E. Dummit's Math 1465 ~ Intensive Mathematical Reasoning, Fall 2024 ~ Homework 9, due Tue Nov 12th.

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly, and clearly identify all problem numbers. Identify all pages containing each problem when submitting the assignment.

Part I: No justifications are required for these problems. Answers will be graded on correctness.

1. For each function $f : A \to B$, decide if f is a bijection, and if so, give a formula or otherwise describe f^{-1}.

   (a) $f_1 = \{(1,3),(2,4),(3,2)\}$ from $A = \{1,2,3\}$ to $B = \{2,3,4\}$.

   - We can see from the list of pairs that f_1 is one-to-one and onto so it $\boxed{\text{is a bijection}}$, and $f_1^{-1} = \boxed{\{(3,1),(4,2),(2,3)\}}$ is simply the inverse relation of f_1.

   (b) $f_2 = \{(1,3),(2,4),(3,3)\}$ from $A = \{1,2,3\}$ to $B = \{2,3,4\}$.

   - From the list of pairs we see f_2 is neither one-to-one (since $f(1) = f(3)$) nor onto (since $2 \notin \text{im}(f)$) so it $\boxed{\text{is not a bijection}}$.

   (c) $f_3(x) = 2x + 3$ from $A = \mathbb{Q}$ to $B = \mathbb{Q}$.

   - First, f_3 is one-to-one since $f_3(a) = f_3(b)$ yields $2a + 3 = 2b + 3$ hence $a = b$. Also, f_3 is onto since $f_3(\frac{y-3}{2}) = y$ for any $y \in \mathbb{Q}$: thus f_3 $\boxed{\text{is a bijection}}$.
   - Alternatively, we could just try to compute the inverse function directly: solving $y = 2x + 3$ for x yields $x = \frac{y-3}{2}$ which is a function from B to A. So we see f_3^{-1} exists and is given by $\boxed{f_3^{-1}(y) = \frac{y-3}{2}}$.

   (d) $f_4(x) = 2x + 3$ from $A = \mathbb{Z}$ to $B = \mathbb{Z}$.

   - Here we can see that f_3 is one-to-one but not onto as a function from $\mathbb{Z}$ to $\mathbb{Z}$ (as its image is only the odd integers) so f_4 $\boxed{\text{is not a bijection}}$.

   (e) $f_5(x) = \dfrac{2x-1}{x+3}$ from $A = \mathbb{Q}\backslash\{-3\}$ to $B = \mathbb{Q}\backslash\{2\}$.

   - Solving $y = \frac{2x-1}{x+3}$ for x yields $x = \frac{3y+1}{2-y}$. Since this is a well-defined function from B to A, we see that f_5 $\boxed{\text{is a bijection}}$ and that $\boxed{f_5^{-1}(y) = \frac{3y+1}{2-y}}$.

---

2. In class, we showed that if A is a finite set and $f : A \to A$ is a function, then f is one-to-one if and only if f is onto. The goal of this problem is for you to show via example that both implications are FALSE in the situation where A is an infinite set.

   (a) Find an example of a function $f : \mathbb{Z}_+ \to \mathbb{Z}_+$ that is one-to-one but not onto.

   - There are many possibilities, but a very simple one is $f(n) = n + 1$. This function is clearly one-to-one, but it is not onto since 1 is missing from the image of f.

   (b) Find an example of a function $f : \mathbb{Z}_+ \to \mathbb{Z}_+$ that is onto but not one-to-one.

   - There are many possibilities, but a simple one is $f(n) = \begin{cases} 1 & \text{if } n = 1,2 \\ n-1 & \text{if } n > 2 \end{cases}$. This function is clearly onto, since $f(n+1) = n$ for every positive integer n, but it is not one-to-one since $f(1) = f(2)$.
   - Another option is $g(n) =$ the value of $n/2$ rounded up to the nearest integer. This function is clearly onto since $g(2n) = n$ but it is not one-to-one since for example $f(1) = f(2)$.

   (c) Find an example of a function $f : \mathbb{R} \to \mathbb{R}$ that is one-to-one but not onto.

   - There are many possibilities, but a fairly simple one is $f(x) = e^x$. This function is one-to-one, but it is not onto because e^x is always positive for any real number x.

(d) Find an example of a function $f : \mathbb{R} \to \mathbb{R}$ that is onto but not one-to-one.

- There are many possibilities, but a fairly simple one is $f(x) = x^3 - x$. This function is onto (as can be seen from its graph) but it is not one-to-one since for example $f(0) = 0 = f(1)$.
- Another fairly simple possibility is $f(x) = x \sin x$ whose graph also indicates it is onto, but it is not one-to-one since $f(0) = 0 = f(\pi)$.

---

3. Identify whether each of the following sets is (i) finite, (ii) countably infinite, or (iii) uncountably infinite:

(a) The set $\mathbb{Q}_+$ of positive rational numbers.

- This set is infinite and a subset of the countable set $\mathbb{Q}$, so it is $\boxed{\text{countably infinite}}$.

(b) The set $\mathbb{R}$ of real numbers.

- This set is $\boxed{\text{uncountably infinite}}$ by Cantor's diagonal argument.

(c) The Cartesian product $\{0, 1\} \times \{0, 1, 2, 3, 4, 5, 6, 7\}$

- Both sets are finite, so their Cartesian product is also $\boxed{\text{finite}}$.

(d) The Cartesian product $\{0, 1\} \times \mathbb{Z}$.

- The set is infinite since $\mathbb{Z}$ is infinite, and it is countable since both sets are countable. So it is $\boxed{\text{countably infinite}}$.

(e) The set of subsets of $\mathbb{Z}$.

- This set is certainly infinite, and by Cantor's theorem, this set is not countable. So it is $\boxed{\text{uncountably infinite}}$.

(f) The Cartesian product $\emptyset \times \mathbb{Z}$.

- The set is $\boxed{\text{finite}}$ since it is the empty set.

(g) The Cartesian product $\emptyset \times \mathbb{R}$.

- The set is $\boxed{\text{finite}}$ since it is (also) the empty set.

(h) The set of functions $f : \mathbb{R} \to \mathbb{R}$.

- Since this set contains the functions of the form $f(x) = c$ for each $c \in \mathbb{R}$, and this set is uncountable, the set of all functions is $\boxed{\text{uncountable}}$.

(i) The Cartesian product $\mathbb{Z} \times \mathbb{Q}$.

- The set is infinite since $\mathbb{Z}$ is infinite, and it is countable since both sets are countable. So it is $\boxed{\text{countably infinite}}$.

(j) The Cartesian product $\mathbb{Z} \times \mathbb{Q} \times \mathbb{R}$.

- The set is $\boxed{\text{uncountably infinite}}$ since $\mathbb{R}$ is uncountable and the other sets are nonempty.

(k) The power set of the power set of the power set of $\{1, 2, 3, 4, 5\}$.

- The power set of $\{1, 2, 3, 4, 5\}$ is finite (it has 2^5 elements) and so its power set is also $\boxed{\text{finite}}$ (it has 2^{2^5} elements).

(l) The set $\mathbb{R} \backslash \mathbb{Q}$ of irrational numbers.

- The set is $\boxed{\text{uncountably infinite}}$ since otherwise $\mathbb{R}$ would be the union of two countable sets $\mathbb{R} \backslash \mathbb{Q}$ and $\mathbb{Q}$ hence would also be countable.

---

4. Suppose $f : A \to B$ and $g : B \to A$ are functions.

   (a) Show that if f is one-to-one and $f \circ g = i_B$ is the identity on B, then $g = f^{-1}$.
   - As shown in class, if $f \circ g = i_B$ then f is onto: for any $b \in B$ taking $a = g(b)$ yields $f(a) = f(g(b)) = b$.
   - Thus f is one-to-one and onto hence a bijection, so it has an inverse f^{-1}. Then $g = i_A \circ g = (f^{-1} \circ f) \circ g = f^{-1} \circ (f \circ g) = f^{-1} \circ i_B = f^{-1}$.

   (b) Show that if f is onto and $g \circ f = i_A$ is the identity on A, then $g = f^{-1}$.
   - As shown in class, if $g \circ f = i_B$ then f is one-to-one: if $f(a_1) = f(a_2)$ then $a_1 = g(f(a_1)) = g(f(a_2)) = a_2$.
   - Thus f is one-to-one and onto hence a bijection, so it has an inverse f^{-1}. Then a similar calculation as in (a) yields $g = f^{-1}$.

   (c) Suppose that $f \circ g = i_B$ but $g \circ f \neq i_A$. Show that f is onto but not one-to-one and g is one-to-one but not onto.
   - As noted in (a), if $f \circ g = i_B$ then f is onto, and as noted in (b), this relation also implies g is one-to-one.
   - If f were also one-to-one then by (a) that would imply $g = f^{-1}$ but this is not true because $g \circ f \neq i_A$, so f cannot be one-to-one.
   - Likewise, if g were also onto then by (b) that would imply $g = f^{-1}$ but this is not true because $g \circ f \neq i_A$, so g cannot be onto.

---

5. Let p be a prime and a be an integer relatively prime to p. The goal of this problem is to give another proof that $a^p \equiv a \pmod{p}$.

   (a) If S is the set of residue classes modulo p, prove that the function $f : S \to S$ given by $f(\overline{b}) = \overline{a} \cdot \overline{b}$ is a bijection. [Hint: $\overline{a}$ has a multiplicative inverse $\overline{a}^{-1}$ modulo p.]
   - As noted in the hint, since $\overline{a}$ is relatively prime to p, $\overline{a}$ has a multiplicative inverse $\overline{a}^{-1}$ modulo p such that $\overline{a}^{-1} \cdot \overline{a} = \overline{1}$.
   - Now observe that the map $g : S \to S$ given by $g(\overline{b}) = \overline{a}^{-1} \cdot \overline{b}$ is a two-sided inverse function for f: we see $f(g(\overline{b})) = \overline{a} \cdot \overline{a}^{-1} \cdot \overline{b} = \overline{1} \cdot \overline{b} = \overline{b}$ and also $g(f(\overline{b})) = \overline{a}^{-1} \cdot \overline{a} \cdot \overline{b} = \overline{1} \cdot \overline{b} = \overline{b}$.
   - Hence f is invertible so it is a bijection as claimed.

   (b) Show that $\overline{a} \cdot \overline{2a} \cdot \overline{3a} \cdot \cdots \cdot \overline{(p-1)a} = \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \cdots \cdot \overline{p-1}$ modulo p. [Hint: Use (a) to show that the two products consist of the same terms, merely rearranged.]
   - With $f(\overline{b}) = \overline{ab}$ as in (a), since $f(\overline{0}) = \overline{0}$ and f is a bijection, f maps the nonzero residue classes to themselves.
   - In particular, this means that the products $\overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \cdots \cdot \overline{p-1}$ and $\overline{a} \cdot \overline{2a} \cdot \overline{3a} \cdot \cdots \cdot \overline{(p-1)a}$ consist of the same terms, merely rearranged, and are therefore equal.

   (c) Prove that $\overline{a}^{p-1} = \overline{1}$ modulo p, and deduce that $a^p \equiv a \pmod{p}$.
   - From the result of (b) we see that $\overline{a} \cdot \overline{2a} \cdot \overline{3a} \cdot \cdots \cdot \overline{(p-1)a} = \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \cdots \cdot \overline{p-1}$ modulo p.
   - Factoring out the a from each term on the left-hand side yields $\overline{a}^{p-1}(\overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \cdots \overline{p-1}) = \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \cdots \overline{p-1}$.
   - Now we can simply cancel each of the terms in the product $\overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \cdots \cdot \overline{p-1}$ from both sides, because they are all invertible modulo p.
   - Cancelling yields the claimed $\overline{a}^{p-1} = \overline{1}$. Finally, since this equivalently says $a^{p-1} \equiv 1 \pmod{p}$, multiplying by a yields $a^p \equiv a \pmod{p}$.

---

6. Suppose $f : \mathbb{Z} \to \mathbb{Z}$ is a function such that $f(f(f(n)) = n$ for all $n \in \mathbb{Z}$.

   (a) Show that f is a bijection.
   - Observe that f is one-to-one, since if $f(a) = f(b)$ then applying f twice yields $f(f(f(a))) = f(f(f(b)))$ so that $a = b$.
   - Also, f is onto, since for any $n \in \mathbb{Z}$, if we take $a = f(f(n))$, we have $f(a) = f(f(f(n))) = n$.

(b) Give an example of such a function f that is NOT equal to the identity function. (You don't need to give an explicit formula, but at least describe how to find the values of f.)

- The idea is to arrange the values of f in cycles of three, so that applying the function three times returns each value back to its start.
- One option is to send $0 \to 1 \to 2 \to 0$, $3 \to 4 \to 5 \to 3$, $6 \to 7 \to 8 \to 6$, and so forth. Explicitly, we have $f(3n) = 3n+1$, $f(3n+1) = 3n+2$, and $f(3n+2) = 3n$ for each integer n.

---

7. The goal of this problem is to give another proof that $\mathbb{Q}$ is countable. Consider the function $f : \mathbb{Q}_+ \to \mathbb{Z}_+$ defined as follows: for positive $a/b \in \mathbb{Q}$ in lowest terms with prime factorizations $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $b = q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l}$, set $f(a/b) = p_1^{2a_1} p_2^{2a_2} \cdots p_k^{2a_k} q_1^{2b_1-1} q_2^{2b_2-1} \cdots q_l^{2b_l-1}$.

Example: Since $9 = 3^2$ and $14 = 2^1 \cdot 7^1$, we have $f(9/14) = 3^{2\cdot 2} \cdot 2^{2\cdot 1-1} \cdot 7^{2\cdot 1-1} = 3^4 2^1 7^1$.

Example: Since 1 is the empty product and $16 = 2^4$, we have $f(1/16) = 1 \cdot 2^{2\cdot 4-1} = 2^7$. Since $2/32 = 1/16$ we also have $f(2/32) = 2^7$.

(a) Find $f(7/3)$, $f(3/7)$, $f(40/3)$, $f(80/6)$, $f(3)$, $f(1/3)$, and $f(1)$.

- We have $f(7/3) = 7^2 \cdot 3^{2-1} = 7^2 3^1$, $f(3/7) = 3^2 7^{2-1} = 3^2 7^1$, $f(40/3) = 2^6 5^2 3^1$, $f(80/6) = f(40/3) = 2^6 5^2 3^1$, $f(3) = 3^2$, $f(1/3) = 3^1$, and $f(1) = 1$.

(b) Explain why $f(a/b)$ is a positive integer for every positive rational number a/b.

- All of the exponents $p_i^{2a_i}$ are nonnegative, as are all of the exponents $q_i^{2b_i-1}$, so the product $p_1^{2a_1} p_2^{2a_2} \cdots p_k^{2a_k} q_1^{2b_1-1} q_2^{2b_2-1} \cdots q_l^{2b_l-1}$ is an integer.

(c) Show that f is one-to-one. [Hint: You will need to use the fact that the primes $p_1, \ldots, p_k$ and $q_1, \ldots, q_l$ are all distinct.]

- Suppose $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $b = q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l}$ with a/b in lowest terms, so that the primes p_i and q_j are all distinct.
- Now suppose $c = r_1^{c_1} r_2^{c_2} \cdots r_m^{c_m}$ and $d = s_1^{d_1} s_2^{d_2} \cdots s_n^{d_n}$ has c/d in lowest terms, so that the primes r_i and s_j are also all distinct, and suppose $f(a/b) = f(c/d)$.
- Comparing factorizations $p_1^{2a_1} p_2^{2a_2} \cdots p_k^{2a_k} q_1^{2b_1-1} q_2^{2b_2-1} \cdots q_l^{2b_l-1} = r_1^{2c_1} r_2^{2c_2} \cdots r_m^{2c_m} s_1^{2d_1-1} s_2^{2d_2-1} \cdots s_n^{2d_n-1}$. Since integers have unique prime factorizations, the primes on the right-hand side must be the same as the primes on the left-hand side, and the exponents must also agree correspondingly.
- Since each p_i and r_i has an even exponent, and each q_j and s_j has an odd exponent, and even numbers cannot equal odd numbers, the p_i must be the same as the r_i and the q_j must be the same as the s_j.
- Matching up the primes with their corresponding exponents yields $a = p_1^{2a_1} p_2^{2a_2} \cdots p_k^{2a_k} = r_1^{2c_1} r_2^{2c_2} \cdots r_m^{2c_m} = c$ and $b = q_1^{2b_1-1} q_2^{2b_2-1} \cdots q_l^{2b_l-1} = s_1^{2d_1-1} s_2^{2d_2-1} \cdots s_n^{2d_n-1} = d$ and thus $a/b = c/d$. Thus, f is one-to-one.

(d) Find $f^{-1}(2^7)$, $f^{-1}(9)$, $f^{-1}(12)$, and $f^{-1}(2^4 3^2 5^3 7^3 11^1)$.

- As noted in the second example, we have $f(1/16) = 2^7$, so taking the inverse yields $1/16 = f^{-1}(2^7)$.
- Likewise, from (a) we have $f(3) = 3^2$, so by taking the inverse we see $3 = f^{-1}(9)$.
- Similarly, since $12 = 2^2 3^1$ we have $f(2/3) = 2^2 3^1 = 12$ so $f^{-1}(12) = 2/3$.
- Finally, since $f(2^2 \cdot 3/(5^2 \cdot 7^2 \cdot 11)) = 2^4 3^2 5^3 7^3 11^1$ we have $f^{-1}(2^4 3^2 5^3 7^3 11^1) = 2^2 \cdot 3/(5^2 \cdot 7^2 \cdot 11)$.

(e) Show that f is onto.

- As motivated by (d) we can see that if we separate the primes in the factorization of n into those with even exponents $p_i^{2a_i}$ and odd exponents $q_j^{2b_j-1}$, with $n = p_1^{2a_1} p_2^{2a_2} \cdots p_k^{2a_k} q_1^{2b_1-1} q_2^{2b_2-1} \cdots q_l^{2b_l-1}$, then for $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $b = q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l}$ we have $f(a/b) = n$ and so f is onto.

(f) Deduce that f is a bijection and conclude that $\mathbb{Q}_+$ is countable.

- By (c) and (e) we see that f is one-to-one and onto, hence a bijection from $\mathbb{Q}_+$ to $\mathbb{Z}_+$, thus establishing that $\mathbb{Q}_+$ is countable.

---

8. The goal of this problem is to give another proof that the power set of the positive integers $\mathbb{Z}_+$ is uncountable. Let S be the set of infinite base-2 sequences $d_1d_2d_3d_4\ldots$, where each digit $d_i \in \{0,1\}$ for all $i \geq 1$.

   (a) Prove that S is uncountable. [Hint: Use Cantor's diagonal argument.]

   - Suppose by way of contradiction that S is countable, and arrange the elements of S as follows:

$$\begin{array}{rcl} s_1 & = & 0.d_{1,1}d_{2,1}d_{3,1}d_{4,1}\ldots \\ s_2 & = & 0.d_{1,2}d_{2,2}d_{3,2}d_{4,2}\ldots \\ s_3 & = & 0.d_{1,3}d_{2,3}d_{3,3}d_{4,3}\ldots \\ s_4 & = & 0.d_{1,4}d_{2,4}d_{3,3}d_{4,4}\ldots \\ \vdots & \vdots & \vdots \end{array}$$

   - Now construct a new sequence t using the diagonal elements $d_{i,i}$: if $d_{i,i} = 1$, set $e_i = 0$, and if $d_{i,i} = 1$, set $e_i = 0$.
   - Then $t \neq s_i$ since t and s_i differ in the ith digit. This means t is an element not on the list, which is a contradiction, so S is uncountable.

   (b) Show that the function $f : S \to \mathcal{P}(\mathbb{Z}_+)$ given by $f(d_1d_2d_3d_4\ldots) = \{n : d_n = 1\}$ is a bijection. Deduce that $\mathcal{P}(\mathbb{Z}_+)$ is uncountable.

   - First observe that f is one-to-one since $f(d_1d_2d_3d_4\ldots) = f(e_1e_2e_3e_4\ldots)$ only when $\{n : d_n = 1\} = \{n : e_n = 1\}$ only when $d_n = 1$ if and only if $e_n = 1$ if and only if $d_n = e_n$ for all n (since the only possible values of d_n and e_n are 0 and 1).
   - Additionally, f is onto, since for any subset $T \subseteq \mathbb{Z}_+$, the digit string $d_1d_2d_3d_4\ldots$ where $d_n = 1$ when $n \in T$ and $d_n = 0$ when $n \notin T$, has $f(d_1d_2d_3d_4\ldots) = T$ by definition. Thus f is a bijection.
   - Hence $\mathcal{P}(\mathbb{Z}_+)$ has the same cardinality as S, so by (a), $\mathcal{P}(\mathbb{Z}_+)$ is uncountable.
