HOMEWORK 10 - DISCRETE MATH SPRING 2023

JOHN ADAMSKI

`11.5.4` **Theorem.** *Write the addition and multiplication tables for* $\mathbb{Z}_6$.

Proof. Addition table:

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

Multiplication table:

$\times$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[2]$	$[0]$	$[2]$	$[4]$	$[0]$	$[2]$	$[4]$
$[3]$	$[0]$	$[3]$	$[0]$	$[3]$	$[0]$	$[3]$
$[4]$	$[0]$	$[4]$	$[2]$	$[0]$	$[4]$	$[2]$
$[5]$	$[0]$	$[5]$	$[4]$	$[3]$	$[2]$	$[1]$

□

`11.5.6` **Theorem 1.** *Suppose* $[a], [b] \in \mathbb{Z}_6$ *and* $[a] \cdot [b] = 0$. *Is it necessarily true that either* $[a] = 0$ *or* $[b] = 0$? *What if* $[a], [b] \in \mathbb{Z}_7$?

Proof. If $[a], [b] \in \mathbb{Z}_6$, then it is *not* necessarily true that $[a] = 0$ or $[b] = 0$. As a counterexample, set $[a] = [2]$ and $[b] = [3]$. Then $[a] \cdot [b] = [2] \cdot [3] = [6] = [0]$.

However, if $[a], [b] \in \mathbb{Z}_7$, then it *is* necessarily true that either $[a] = [0]$ or $[b] = [0]$. To prove this, assume for the sake of contradiction that there exist $[a], [b] \in \mathbb{Z}_7$ such that $[a] \cdot [b] = [0]$ and $[a] \neq [0]$ and $[b] \neq [0]$. Since $[a] \cdot [b] = [0]$, this means $[ab] = [0]$, and so $ab = 7n$ for some $n \in \mathbb{Z}$. That is, ab is a multiple of 7. On the other hand, since $[a] \neq [0]$ and $[b] \neq [0]$, neither a nor b is a multiple of 7. But since 7 is prime, a

or b would *have* to be a multiple of 7 for their product to be a multiple of 7.[1] This is a contradiction. Thus it must be impossible for both $[a] \cdot [b]$ to be $[0]$ and for neither $[a]$ nor $[b]$ to be $[0]$. That is, if $[a] \cdot [b] = 0$ then $[a] = [0]$ or $[b] = [0]$.

Alternatively, we could show by brute force that this is impossible by producing the mutliplcation table for $\mathbb{Z}_7$. Observe that $[0]$ does not appear outside of the first column or first row.

×	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[0]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[0]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[0]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[0]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[0]	[6]	[5]	[4]	[3]	[2]	[1]

□

11.5.8 **Theorem 2.** *Suppose $[a], [b] \in \mathbb{Z}_n$, and $[a] = [a']$ and $[b] = [b']$. Alice adds $[a]$ and $[b]$ as $[a] + [b] = [a + b]$. Bob adds them as $[a'] + [b'] = [a' + b']$. Show that their answers $[a + b]$ and $[a' + b']$ are the same.*

Proof. Let $[a] = [a']$ and $[b] = [b']$. We need to show that $[a = b] = [a' + b']$. Since $[a] = [a']$, we have $a \equiv a' \pmod{n}$ and so $a - a' = jn$, $j \in \mathbb{Z}$. Similarly, since $[b] = [b']$, we have $b \equiv b' \pmod{n}$ and so $b - b' = kn$, $k \in \mathbb{Z}$. Thus $a = a' + jn$ and $b = b' + kn$, and so

$$a + b = a' + jn + b' + kn.$$

That is,

$$(a + b) - (a' + b') = n(j + k).$$

Since $j + k \in \mathbb{Z}$, this means that $a + b \equiv a' + b' \pmod{n}$, and so $[a + b] = [a' + b']$. □

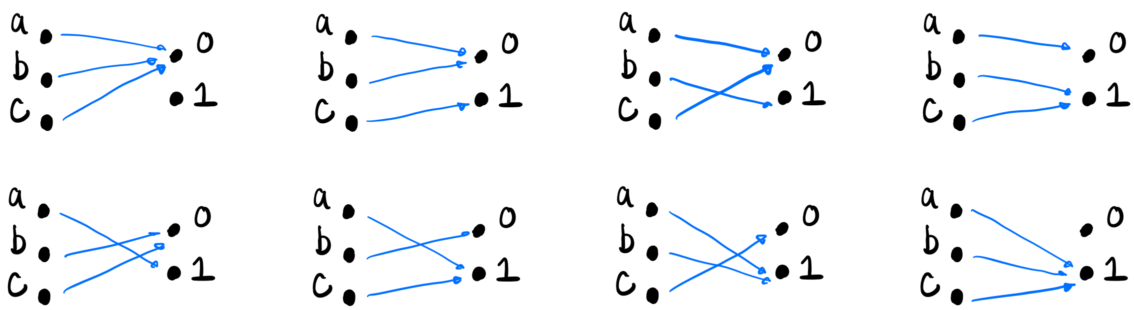
12.1.2 **Theorem 3.** *Suppose $A = \{a, b, c, d\}$, $B = \{2, 3, 4, 5, 6\}$, and $f = \{(a, 2), (b, 3), (c, 4), (d, 5)\}$. State the domain and range of f. Find $f(2)$ and $f(1)$.*

Proof. The domain of f is the set of all first components of ordered pairs in f. That is, $\{a, b, c, d\}$, which is A. The range of f is the set of all second components of ordered pairs in f. That is, $\{2, 3, 4, 5\}$, which is a subset of B. Since $(b, 3) \in f$, we have $f(b) = 3$. Since $(d, 5) \in f$, we have $f(d) = 5$. □

[1]A more technical argument would point out that the integers ab and $7n$ have unique prime factorizations (see Fundamental theorem of arithmetic). Since 7 appears in the prime factorization of $7n$, it must appear in the prime factorization of ab, which is the product of prime factors of a and prime factors of b. Thus 7 must be a (prime) factor of a or b.

12.1.4 **Theorem 4.** *There are eight diferent functions $f : \{a, b, c\} \to \{0, 1\}$. List them. Diagrams suffice.*

Proof. We take every possible assignment of an element in the codomain to each element of the domain.



$\square$

12.1.6 **Theorem 5.** *Suppose $f : \mathbb{Z} \to \mathbb{Z}$ is defined as $f = \{(x, 4x + 5) \,:\, x \in \mathbb{Z}\}$. State the domain, codomain, and range of f. Find $f(10)$.*

Proof. The domain is $\mathbb{Z}$ and the codomain is $\mathbb{Z}$, the range is the set

$$\{4x + 5 \,:\, x \in \mathbb{Z}\} = \{\dots, -7, -3, 1, 5, 9, 13, 17, \dots\},$$

and $f(10) = 45$. $\square$

12.1.8 **Theorem 6.** *Consider the set $f = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \,:\, x + 3y = 4\}$. Is this a function from $\mathbb{Z}$ to $\mathbb{Z}$? Explain.*

Proof. For the sake of contradiction, assume that f is a function from $\mathbb{Z}$ to $\mathbb{Z}$. Then for every $x \in \mathbb{Z}$, there must be some $y \in \mathbb{Z}$ such that $x + 3y = 4$. In particular, when $x = 0$ there must be some $y \in \mathbb{Z}$ such that $3y = 4$. But this means that 3 divides 4, which is false. This contradiction implies that f is *not* a function from $\mathbb{Z}$ to $\mathbb{Z}$. $\square$

12.1.12 **Theorem 7.** *Is the set $\theta = \{\big((x, y), (3y, 2x, x + y)\big) \,:\, x, y \in \mathbb{R}\}$ a function? If so, what is its domain and range? What can be said about the codomain?*

Proof. For every point $(x, y) \in \mathbb{R}^2$, exactly one ordered pair with the point (x, y) as its first component appears in θ. This is enough to conclude that θ is a function with domain $\mathbb{R}^2$. The range of f is the set

$$\{(3y, 2x, x + y) \,:\, (x, y) \in \mathbb{R}^2\}.$$

If you are familiar with vectors, we can describe this set as

$$\{x\langle 0, 2, 1\rangle + y\langle 3, 0, 1\rangle \,:\, x, y \in \mathbb{R}\},$$

which is the plane though the origin that contains the two vectors $\langle 0,2,1\rangle$ and $\langle 3,0,1\rangle$. The codomain can be any set that contains the range as a subset. One possibility for the codomain is $\mathbb{R}^3$. □

12.2.4 **Theorem 8.** *A function $f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ is defined as $f(n) = (2n, n+3)$. Verify whether this function is injective and whether it is surjective.*

Proof. The function is injective. To prove this, assume $x, y \in \mathbb{Z}$ and $f(x) = f(y)$. Then $(2x, x+3) = (2y, y+3)$. This means, in particular, that $2x = 2y$ Therefore $x = y$, and this completes the proof.

The function $f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ is not surjective. That is to say that there exists at least one point (a, b) in the codomain $\mathbb{Z} \times \mathbb{Z}$ that is not in the range of f. Notice that for every $x \in \mathbb{Z}$, the first component of $f(x)$ is $2x$, which is even. Thus, no point $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ with a odd appears in the range of f. For a specific example, $(1, 0)$ is in the codomain $\mathbb{Z} \times \mathbb{Z}$, but not in the range of f. □

12.2.6 **Theorem 9.** *A function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ is defined as $f(m, n) = 3n - 4m$. Verify whether this function is injctive and whether it is surjective.*

Proof. The function f is not injective. To prove this, it is enough to provide an example of two points (m, n) and (m', n') in the domain $\mathbb{Z} \times \mathbb{Z}$ such that $f(a, b) = f(a', b')$. Oberve that $(0, 0)$ and $(3, 4)$ are two such points:

$$f(0,0) = 3 \cdot 0 - 4 \cdot 0 = 0 = 3 \cdot 4 - 4 \cdot 3 = f(3,4).$$

The function f is surjective. To prove this, let a be any integer. We must show that there exists an orderd pair $(m, n) \in \mathbb{Z} \times \mathbb{Z}$ such that $f(m, n) = a$. If we first observe that $f(-1, -1) = 3(-1) - 4(-1) = 1$, then we are halfway there. In fact, for any $a \in \mathbb{Z}$, we have

$$f(-a, -a) = 3(-a) - 4(-a) = a.$$

This completes the proof. □

12.2.10 **Theorem 10.** *Prove the function $f : \mathbb{R} - \{1\} \to \mathbb{R} - \{1\}$ defined by $f(x) = \left(\frac{x+1}{x-1}\right)^3$ is bijective.*

Proof. First we prove that f is injective. Assume $x, x' \in \mathbb{R} - \{1\}$ and $f(x) = f(x')$. Then

$$\begin{aligned}
\left(\frac{x+1}{x-1}\right)^3 &= \left(\frac{x'+1}{x'-1}\right)^3 \\
\frac{x+1}{x-1} &= \frac{x'+1}{x'-1} \\
(x+1)(x'-1) &= (x-1)(x'+1) \\
xx' - x + x' - 1 &= xx' + x - x' - 1 \\
2x' &= 2x \\
x' &= x.
\end{aligned}$$

Thus, $f(x) = f(x') \implies x = x'$ and so f is injective.

Now we prove that f is surjective. Let $y \in \mathbb{R} - \{1\}$. By setting[2]

$$x = \frac{y^{1/3}+1}{y^{1/3}-1} \in \mathbb{R} - \{1\},$$

we see that

$$\begin{aligned}
f(x) &= f\left(\frac{y^{1/3}+1}{y^{1/3}-1}\right) \\
&= \left(\frac{\frac{y^{1/3}+1}{y^{1/3}-1}+1}{\frac{y^{1/3}+1}{y^{1/3}-1}-1}\right)^3 = \left(\frac{(\frac{y^{1/3}+1}{y^{1/3}-1}+1)\cdot(y^{1/3}-1)}{(\frac{y^{1/3}+1}{y^{1/3}-1}-1)\cdot(y^{1/3}-1)}\right)^3 \\
&= \left(\frac{y^{1/3}+1+y^{1/3}-1}{y^{1/3}+1-(y^{1/3}-1)}\right)^3 \\
&= \left(\frac{2y^{1/3}}{2}\right)^3 = \left(y^{1/3}\right)^3 \\
&= y.
\end{aligned}$$

□

Department of Mathematics, Fordham University
Email address: adamski@fordham.edu
URL: www.johnadamski.com

[2]This is $f^{-1}(y)$, which is found by solving the equation $y = \left(\frac{x+1}{x-1}\right)^3$ for x.