Math 112 final exam review

The final exam covers everything that we have done this quarter. There will be some emphasis on mod n arithmetic since this did not appear on your midterms.

Topics include:

- Sets, numbers and rules of arithmetic
- Using the axioms of arithmetic to prove theorems; verifying whether an arithmetic system satisfies all or some of the axioms
- Inequalities and orders, well-ordering, using the order axioms to prove theorems, verifying whether an order $<$ satisfies all or some of the axioms
- Divisors, greatest common divisors, proofs using the definition of "divides"
- Prime numbers (including factoring integers into primes)
- The division algorithm theorem (finding remainders), the Euclidean algorithm, using the Euclidean algorithm to find greatest common divisors or to solve a Diophantine equation.
- Mod n (remainder) arithmetic, units, zero divisors, etc. Applications.
- Groups (order, generators, etc)
- Basic comprehension questions on infinity, cardinality, and rational and irrational numbers
- Basic comprehension questions on any of the readings.

Definitions

- Know how to define all the terms (and give an example if appropriate) from both of the midterm review sheets.
- Additionally we have: Mod n arithmetic, congruence, residue class, unit, zero divisor, group, cyclic group, generate, identity element, order of an element in a group, order of a group, ϕ function, cardinality of a set, countably infinite set, continuum hypothesis, irrational number.

Review Questions

Make sure that you understand how to do *all* of the questions on the previous review sheets and the midterms. You probably do not need to re-do all of the questions, but you should make sure you remember how to do each one.
This sheet consists of review questions on the topics covered since the second midterm, followed by a few sample questions on earlier material.

(A) Questions on mod n arithmetic, groups and infinity:

(1) Practice problems: All the practice problems in Ch. 6 (these are easy), also 7.5, 8.3, 8.4

(2) Exercises 6.1-6.3, 6.5, 6.6, 6.9-6.14, 6.19, 6.30, 6.31. Many of these were homework

(3) Challenging exercise: 6.20

(4) Find the residue class of $99(12 + 54^2 + 13^2)$ mod 8.

(5) Verify that $\mathbb{Z}_n$ is a group? Is it an *abelian group*? Why? What are some other examples of abelian groups? Is mod n arithmetic a group with multiplication rather than addition? Why/why not?

(6) Let $\mathbb{R} \times \mathbb{R}$ be the set of pairs of real numbers, with addition defined by $(a, b) + (c, d) = (a + b, c + d)$ and multiplication $(a, b) \times (c, d) = (ab, cd)$. Verify that this a group with operation $+$? Is it an abelian group? Is it cyclic? If instead of $+$, we use the operation $\times$, is it a group? What are the units? What are the zero divisors (if any)?

(7) Suppose that a is a generator of $\mathbb{Z}_n$. Prove that $n - a$ is also a generator by showing that the numbers $n - a, n - a + n - a, n - a + n - a + n - a, ...$ are all different mod n. As a warm up, you might wish to do this concretely for 2 and 7 in mod 9.

(8) Show that the set of natural numbers and the set of multiples of three have the same cardinality by writing down a matching. Then show that the set $\{0, 1, 2, 3, 4, ...\}$ and the set $\{10, 11, 12, 13, 14, ...\}$ have the same cardinality by writing down a matching.

(9) Is 9857135 divisible by 9? How do you know?

(10) Find a perfect matching between the set of natural numbers and the set $\{10, 11, 12, 13, 14...\}$. Does this mean this set is countable?

(11) Challenge problem: Is the set of positive real numbers, $\{x \in \mathbb{R} : x > 0\}$, countable? [hint: if it were, you could construct a matching between it an the even numbers. Then make a matching between the set of non-positive real numbers and the odd natural numbers. What does this give you?]

(12) Following the proof we did in class for $\sqrt{2}$, show that $\sqrt{3}$ is irrational.

(B) Sample questions on earlier topics

(1) Which of the following are subsets of $\mathbb{R}$?
$\mathbb{R}$, the empty set, $\mathbb{R} \times \mathbb{N}$, $\mathbb{Q}$, $\{1, 3, 5, 7...\}$, $\mathbb{N} \cup \mathbb{Q}$, a function from $\mathbb{R}$ to $\mathbb{R}$.

(2) For what sets A is it true that $\mathbb{N} = \mathbb{N} \cup A$?

(3) Suppose a and b are elements of a set with $+$ and $\times$ that satisfiy A1 to A4 and M1 to M4. Prove using the axioms that if $a \neq 0$ and $ab - a = 0$, then $b = 1$. At each step, state which axiom you are using.

(4) Does $\mathbb{R} \times \mathbb{R}$ as defined in question (6) above satisfy all the axioms of arithmetic?

(5) Prove using the order axioms that if $ab > 0$, then either $a > 0$ and $b > 0$, or $a < 0$ and $b < 0$. Hint: do three cases. First, what if $a > 0$ – show in this case that b must be positive. Second, what if $a < 0$. Third, can we have $a = 0$?

(6) Prove using the definition of divides that if $a|b$ and $a|c$ then $a^2|bc$.

(7) Suppose that a number N has a prime factor of 3. Can $N + 17$ have a prime factor of 3?

(8) Explain why there are infinitely many prime numbers.

(9) Use the Euclidean algorithm to compute the greatest common divisor of 423 and 21

(10) How many natural numbers less than 18 are relatively prime to 18?

(11) What is the greatest common divisor of 42 and $2^2 \times 7 \times 17$?