E. Dummit's Math 1365 ∼ Intro to Proof, Fall 2022 ∼ Homework 9, due Tue Nov 15th.

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 of the following sets, identify whether it is finite, countably infinite, or uncountably infinite:

   (a) The set $\mathbb{Q}_{>0}$ of positive rational numbers.

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

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

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

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

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

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

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

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

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

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

   (l) The set of infinite sequences $(d_1, d_2, d_3, \dots, d_n, \dots)$ of base-10 digits.

Part II: Solve the following problems. Justify all answers with rigorous, clear arguments.

2. Suppose A, B, and C are sets.

   (a) If $f : B \to C$ and $g : A \to B$ are both one-to-one, prove that $f \circ g$ is also one-to-one.

   (b) If $f : B \to C$ and $g : A \to B$ are both onto, prove that $f \circ g$ is also onto.

---

3. 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 $f(\bar{b}) = \bar{a} \cdot \bar{b}$ is a bijection. [Hint: $\bar{a}$ has a multiplicative inverse $\bar{a}^{-1}$ modulo p.]

   (b) Suppose u_1, u_2, ... , u_{p-1} represent the distinct nonzero residue classes modulo p. Show that $(au_1) \cdot (au_2) \cdot \dots \cdot (au_{p-1}) \equiv u_1 \cdot u_2 \cdot \dots \cdot u_{p-1}$ modulo p. [Hint: Use (a) to show that the two products consist of the same terms, merely rearranged.]

   (c) Prove that $a^{p-1} \equiv 1 \pmod{p}$ and deduce that $a^p \equiv a \pmod{p}$.

---

4. The goal of this problem is to provide a different proof that there are infinitely many primes. If S is a set of integers, the characteristic function of S is the function $f : \mathbb{Z} \to \{0, 1\}$ defined by $f_S(n) = \begin{cases} 1 & \text{if } n \in S \\ 0 & \text{if } n \notin S \end{cases}$. We say a set S has period k if its characteristic function has period k, which is to say, if $f(n + k) = f(n)$ for all integers n. A set is periodic if it is periodic with some period k.

   (a) For a positive integer p, define $S_p = \{np : n \in \mathbb{Z}\}$. Show that S_p is periodic with period p.

   (b) Show that the complement of a periodic set is periodic.

   (c) Show that the characteristic function of $S \cup T$ is $f_{S \cup T}(n) = \max(f_S(n), f_T(n))$.

   (d) Show that the union of two periodic sets is periodic. [Hint: If S has period a and T has period b, show that $S \cup T$ has period ab.]

   (e) Suppose that there are finitely many prime numbers $\{p_1, p_2, ..., p_n\}$. Show that the complement of $S_{p_1} \cup S_{p_2} \cup ... \cup S_{p_n}$ is the set $\{-1, 1\}$. Explain why this is impossible and conclude that there are infinitely many prime numbers.

   - Remark: This approach to proving that there are infinitely many primes is an adaptation of a proof of Furstenberg.

---

5. 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 $a/b \in \mathbb{Q}$ 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 $f(a/b) = p_1^{2a_1} p_2^{2a_2} \cdots p_k^{2a_k} q_1^{2b_1-1} q_2^{2b_2-1} \cdots q_l^{2b_l-1}$.

   (a) Find $f(7/3)$, $f(9/14)$, $f(1/12)$, $f(1)$, and $f(1000/75)$.

   (b) Show that $f(a/b)$ is a positive integer for every positive rational number a/b.

   (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.]

   (d) Find $f^{-1}(12)$, $f^{-1}(180)$, $f^{-1}(2)$, and $f^{-1}(2^4 3^2 5^3 7^4 11^1)$.

   (e) Show that f is onto.

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

---

6. The goal of this problem is to give an alternate proof that $\mathbb{R}$ is uncountable. Let $f : \mathcal{P}(\mathbb{Z}_{>0}) \to \mathbb{R}$ be the function defined as follows: $f(A)$ is the decimal whose nth decimal place is 1 if $n \in A$, and is 2 if $n \notin A$.

   (a) Find the decimal expansion to 10 digits of the value of f on each of these sets: (i) the set of even integers, (ii) the set of odd integers, and (iii) the set of prime numbers.

   (b) Prove that f is one-to-one. [Hint: You may use the fact that $f(A)$ has a unique decimal expansion for any set A.]

   (c) Using the fact that $\mathcal{P}(\mathbb{Z}_{>0})$ is uncountable, show that $\mathbb{R}$ is uncountable.
