. Let $m \in \mathbb{N}$. If m is not prime, then there exists $[a]_m, [b]_m \in \mathbb{Z}/m\mathbb{Z}$ such that $[a]_m \cdot [b]_m = [0]_m$ but $[a]_m \neq [0]_m$ and $[b]_m \neq [0]_m$.

Theorem 6.80. Let $m \in \mathbb{N}$. For all $k \in \mathbb{N}$, if $[a_1]_m, [a_2]_m, \dots, [a_k]_m \in \mathbb{Z}/m\mathbb{Z}$, then

1. $[a_1]_m + [a_2]_m + \dots + [a_k]_m = [a_1 + a_2 + \dots + a_k]_m$, and
2. $[a_1]_m [a_2]_m \dots [a_k]_m = [a_1 a_2 \dots a_k]_m$.⁶

Remark 6.81. Part two of Theorem 6.80 implies that $([a]_m)^k = [a^k]_m$.

Exercise 6.82. For each of the following, find a number a with $0 \leq a \leq 6$ such that the given quantity is equal to $[a]_7$. The first one is done as an example.

1. $[8^{179}]_7$ *Solution:* $[8^{179}]_7 = ([8]_7)^{179} = ([1]_7)^{179} = [1^{179}]_7 = [1]_7$. Thus, $a = 1$.⁷
2. $[6^{179}]_7$ (There is a hint in the footnotes.⁸)
3. $[2^{300}]_7$ (There is a hint in the footnotes.⁹)
4. $[2^{301} + 5]_7$

Theorem 6.83. Let $n \in \mathbb{N}$, and let $a_k, a_{k-1}, \dots, a_1, a_0$ be the digits of n , i.e. $n = a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_1 10 + a_0$. Then $[n]_3 = [a_k + a_{k-1} + \dots + a_1 + a_0]_3$.

Theorem 6.84. An integer is divisible by 3 iff the sum of its digits is divisible by 3.¹⁰

Exercise 6.85. Using modular arithmetic, prove that for all integers $n \geq 0$, $3^{2n} - 1$ is divisible by 8.¹¹ Did you find this easier than, harder than, or the same as using induction?

⁵This means for all $[a]_m, [b]_m, [c]_m \in \mathbb{Z}/m\mathbb{Z}$, $([a]_m + [b]_m) + [c]_m = [a]_m + ([b]_m + [c]_m)$ and $[a]_m + [b]_m = [b]_m + [a]_m$.

⁶Consider using induction (with respect to k) for both parts.

⁷Remark 6.81 was used twice. We also used that $[8]_7 = [1]_7$.

⁸Hint: $[6]_7 = [-1]_7$.

⁹Hint: $[2^3]_7 = [1]_7$.

¹⁰Consider using Theorem 6.70.

¹¹By Theorem 6.70, you just need to show that $[3^{2n} - 1]_8 = [0]_8$.