Introduction to advanced mathematics
2nd Midterm Examples

November 7, 2022

Instruction

The midterm consists of 3 problems, each worth 34 points (The maximal grade is 100). For this you will have 45 minutes during class. The identities file will be appended to the exam and no other material is allowed. The answers to the problems should be answered in the designated areas.

Examples for problems

Problem 1. Prove that $(A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C)$.

Proof. We need to prove a set equality. We will prove that by a double inclusion:

- $\underline{(A \setminus B) \setminus C \subseteq (A \setminus C) \setminus (B \setminus C)}$: Let $a \in (A \setminus B) \setminus C$, we want to prove that $a \in (A \setminus C) \setminus (B \setminus C)$. By definition of difference we know that $a \in A \setminus B$ and $a \notin C$ and therefore $a \in A$ and $a \notin B$. Since $a \in A$ and $a \notin C$, it follows that $a \in A \setminus C$ and since $a \notin B$ it follows that $a \notin B \setminus C$. Thus $a \in (A \setminus C) \setminus (B \setminus C)$.

- $\underline{(A \setminus C) \setminus (B \setminus C) \subseteq (A \setminus B) \setminus C}$: Let $a \in (A \setminus C) \setminus (B \setminus C)$ we want to prove that $a \in (A \setminus B) \setminus C$. By definition $a \in A \setminus C$ and $a \notin B \setminus C$. By definition, $a \in A$ and $a \notin C$. Also, since $a \notin B \setminus C$, then $a \notin B$ **or** $a \in C$. Since $a \notin C$, it follows that $a \notin B$. Since $a \in A$ and $a \notin B$, $a \in A \setminus B$. Since $a \notin C$, it follows that $a \in (A \setminus B) \setminus C$.

$\square$

Problem 2. Prove by induction that for every $n \in \mathbb{N}_+$, $1+3+...+(2n-1) = n^2$.

Proof.

- Base: For $n = 1$, we want to prove that $1 = 1^2$ which is clear.
- Induction hypothesis: Suppose that

$$1 + 3 + 5 + ... + (2n - 1) = n^2$$

  for some general n.

- Induction step: We want to prove that

$$1 + 3 + 5... + (2n - 1) + (2(n + 1) - 1) = (n + 1)^2$$

  Indeed, by the induction hypothesis

$$[1 + 3 + .. + (2n - 1)] + (2n + 1) = [n^2] + (2n + 1) = (n + 1)^2$$

$\square$

Problem 3. Prove that for every integer $n > 0$, $n, n + 1$ are coprime.

Proof. Let $n > 0$ be any integer. We want to prove that $n, n+1$ are coprime. Note that

$$1 \cdot (n + 1) + (-1) \cdot n = n + 1 - n = 1$$

Thus 1 is a linear combination of $n + 1$ and n. By the Beźout Identity, this implies that $n, n + 1$ are coprime. $\square$

Problem 4. Prove that for all $n \in \mathbb{N}$, $9^n - 5^n$ is divisible by 4.

Proof. By induction on n,

- Base: For $n = 0$ we have that $9^0 - 5^0 = 1 - 1 = 0$ which is divisible by 4 (since $0 = 4 \cdot 0$).
- Induction hypothesis: Suppose that for some general n, $9^n - 5^n$ is divisible by 4.

- Induction step: We want to prove that $9^{n+1} - 5^{n+1}$ is divisible by 4. Indeed,

  $$9^{n+1} - 5^{n+1} = 9 \cdot 9^n - 5 \cdot 5^n = 9 \cdot 9^n - 9 \cdot 5^n + 4 \cdot 5^n = 9(9^n - 5^n) + 4 \cdot 5^n$$

  By the induction hypothesis $9^n - 5^n$ is divisible by 4 and therefore the term $9(9^n - 5^n)$ divisible by 4. Clearly, the $4 \cdot 5^n$ is divisible by 4 and therefore $9^{n+1} - 5^{n+1}$ is divisible by 4.

$\square$

Problem 5. Express the following sets using the list principle. No proof required.

1. $(-5, 5) \cap \mathbb{Z} = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$.
2. $\{\emptyset, 1\} \times \{n \in \mathbb{N} \mid |P(\{0, \ldots, n\})| < 4\} = \{\emptyset, 1\} \times \{0\} = \{\langle \emptyset, 0\rangle, \langle 1, 0\rangle\}$.
   Explanation: Note that $\{n \in \mathbb{N} \mid |P(\{0, \ldots, n\})| < 4 = \{n \in \mathbb{N} \mid 2^{n+1} < 4\} = \{0\}$
3. $\{\langle x, y\rangle \in \mathbb{R}^2 \mid x^2 + y^2 = 1\} \cap \{\langle x, x\rangle \mid x \in \mathbb{R}\} = \{\langle -\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\rangle, \langle \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\rangle\}$.
   Explanation: a pair in the intersection is a pair of the form $\langle x, x\rangle$ such that $x^2 + x^2 = 1$, namely $2x^2 = 1$ and therefore $x^2 = \frac{1}{2}$. It follows that there exactly two such x's $x = \frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}$. Note that this is the intersection of the unit circle or radius 1 around the origin with the line $y = x$.

Problem 6. Compute the following

1. Compute A_3, where A_n is defined recursively by $A_0 = \emptyset$ and $A_{n+1} = A_n \cup \{A_n\}$.
   Solution: $A_0 = \emptyset$
   $A_1 = A_0 \cup \{A_0\} = \emptyset \cup \{\emptyset\} = \{\emptyset\}$
   $A_2 = A_1 \cup \{A_1\} = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}$
   $A_3 = A_2 \cup \{A_2\} = \{\emptyset, \{\emptyset\}\} \cup \{\{\emptyset, \{\emptyset\}\}\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$
2. a_4 where a_n is defined recursively by $a_0 = 0$ and $a_{n+1} = 2^{a_n}$
   Solution: $a_0 = 0$
   $a_1 = 2^{a_0} = 2^2 = 1$
   $a_2 = 2^{a_1} = 2^1 = 2$
   $a_3 = 2^{a_2} = 2^2 = 4$
   $a_4 = 2^{a_3} = 2^4 = 16$

3. a_{100} where a_n is defined recursively by $a_0 = 2$, $a_1 = 3$ and $a_{n+1} = gcd(a_n, a_{n-1}) + 1$.
   Solution: $a_0 = 2$
   $a_1 = 3$
   $a_2 = gcd(2,3) + 1 = 1 + 1 = 2$
   $a_3 = gcd(3,2) + 1 = 1 + 1 = 2$
   $a_4 = gcd(2,2) + 1 = 2 + 1 = 3$
   $a_5 = gcd(3,2) + 1 = 2$
   $a_6 = gcd(2,3) + 1 = 2$
   $a_7 = gcd(2,2) + 1 = 3$ We see that any number of the form $3k + 1$ e.g. 1,4,7,10,13,16,19,...) satisfy that $a_k = 3$. Since $100 = 3 \cdot 99 + 1$ we have that $a_{100} = 3$.

Two more problems:

Problem 7. Prove that for any integers n_1, n_2, m, where $m > 0$,

$$n_1 \text{mod} m = 1 \Rightarrow n_1 \cdot n_2 \equiv n_2 (\text{mod} m).$$

Proof. Let n_1, n_2, m be integers such that $m > 0$. Suppose that $n_1 \text{mod} m = 1$, we want to prove that $n_1 \cdot n_2 \equiv n_2 (\text{mod} m)$. By definition of the remainder, it follows that $n_1 = qm + 1$. Apply the division theorem there are q', r such that $n_2 = q'm + r$. Again by definition of remainder $n_2 \text{mod}(m) = r$. It follows that:

$$n_1 n_2 = (qm + 1)(q'm + r) = qq'm^2 + q'm + qmr + r = m(qq'm + q' + q) + r$$

Hence by definition, we have that

$$n_1 n_2 \text{mod} m = r = n_2 \text{mod} m$$

By definition of congruence, it follows that

$$n_1 n_2 \equiv n_2 (\text{mod} m)$$

□