Proof Portfolio
Name: - Math 100 - Summer 2023

Here are the problems for Direct Proof: Choose two out of three of these

(1) Let $p \in \mathbb{Z}$. This question gives us two equivalent ways of thinking about prime numbers. Show that the following are equivalent: (ie, prove (a) iff (b))

(a) p has no factors other than 1 or itself

(b) If $p \mid ab$, for integers a and b, then $p \mid a$ or $p \mid b$.

(Hint: for $(a) \implies (b)$, you may use that if a and p have no common divisors, then there exist $n, m \in \mathbb{Z}$ such that $np + ma = 1$)

Solution:

(2) Show that $a \equiv b \bmod 10$ if and only if $a \equiv b \bmod 2$ and $a \equiv b \bmod 5$ (Hint: for one direction you will have to use something from question 1)

Solution:

(3) Let $a, b \in \mathbb{Z}$. Using only the definition of congruence, prove that if $a \equiv b \bmod n$, then $a^3 \equiv b^3 \bmod n$.

Solution:

Here are the problems for Contrapositive: Choose two out of three of these

(1) Let $a.b \in \mathbb{Z}$. Show that if $a^2 + b^2 = c^2$ for some $c \in \mathbb{Z}$ then $3 \mid ab$

Solution:

(2) We call n a perfect square if $n = k^2$ for some integer k. Show that if either

$$n \equiv 2 \bmod 4 \text{ or } n \equiv 3 \bmod 4$$

then n is not a perfect square.

Solution:

(3) Suppose $m, n, t \in \mathbb{Z}$. Prove the following:

(a) If $m^2(n^2+5)$ is even, then m is even or n is odd

(b) If $(m^2+4)(n^2-2mn)$ is odd, then m and n are odd

(c) If $m \nmid nt$ then $m \nmid n$ and $m \nmid t$

Solution:

Here are the problems for Contradiction: Choose two out of three of these

(1) We call $n \in \mathbb{N}$ composite if it is not prime. Show that for all composite numbers n there exists a nontrivial factor $1 < a < n$ such that $a \leq \sqrt{n}$

Solution:

(2) Let A, B be finite sets. Prove that if $A \subseteq B$ then $|A| \leq |B|$

Solution:

(3) Show that if $a, b \in \mathbb{Z}$ then $a^2 - 4b - 2 \neq 0$

Solution:

Here are the problems for Induction: Choose two out of three of these

(1) Prove that every $n \in \mathbb{N}$ has a unique prime decomposition $n = p_1 p_2 \ldots p_k$ for prime's p_i. That is, show there exists such a prime factorization as above, and moreover show that if we also have $n = q_1 q_2 \ldots q_l$ then $k = l$ and $p_i = q_j$ for some i, j (ie, show that the primes are all the same up to some reordering of the multiplication: For example $12 = 2 \times 2 \times 3 = 3 \times 2 \times 2 = 2 \times 3 \times 2$).

Solution:

(2) For $n \in \mathbb{N}$ prove that

$$\int_0^\infty x^n e^{-x} dx = n!$$

Solution:

(3) Let X be a finite set with cardinality $|X| = n$. Show that $|\mathcal{P}(X)| = 2^n$.
(Hint: count the number of subsets in two cases:

(1) when an element x_n is an element of a given subset
(2) when an element x_n is not an element of the given subset)

Solution:

Here are the problems for Set Proofs: Choose two out of three of these

(1) If A, B, C are sets: Prove that

(a) $(A \cap B)^c = A^c \cup B^c$
(b) $A - (B \cap C) = (A - B) \cup (A - C)$

Solution:

(2) Let $f : A \to B$ be a function. Recall that for $Y \subseteq B, X \subseteq A$ the pre-image of Y and the image of X are defined to be

$$f^{-1}(Y) = \{x \in A : f(x) \in Y\}$$
$$f(X) = \{z \in B : z = f(x) \text{ for some } x \in X\}$$

Prove or disprove the following

(a) $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$
(b) $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$
(c) $f(X_1 \cap X_2) = f(X_1) \cap f(X_2)$
(d) $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$

Solution:

(3) Let A and B be sets. Prove or disprove the following:

(a) $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$

(b) $\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B)$

Solution:

Here are the problems for Functions/Relations: Choose two out of three of these

(1) Define a function $f : \mathcal{P}(\mathbb{Z}) \to \mathcal{P}(\mathbb{Z})$ that sends a subset $X \subseteq \mathbb{Z}$ to its compliment X^c. Prove or disprove that this function is a bijection. If it is a bijection, find its inverse; if it is not, explain why.

Solution:

(2) Let R and S be equivalence relations on a set X. Prove or disprove the following:

(a) $R \cap S$ is an equivalence relation on X

(b) $R \cup S$ is an equivalence relation on X

Solution:

(3) Let $n \in \mathbb{N}$. We can define a multiplication on $\mathbb{Z}/n\mathbb{Z}$ by $[a][b] = [ab]$ (We will show this is well defined in class).

(a) Note that, in general, it is possible for two nonzero elements of $\mathbb{Z}/n\mathbb{Z}$ to multiply together to get [0] (for example, [2][2]=[0] in $\mathbb{Z}/4\mathbb{Z}$). We call a nonzero element $[0] \neq [x] \in \mathbb{Z}/n\mathbb{Z}$ a zero divisor if there exists another element $0 \neq [y]$ such that $[x][y] = [0]$. Prove that $\mathbb{Z}/n\mathbb{Z}$ has a zero divisor if and only if n is a composite number

(b) We call an element [x] a unit if there exists [y] such that $[x][y] = [1]$ (we think of these elements as the ones we can 'divide' by). First, convince yourself that for a general n, not every element is a unit. Next, prove that every nonzero element is a unit in $\mathbb{Z}/n\mathbb{Z}$ iff n is prime.
(Hint: for one direction you will use part (a). For the other direction you will again use the fact that if p is prime, and p does not divide a number a (ie, a and p have no common divisors), then there are integers n and m such that $np + ma = 1$)

Solution: