

Math 52B Practice Problems for Final Examination (8am 5/8/09)
Exam problems will be similar to some of these, but the exam will be shorter

1. SETS AND RELATIONS

- a. Define what it means to say that S is a subset of T .
- b. Show that $S = \{a \in \mathbb{Z} : a \equiv 3 \pmod{5}\}$ is a subset of $T = \{a \in \mathbb{Z} : a^2 \equiv 4 \pmod{5}\}$
- c. Suppose that X is a set and $P(X)$ is the collection of all subsets of X (called the “power set” of X). We define a relation ρ on $P(X)$, i.e. on the subsets of X . The relation is $\rho = \{(S, T) : S \subset T\}$. So the subset S is related to the subset T if and only if $S \subset T$. Show that ρ is a partial order relation.
- d. 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 this is an equivalence relation on the set of all triangles.
- e. Show that all equilateral triangles are in the same equivalence class for the equivalence relation in part (c).
- f. Show that there are infinitely many different equivalence classes of isosceles triangles.

2. **INDUCTION** Prove by induction that if $a \equiv b \pmod{m}$ then $a^n \equiv b^n \pmod{m}$ for every positive integer n .

3. THE EUCLIDEAN ALGORITHM

- a. Describe the Extended Euclidean algorithm, what it is used for, and what the steps in the algorithm are.
- b. 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 $d|g$.
- c. Show how to use the Euclidean algorithm to solve for x such that $37x \equiv 51 \pmod{423}$

4. NUMBER REPRESENTATIONS

- a. Explain the method for finding the representation of a positive integer x in base b .
- b. Is this method an algorithm? Explain.
- c. Find the representation of 213 in base 5.
- d. Convert $(0.314)_5$ to base 10.
- d. Prove the formula for a repeating decimal in base b : $(\overline{a_1 a_2})_b = (a_1 b + a_2)/(b^2 - 1)$

5. LOGIC

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

6. 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 $\sigma = \{(2, 8), (4, 7), (6, 9)\}$. Show that σ is a function.
- What is the definition of one-to-one?
- Show that σ is one-to-one.
- Why doesn't σ have an inverse function?
- Now suppose that we consider σ to be a function from $S = \{2, 4, 6\}$ to $R = \{7, 8, 9\}$. Write down the inverse function of σ from R to S .
- Suppose that f and g are functions for which we can define $f \circ g$. If f and g are one-to-one, prove that $f \circ g$ is one-to-one.
- If f and g have inverse functions, prove that $f \circ g$ has an inverse, namely $g^{-1} \circ f^{-1}$.

7. 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.)
- State the definition of the Euler phi function and State the Euler-Fermat Theorem.
- 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 $GCD(m, n) = 1$.
- Use Fermat's Little Theorem and the Chinese remainder 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 $a^{12} \equiv 1 \pmod{5 \cdot 7 \cdot 13}$.

8. COMPLEX NUMBERS

- State DeMoivre's Theorem.
- Prove that $\overline{e^z} = e^{\bar{z}}$.
- Prove that $(e^{i\theta})^{-1} = e^{-i\theta}$.
- Prove that $(e^{i\theta})^{-m} = e^{-im\theta}$ for any positive integer m .
- Simplify the complex number $(2 - 7i)/(3 + 4i)$.

9. **ESSAY** Write an outline of the development of one of the following topics (your choice): Logic, Sets, Relations, Functions, Modular Arithmetic, Complex Numbers. Include statements of important definitions and theorems, and at least one proof.