Math S–101. Midterm 1. Solutions.

T. Judson

Tuesday, July 18, 2006

1. Use the Division Algorithm to prove that all primes greater than 3 must be of the form $6k-1$ or $6k+1$ for some $k \in \mathbb{N}$.

   Solution. If p is a prime number greater than 3, then $p = 6k + r$ by the Division Algorithm, where $r = 0, 1, 2, 3, 4, 5$. If $r = 0, 2, 4$, then p is divisible by 2 and cannot be prime. If $r = 3$, then p is divisible by 3 and cannot be prime. Thus, $r = 1$ or 5. If $r = 5$, then $p = 6k + 5 = 6k + 6 - 1 = 6(k + 1) - 1$ and p is in the correct form.

2. Prove $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

   Solution. If $x \in A \cap (B \cup C)$, then $x \in A$ and $x \in B \cup C$. So $x \in A$ and either $x \in B$ or $x \in C$. Hence, either we have $x \in A$ and $x \in B$, or we have $x \in A$ and $x \in C$. Thus, $x \in A \cap B$ or $x \in A \cap C \Rightarrow x \in (A \cap B) \cup (A \cap C) \Rightarrow A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$.

   Conversely, let $x \in (A \cap B) \cup (A \cap C)$. Then either $x \in A \cap B$ or $x \in A \cap C$. It follows that $x \in A$, and either $x \in B$ or $x \in C$. So $x \in A$ and $x \in B \cup C \Rightarrow x \in A \cap (B \cup C) \Rightarrow (A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$.

3. Prove $(A \cup B) \times C = (A \times C) \cup (B \times C)$.

   Solution. If $(x, y) \in (A \cup B) \times C$, then $x \in A \cup B$ and $y \in C$. Thus $x \in A$ or $x \in B \Rightarrow (x, y) \in A \times C$ or $(x, y) \in B \times C \Rightarrow (x, y) \in (A \times C) \cup (B \times C) \Rightarrow (A \cup B) \times C \subset (A \times C) \cup (B \times C)$.

   Conversely, suppose that $(x, y) \in (A \times C) \cup (B \times C)$. Then $(x, y) \in A \times C$ or $(x, y) \in B \times C$. Thus, $x \in A$ or $x \in B$ while $y \in C$. Hence, $x \in A \cup B$ and $y \in C$. Therefore, $(x, y) \in (A \cup B) \times C$, or $(A \times C) \cup (B \times C) \subset (A \cup B) \times C$.

4. Define a relation $\sim$ on $\mathbb{R}^2$ by stating that $(a, b) \sim (c, d)$ if and only if $a^2 + b^2 \leq c^2 + d^2$. If the relation is an equivalence relation, describe the corresponding partition of $\mathbb{R}^2$. If the relation is not an equivalence relation, state why it fails to be one.

   Solution. The relation fails to be symmetric, since $(0, 0) \sim (1, 1)$ but $(1, 1) \not\sim (0, 0)$.

5. Let $f : X \to Y$ be a map with $A_1, A_2 \subset X$. Prove $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

   Solution. Let $y \in f(A_1 \cup A_2) \Rightarrow$ there exists an $x \in A_1 \cup A_2$ such that $f(x) = y \Rightarrow y \in f(A_1)$ or $f(A_2) \Rightarrow y \in f(A_1) \cup f(A_2) \Rightarrow f(A_1 \cup A_2) \subset f(A_1) \cup f(A_2)$.

   Conversely, let $y \in f(A_1) \cup f(A_2) \Rightarrow y \in f(A_1)$ or $f(A_2) \Rightarrow$ there exists an $x \in A_1$ or there exists an $x \in A_2$ such that $f(x) = y \Rightarrow$ there exists an $x \in A_1 \cup A_2$ such that $f(x) = y \Rightarrow f(A_1) \cup f(A_2) \subset f(A_1 \cup A_2)$. Hence, $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

6. Prove that
$$1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$$
for $n \in \mathbb{N}$.

Solution. We will prove this statement using mathematical induction.

$S(1) : [1^2(1+1)^2]/4 = 1 = 1^3$ is true.

Assume $S(k) : 1^3 + 2^3 + \cdots + k^3 = [k^2(k+1)^2]/4$ is true. Then
$$1^3 + 2^3 + \cdots + k^3 + (k+1)^3 = [k^2(k+1)^2]/4 + (k+1)^3 = [(k+1)^2((k+1)+1)^2)]/4,$$
so $S(k+1)$ is true; consequently, $S(n)$ is true for all positive integers n.

7. Let X be a set. Define the *power set* of X, denoted $\mathcal{P}(X)$, to be the set of all subsets of X. For example,
$$\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}.$$
If $X = \{1, 2, \ldots, n\}$ show that $\mathcal{P}(X)$ contains exactly 2^n elements.

Solution. We will prove this statement using mathematical induction. If $X = \{1\}$, then $\mathcal{P}(X) = \{\emptyset, \{1\}\}$, which contains $2^1 = 2$ elements. Now assume that $\mathcal{P}(\{1, 2, \ldots, n\})$ contains exactly 2^n elements. The only new subsets that can be created are in $\mathcal{P}(\{1, 2, \ldots, n, n+1\})$ are those obtained by adding the element $n+1$ to an existing subset. Thus,
$$|\mathcal{P}(\{1, 2, \ldots, n+1\}| = 2 \cdot |\mathcal{P}(\{1, 2, \ldots, n\}| = 2^{n+1}.$$

8. Prove that there are an infinite number of primes of the form $4m - 1$, where $m \in \mathbb{N}$. *Hint*: Assume there are only a finite number $p_1, p_2, \ldots, p_n$ of primes in the form $4m - 1$. Form a number $N = 4p_1p_2 \cdots p_n - 1$.

Solution. By the Division Algorithm, any integer can be written as $4m$, $4m+1$, $4m+2$, $4m+3$. Numbers of the form $4d$ and $4d+2$ are divisible by 4 and 2, respectively, and thus cannot be prime (except for 2). Numbers of the form $4d+1$ have the property that the product of any two of them is again a number in the same form: $(4k+1)(4m+1) = 4(k+m+4km)+1$. Also note that numbers in the form $4m+3$ may also be written as $4m+3 = 4(m+1)-1 = 4k-1$.

Assume there are only a finite number $p_1, p_2, \ldots, p_n$ of primes in the form $4m - 1$. Form a number $N = 4p_1p_2 \cdots p_n - 1$. Since N itself is in the form $4m - 1$, all of its prime factors cannot be in the form $4m+1$. Therefore, there must be at least one prime factor in the form $p = 4m - 1$. Whatever it is, it must be different from any of $p_1, p_2, \ldots, p_n$; otherwise p would divide $4p_1p_2 \cdots p_n - P = 1$.