

Math 52B Practice Problems for Final Examination (3:30 pm 12/17/09)

Exam problems will be similar to some of these, but the exam will be shorter

1. SETS

- Define what it means to say that S is a subset of T .
- Show that $S = \{a \in \mathbb{Z} : a \equiv 3 \pmod{5}\}$ is a subset of $T = \{a \in \mathbb{Z} : a^2 \equiv 4 \pmod{5}\}$
- Suppose that S and W are subsets of T . Prove that $S \cap (S \cup W) = S$

RELATIONS

- In this problem, $X = \{1, 2, 3, 4\}$ and $P(X)$ is the collection of all subsets of X (called the “power set” of X).
 - How many subsets does X have?
 - We define a relation ρ on $P(X)$, i.e. on the subsets of X . So S and T will represent two subsets of X . Remember that the number of elements in S is denoted by $|S|$. The relation is $\rho = \{(S, T) : |S| = |T|\}$. So the subset S is related to the subset T if and only if S has the same number of elements as T . Show that ρ is an equivalence relation.
 - Write out the equivalence class of $S = \{1, 3, 4\}$.
 - How many different equivalence classes are there?
 - How many different equivalence classes does the subset $\{2, 4\}$ belong to?
 - State a theorem about equivalence relations.
- Two triangles T_1 and T_2 are similar if you can multiply the lengths of the sides of T_1 by a positive real number r and get the lengths of the sides of T_2 .
 - Show that similarity is an equivalence relation on the set of all triangles.
 - Show that all equilateral triangles are in the same equivalence class for the equivalence relation in part (a).
 - Show that there are infinitely many different equivalence classes of isosceles triangles.

4. INDUCTION

- Prove by induction that if $a \equiv b \pmod{m}$ then $a^n \equiv b^n \pmod{m}$ for every positive integer n .
- A sequence is defined by $a_1 = 3$, $a_2 = 3$, and $a_{n+1} = a_n + 2a_{n-1}$ for $n \geq 1$. Prove by complete induction that $a_n = (2)^n - (-1)^n$ for all positive integers n .

5. THE EUCLIDEAN ALGORITHM

- Describe the Extended Euclidean algorithm, what it is used for, and what the steps in the algorithm are.
- Suppose that a and b are two positive integers, and their greatest common divisor is g . Show that if d is a positive integer such that $d|a$ and $d|b$, then $d|g$.
- Show how to use the Euclidean algorithm to solve for x and y such that $37x + 99y = 1$.
- Use part (c) to find $37^{-1} \pmod{99}$.
- Use your answers above to solve for z such that $37z \equiv 10 \pmod{99}$.

6. LOGIC

- Define what it means for two logical statements to be equivalent.
- If A and B are two statements, show that the statement $\neg A \wedge (A \vee B)$ is equivalent to the statement $B \wedge \neg A$.
- Write the converse and the contrapositive of the statement “If you ace Math 52, then you understand modular arithmetic and you understand equivalence relations.” Which of these is equivalent to the original statement?

7. FUNCTIONS

- According to our formal definition, what is a function?
- Let $S = \{2, 4, 6\}$ and $T = \{7, 8, 9, 10\}$. Define a relation σ from S to T by $\sigma = \{(2, 8), (4, 7), (6, 8)\}$. Show that σ is a function from S to T .
- What is the definition of one-to-one?
- Show that σ is not one-to-one.
- What is the definition of onto?
- Show that σ is not onto.
- What is the range of σ ? Write out this set.
- Does σ have an inverse function? Does σ have an inverse relation? Why or why not?
- Suppose that f is a function from X to Y and g is a function from Y to Z . If f and g are onto, prove that $g \circ f$ is onto.
- If f and g have inverse functions, prove that $g \circ f$ has an inverse, namely $f^{-1} \circ g^{-1}$.

8. MODULAR ARITHMETIC

- Write the table for multiplication in $\mathbb{Z}/7\mathbb{Z}$.
- Suppose that p is a prime number greater than 2. Show that 2 has an inverse modulo p .
- Let $b = 2^{-1} \pmod{p}$. Define a function $f : \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ by $f(x) = 2x \pmod{p}$ and define $g(y) = by \pmod{p}$. Show that g is the inverse function of f .
- Show that f is a bijection.
- Use part (d) to show that

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-2)(p-1) \equiv (2 \cdot 1) \cdot (2 \cdot 2) \cdot (2 \cdot 3) \cdots (2 \cdot (p-2))(2 \cdot (p-1)) = 2^{p-1}(p-1)! \pmod{p}.$$

- Show that $1 \equiv 2^{p-1} \pmod{p}$. Congratulations, you have proved Fermat's Little Theorem again. (This same argument works for any number from 1 to $p-1$ in place of 2.)
- If $A \equiv a \pmod{mn}$, show that $A \equiv a \pmod{m}$ and $A \equiv a \pmod{n}$. Show that the converse is not always true, but it is true if $\text{GCD}(m, n) = 1$.
- Use Fermat's Little Theorem to prove that if a is not a multiple of 13 or 5 or 7, then $a^{12} \equiv 1 \pmod{13}$ and $a^{12} \equiv 1 \pmod{7}$ and $a^{12} \equiv 1 \pmod{5}$, so $a^{12} \equiv 1 \pmod{5 \cdot 7 \cdot 13}$.
- Find the smallest positive integer A such that $A \equiv 7 \pmod{31}$ and $A \equiv 9 \pmod{35}$.

9. MATHEMATICAL WRITING

Summarize how one of the following topics (your choice) unfolded in this course: Logic, Sets, Relations, Functions, or Modular Arithmetic. Include statements of important definitions and theorems in a logical order, and at least one proof. Follow the guidelines for clear mathematical writing.