Homework

Jon Allen

September 17, 2014

Section 1.3: #12, 20 Section 2.1: # 18, 8

1.3 12. Show that $4 \cdot (n^2 + 1)$ is never divisible by 11.

proof

First we note that $\gcd(4, 11) = 1$ and 11 is prime, so then if $11|4\cdot(n^2+1)$ then by the fundamental theorem of arithmetic, $11|(n^2 + 1)$. That is to say

$$\begin{aligned} n^2 + 1 &\equiv 0 \mod 11 \\ n^2 &\equiv -1 \mod 11 \\ n^2 &\equiv 10 \mod 11 \end{aligned}$$

Noting that $\mathbb{Z}_{11}$ partitions $\mathbb{Z}$ we see that there must exist some $[a]_{11} \in \mathbb{Z}_{11}$ such that $[a^2]_{11} = [10]_{11}$ So looking at all the elements of $\mathbb{Z}_{11}$:

$$\begin{array}{cccccc} [0^2] = [0] & [1^2] = [1] & [2^2] = [4] & [3^2] = [9] & [4^2] = [5] & [5^2] = [3] \\ [6^2] = [3] & [7^2] = [2] & [8^2] = [-2] = [9] & [9^2] = [4] & [10^2] = [1] & \end{array}$$

We see by exhaustion that $[a]_{11} \notin \mathbb{Z}_{11}$ such that $[a^2]_{11} = [10]_{11}$ and so 11 does not divide $4\cdot(n^2+1)$. $\square$

20. Solve the following system of congruences.

$$2x \equiv 5 \mod 7 \qquad\qquad 3x \equiv 4 \mod 8$$

Hint: First reduce to the usual form.

$$\begin{aligned} 2x &\equiv 5 \mod 7 & 3x &\equiv 4 \mod 8 \\ \gcd(2,7) &= 1 & \gcd(3,8) &= 1 \end{aligned}$$

So both congruencies have one solution

$$\begin{aligned} c \cdot 2 &\equiv 1 \mod 7 & c \cdot 3 &\equiv 1 \mod 8 \\ 4 \cdot 2 &\equiv 1 \mod 7 & 3 \cdot 3 &\equiv 1 \mod 8 \\ x &\equiv 5 \cdot 4 \mod 7 & x &\equiv 3 \cdot 4 \mod 8 \\ x &\equiv 6 \mod 7 & x &\equiv 4 \mod 8 \end{aligned}$$

Now because $\gcd(7,8) = 1$ we can apply the Chinese Remainder Theorem.

$$\begin{aligned} 7a + 8b &= 1 \\ 7(-1) + 8(1) &= 1 \\ 4(7)(-1) + 6(1)(8) &= 48 - 28 = 20 \text{ is a specific solution} \\ 20 + 7 \cdot 8t &= 20 + 56t \text{ is all solutions} \end{aligned}$$

2.1 8. Which of the following formulas define functions from the set of rational numbers into itself? (Assume in each case the n, m are integers and that n is nonzero.)

(a) $f\left(\frac{m}{n}\right) = \frac{m+1}{n+1}$
Not a function from $\mathbb{Q} \to \mathbb{Q}$ because when $n = -1$ there is no image.

(b) $g\left(\frac{m}{n}\right) = \frac{2m}{3n}$
This is a function because rational numbers are closed under multiplication so for any $q \in \mathbb{Q}$ we know that $\frac{2}{3}q \in \mathbb{Q}$

(c) $h\left(\frac{m}{n}\right) = \frac{m+n}{n^2}$
This is not a function. Counterexample: $\frac{1}{2} = \frac{2}{4}$. $\frac{1+2}{2^2} = \frac{3}{4} \neq \frac{2+4}{4^2} = \frac{6}{16} = \frac{3}{8}$. $\frac{1}{2}$ has more than one image so the map is not well defined and not a function.

(d) $k\left(\frac{m}{n}\right) = \frac{(m-n)^2}{n^2}$
$\frac{(m-n)^2}{n^2} = \frac{m^2 - 2mn + n^2}{n^2} = \left(\frac{m}{n}\right)^2 - 2\frac{m}{n} + 1$. Looks like a good function. It will have the same result independent of representation of the rational number, and has an image for every element of $\mathbb{Q}$.

(e) $p\left(\frac{m}{n}\right) = \frac{4m^2}{7n^2} - \frac{m}{n}$
Is a function of rationals. They are closed under multiplication and subtraction. all equivalent elements will have the same image, regardless if their representation in terms of m, n.

(f) $q\left(\frac{m}{n}\right) = \frac{m+1}{m}$
Not a function. No representation of zero has an image. For example $\frac{0}{1}$ does not have an image as $\frac{1}{0}$ is undefined.

18. Let A be a nonempty set, and let $f : A \to B$ be a function. Prove that f is one-to-one if and only if there exists a function $g : B \to A$ such that $g \circ f = 1_A$

proof

Lets start by assuming that f is a one to one function. Because f is a function, we know that for every $x \in A$ there exists some $x' \in B$. Furthermore, because f is one to one, we know that x' is unique. Now we simply define $g(x') = x$. If B has more elements than A then we can define those elements that aren't images of A under f to map to random $a \in A$. Now we see that $g(f(x)) = g(x') = x$ and so we've found a function that satisfies our result.

Now let us assume that the function f is not one to one. Because f is a function, we can't have any elements of A map to more than one element in B. Therefore $|f| \leq |A|$. Now because f is not one to one, we know that there are two elements in A that have the same image in B. This makes our cardinality inequality strict: $|f| < |A|$. This means that if we have a function $g : B \to A$ and feed it the images created by f it will only be able to spit out at most $|A| - 1$ images of it's own. So we have $|g \circ f| < |A|$. Because $|g \circ f| \neq |A|$ it is certain that $g \circ f \neq 1_A$ $\square$