Math 620: Homework 3, Functions

Due on Wednesday, September 16, 2015

Boynton 10:00

Kailee Gray

Exercise 2.1.1: Determine whether the given function is one-to-one and whether it is onto.

(a) $f : \mathbb{R} \to \mathbb{R}; f(x) = x + 3$

(1-1) This function is one-to-one: If $f(x_1) = f(x_2)$, then $x_1 + 3 = x_2 + 3$ implies $x_1 = x_2$.
(onto) This function is onto: for any $y \in \mathbb{R}$, $y-3 \in \mathbb{R}$ will map to y; $f(y-3) = y-3+3 = y$.

(b) $f : \mathbb{C} \to \mathbb{C}; f(x) = x^2 + 2x + 1$

(1-1) This function is not one-to-one: notice $f(0) = 1 = f(-2)$, but $0 \neq -2$.
(onto) This function is onto: for any $y \in \mathbb{C}$, $\sqrt{y} \in \mathbb{C}$ so $-1 \pm \sqrt{y} \in \mathbb{C}$ will map to y; $f\left(-1 \pm \sqrt{y}\right) = \left(-1 \pm \sqrt{y}\right)^2 + 2\left(-1 \pm \sqrt{y}\right) + 1 = 1 \pm 2\sqrt{y} + y - 2 \pm 2\sqrt{y} + 1 = y$.

(c) $f : \mathbb{Z}_n \to \mathbb{Z}_n; f([x]_n) = [mx + b]_n$ **where** $m, b \in \mathbb{Z}$

(1-1) This function is not one-to-one: Let $n = 8, m = 4, b = 1$. Then, $f([0]_8) = [4 \cdot 0 + 1] = 1 = [4 \cdot 2 + 1] = f([2]_8$ but $[0]_8 \neq [2]_8$.
However, note if $\gcd(m, n) = 1$, then f is 1-1. if $f([x_1]_n) = 1 = f([x_2]_n)$, then $[mx_1 + b]_n = [mx_2+b]_n$ so $mx_1+b \equiv mx_2+b \pmod{n}$ which, since $\gcd(m, n) = 1$, implies $x_1 \equiv x_2 \pmod{n}$.
(onto) This function is not onto: using $n = 8, m = 4, b = 1$, there is no element in $\mathbb{Z}_8$ that maps to 2. If there were, there would be a solution to $4x+1 \equiv 2 \pmod{8}$ which would imply $4x \equiv 7 \pmod{8}$. If x is even, $4x \equiv 0 \pmod{8}$ and if x is odd, $4x \equiv 4 \pmod{8}$ so no such x exists in $\mathbb{Z}_8$.
However, as above, if $\gcd(m, n) = 1$, then m has a unique multiplicative inverse, m^{-1}, mod n and so f is onto: for any $y \in \mathbb{Z}_8$, $m^{-1}(y - b)$ maps to y.

continued on page 3...

2.1.1 (d) $f : \mathbb{R}^+ \to \mathbb{R}; f(x) = \ln(x)$

(1-1) This function is one-to-one: If $f(x_1) = f(x_2)$, then $\ln x_1 = \ln x_2 + 3$, so $e^{\ln x_1} = e^{\ln x_2}$, which implies $x_1 = x_2$.

(onto) This function is onto: for any $y \in \mathbb{R}$, $e^y \in \mathbb{R}^+$ and $f(e^y) = \ln(e^y) = y$.

Exercise 2.1.3: For each one-to-one and onto function in exercise 2, find the inverse of the function.

(a) $f : \mathbb{R} \to \mathbb{R}; f(x) = x+3$ $\qquad f^{-1}(x) = x - 3$

(b) $f : \mathbb{C} \to \mathbb{C}; f(x) = x^2+2x+1$ $\qquad f^{-1}(x) = -1 \pm \sqrt{x}$

(c) $f : \mathbb{Z}_n \to \mathbb{Z}_n; f([x]_n) = [mx + b]_n$ **where** $m, b \in \mathbb{Z}$

If $\gcd(m, n) = 1$, the multiplicative inverse of m exists mod n. So let m^{-1} be the multiplicative inverse of m. Then, $f^{-1}([x]_n) = [m^{-1} \cdot (x - b)]_n$.

(d) $f : \mathbb{R}^+ \to \mathbb{R}; f(x) = \ln(x)$ $\qquad f^{-1}(x) = e^x$

Exercise 2.1.9: Show that the following formula yields a well-defined function.

(a) $f : \mathbb{Z}_8 \to \mathbb{Z}_8; f([x]_8) = [mx]_8$**, for any** $m \in \mathbb{Z}$

(WD1) For every $[x]_8 \in \mathbb{Z}_8$ we have $[x]_8 \in \mathbb{Z}_8$ so this condition is satisfied.

(WD2) Assume $[x_1]_8 = [x_2]_8$. Then, $x_1 \equiv x_2 \pmod 8$. Multiply both sides of this congruence by m to obtain $mx_1 \equiv mx_2 \pmod 8$. This implies $f([x_1]_8) = f([x_2]_8)$.

Exercise 2.1.10: Give an example to show that the formula does not define a function.

(d) $p : \mathbb{Z}_{12} \to \mathbb{Z}_5;\ p([x]_{12}) = [2x]_5$

Notice $[0]_{12} = [12]_{12}$ but $f([0]_{12}) = [0]_5$ and $f([12]_{12}) = [4]_5$. Since $f([0]_{12}) \neq f([12]_{12})$, we have the same input mapping to two different outputs, so f is not a function.

Exercise 2.1.11: Let k and n be positive integers. For a fixed $m \in \mathbb{Z}$ define $f : \mathbb{Z}_n \to \mathbb{Z}_k$ by $f([x]_n) = ([mx]_k)$ for $x \in \mathbb{Z}$. Show that f defines a function if and only if $k \mid mn$.

Proof. ($\Rightarrow$) Assume f is a function. Then, $[0]_n$, which is equivalent to $[n]_n$, must map to exactly one element in $\mathbb{Z}_k$. Thus $f([0]_n) = f([n]_n)$ and so $[m \cdot 0]_k = [m \cdot n]_k$. Thus $0 \equiv mn \pmod{k}$ which implies $k \mid mn$.

($\Leftarrow$) Next, suppose $k \mid mn$.

(WD1) For every $[x]_n \in \mathbb{Z}_n$ we have $[mx]_k \in \mathbb{Z}_k$ so this condition is satisfied.

(WD2) We must show that when $[x_1]_n = [x_2]_n$, $f([x_1]_n) = f([x_2]_n)$. Let $x_1, x_2 \in \mathbb{Z}_n$ such that $[x_1]_n = [x_2]_n$. Then $x_1 \equiv x_2 \pmod{n}$ and so $x_1 = x_2 + bn$ for some $b \in \mathbb{Z}$. Multiply both sides of $x_1 = x_2 + bn$ by m to obtain $mx_1 = mx_2 + mbn$. Equivalently, $mx_1 = mx_2 + b(mn)$. Notice if $k \mid mn$, $mn = ka$ for some $a \in \mathbb{Z}$. So we can substitute $mn = ka$ into $mx_1 = mx_2 + b(mn)$ to obtain $mx_1 = mx_2 + b(ka)$. Thus, $mx_1 \equiv mx_2 \pmod{k}$ and $f([x_1]_n) = f([x_2]_n)$. $\square$

Exercise 2.1.12: Let k and n be positive integers such that $k \mid mn$. Show that f defined by: $m \in \mathbb{Z}$, $f : \mathbb{Z}_n \to \mathbb{Z}_k$, and $f([x]_n) = ([mx]_k)$ is a one-to-one correspondence if and only if $k = n$ and $\gcd(m, n) = 1$.

Proof. ($\Rightarrow$) Assume f defined by $m \in \mathbb{Z}$, $f : \mathbb{Z}_n \to \mathbb{Z}_k$, and $f([x]_n) = ([mx]_k)$ is a one-to-one correspondence. Then, f is one-to-one and onto.

If f is one-to-one, the Pigeon-hole Principle as presented in Boyton implies $n < k$ or $n = k$. If $n < k$, $|\mathbb{Z}_n| < |\mathbb{Z}_k|$. Since f is one-to-one, there exist a maximum of n elements mapped to in $|\mathbb{Z}_k|$ by f. So there would exist some $b \in \mathbb{Z}_k$ such that there was no $x \in \mathbb{Z}_n$ with $f([x]_n) = [b]_k$. However, f is onto so such a $b \in \mathbb{Z}_n$ is a contradiction. Thus, $k = n$.

Because f is onto, there exists $x \in \mathbb{Z}_n$ such that $f([x]_n) = [1]_k$; $f([x]_n) = [mx]_k$, so there must exist $x \in \mathbb{Z}_n$ such that $mx \equiv 1 \pmod{k}$. Then, $mx = 1 + bk$ for some $b \in \mathbb{Z}$. Equivalently, $1 = mx + (-b)k$. We showed above that $k = n$, so we can substitute to obtain $1 = mx + (-b)n$. Since we can write 1 as a linear combination of m, n, $\gcd(m, n) = 1$.

($\Leftarrow$) Assume $k = n$ and $\gcd(m, n) = 1$. We will show f is one-to-one and then use theorem 14 in Boynton to show f is a one-to-one correspondence. Suppose $x_1, x_2 \in \mathbb{Z}_n$ such that $f([x_1]_n) = f([x_2]_n)$. Since $f([x_1]_n) = [mx_1]_k$ and $f([x_2]_n) = [mx_2]_k$, we have $mx_1 \equiv mx_2 \pmod{k}$. Since $k = n$, the previous equivalence can be written $mx_1 \equiv mx_2 \pmod{n}$.

If $\gcd(m, n) = 1$, m has a multiplicative inverse mod n, so multiplying both sides of $mx_1 \equiv mx_2 \pmod{n}$ by this multiplicative inverse gives us $x_1 \equiv x_2 \pmod{n}$. Thus $f([x_1]_n) = f([x_2]_n)$ implies $[x_1]_n = [x_2]_n$; so f is one-to-one.If $k = n$, $\mathbb{Z}_k = \mathbb{Z}_n$ and $|\mathbb{Z}_k| = |\mathbb{Z}_n|$. Thus, because f has domain and co-domain with the same cardinality and because f is one-to-one, theorem 14 in Boynton implies f is a one-to-one correspondence.

□

Exercise 2.1.14: Let $f : A \to B$ and $g : B \to C$ be one-to-one and onto. Show that $(g \circ f)^{-1}$ exists and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Proof. Let $f : A \to B$ and $g : B \to C$ be one-to-one and onto.

First we will show that $(g \circ f)^{-1}$ exists. By proposition 2.1.5 (Beachy), if g, f are one-to-one and onto, $g \circ f$ is one-to-one and onto. So, by proposition 2.1.7 (Beachy), $(g \circ f)^{-1}$ exists and is unique. Next, we will prove $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. By definition 2.1.6 (Beachy), if $(g \circ f)^{-1}$ is the inverse of $g \circ f$, $(g \circ f) \circ (g \circ f)^{-1} = 1_C$ and $(g \circ f)^{-1} \circ (g \circ f) = 1_A$. So, we will evaluate $(g \circ f) \circ (f^{-1} \circ g^{-1})$ and $(f^{-1} \circ g^{-1}) \circ (g \circ f)$:

$$\begin{aligned}
(g \circ f) \circ (f^{-1} \circ g^{-1}) &= g \circ (f \circ f^{-1}) \circ g^{-1} && \text{by associative property of } \circ \\
&= g \circ (1_B) \circ g^{-1} && \text{by definition 2.1.6 (Beachy)} \\
&= g \circ (1_B \circ g^{-1}) && \text{by associative property of } \circ \\
&= g \circ g^{-1} && \text{by definition 2.1.6 (Beachy)} \\
&= 1_C && \text{by definition 2.1.6 (Beachy.)}
\end{aligned}$$

$$\begin{aligned}
(f^{-1} \circ g^{-1}) \circ (g \circ f) &= f^{-1} \circ (g^{-1} \circ g) \circ f && \text{by associative property of } \circ \\
&= f^{-1} \circ (1_B) \circ f && \text{by definition 2.1.6 (Beachy)} \\
&= f^{-1} \circ (1_B \circ f) && \text{by associative property of } \circ \\
&= f^{-1} \circ f && \text{by definition 2.1.6 (Beachy)} \\
&= 1_A && \text{by definition 2.1.6 (Beachy.)}
\end{aligned}$$

Thus $f^{-1} \circ g^{-1}$ is an inverse of $g \circ f$. Additionally, $(g \circ f)^{-1}$ is unique so $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. □

Exercise 2.1.15, part 1: Let $f : A \to B$ and $g : B \to C$ be functions. Prove that if $g \circ f$ is one-to-one, then f is one-to-one

Proof. Assume $g \circ f$ is one-to-one. Let $x_1, x_2 \in A$ such that $f(x_1) = f(x_2)$. Then, since g is a function, $g(f(x_1)) = g(f(x_2))$ and so $(g \circ f)(x_1) = (g \circ f)(x_2)$. Since $g \circ f$ is one-to-one, $(g \circ f)(x_1) = (g \circ f)(x_2)$ implies $x_1 = x_2$. Thus, f is one-to-one. □

Exercise 2.1.15, part 2: Let $f : A \to B$ and $g : B \to C$ be functions. Prove that if $g \circ f$ is onto, then g is onto.

Proof. If $g \circ f$ is onto for any $c \in C$, there exists $a \in A$ such that $(g \circ f)(a) = c$. This implies $g(f((a)) = c$. f is a function so for any $a \in A$, there exists $b \in B$ with $f(a) = b$. Thus, for any $c \in C$, there exists $b \in B$, $f(a) = b$ such that $g(b) = g(f((a)) = c$. Thus g is onto. $\square$

Exercise 2.1.17: Let $f : A \to B$ be a function. Prove that f is onto if and only if $h \circ f = k \circ f$ implies $h = k$, for every set C and all choice of functions $h : B \to C$ and $k : B \to C$.

Proof. $(\Rightarrow)$ Assume f is onto. Then, for any $b \in B$, there exists $a \in A$ such that $f(a) = b$. Next, assume $h \circ f = k \circ f$. Then, by definition of function equality, for all $a \in A$, $(h \circ f)(a) = (k \circ f)(a)$. Equivalently, $h(f(a)) = k(f(a))$. Again, since f is onto and because h, k are functions, for any $b \in B$ there exists an $a \in A$ such that $h(b) = h(f(a))$ and $k(b) = k(f(a))$. Thus $h(f(a)) = k(f(a))$, $h(b) = h(f(a))$ and $k(b) = k(f(a))$ imply $h(b) = k(b)$ for any $b \in B$. Therefore, $h = k$.

$(\Leftarrow)$ Assume $h \circ f = k \circ f$ implies $h = k$, for every set C and all choice of functions $h : B \to C$ and $k : B \to C$. Since $h \circ f = k \circ f$, h, k agree on the image on f. Suppose f is not onto. Then, there exists $b \in B$ such that there are no $a \in A$ with $f(a) = b$. We will define h, k such that h, k agree on the image of f but not on all of B. Let $h(x) = 1$ if $x = b$, $k(x) = 2$ if $x = b$, and let $h(x) = 0 = k(x)$ when $x \neq b$. Then, $(h \circ f)(x) = (k \circ f)(x)$ for all x but $h(x) \neq k(x)$ when $x = b$. This is a contradiction, so f must be onto.

$\square$

Exercise 2.1.20: Define $f\colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ by $f([x]_{mn}) = ([x]_m, [x]_n)$. Show that f is a function and that f is onto if and only if $\gcd(m, n) = 1$.

Proof. ($\Rightarrow$) Assume $f\colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ defined by $f([x]_{mn}) = ([x]_m, [x]_n)$ is a function and is onto. Since f is onto, there must exist some $[x]_{mn} \in \mathbb{Z}_{mn}$ such that $f([x]_{mn}) = ([0]_m, [1]_n)$. Then, $x \equiv 0 \pmod{m}$ and $x \equiv 1 \pmod{n}$ so $x = mk$ and $x = 1 + ns$ for some $k, s \in \mathbb{Z}$. Thus, $mk = 1 + ns$ and $1 = ns + (-k)m$. Since we can write 1 as a linear combination of m and n, $\gcd(m, n) = 1$.

($\Leftarrow$) Assume $\gcd(m, n,) = 1$.

First, we will show $f\colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ defined by $f([x]_{mn}) = ([x]_m, [x]_n)$ is a function.

(WD1) For every $[x]_{mn} \in \mathbb{Z}_{mn}$ we have $([x]_m, [x]_n) \in \mathbb{Z}_m \times \mathbb{Z}_n$ so this condition is satisfied.

(WD2) Assume $[x_1]_{mn} = [x_2]_{mn}$. Then, $x_1 \equiv x_2 \pmod{mn}$ so $x_1 = x_2 + mn(k)$ for some $k \in \mathbb{Z}$. Thus, $x_1 \equiv x_2 \pmod{m}$ and $x_1 \equiv x_2 \pmod{n}$ and $([x_1]_m, [x_1]_n) = ([x_2]_m, [x_2]_n)$. This implies $f([x_1]_{mn}) = f([x_2]_{mn})$.

Now we will show f is onto. Consider any element in $([b]_m, [a]_n) \in \mathbb{Z}_m \times \mathbb{Z}_n$. If $f([x]_{mn}) = ([b]_m, [a]_n)$, then $x \equiv b \pmod{m}$ and $x \equiv a \pmod{n}$. Because $\gcd(m, n) = 1$, the Chinese Remainder Theorem implies there exists a unique solution, mod mn to the previous system of congruences. Also, since $\gcd(m, n) = 1$ there exists $r, s \in \mathbb{Z}$ such that $rm + sn = 1$. Following the construction in the proof of the Chinese Remainder Theorem, let $x = arm + bsn$, so that $f([arm + bsn]_{mn}) = ([arm + bsn]_m, [arm + bsn]_n) = ([bsn]_m, [arm]_n)$. Since $sn \equiv 1 \pmod{m}$ and $rm \equiv 1 \pmod{n}$, we have $f([arm + bsn]_{mn}) = ([b]_m, [a]_n)$. $\square$