Mathematics 243, section 2 – Mathematical Structures
Information on Exam 3
November 28, 2017

General Information

The third exam this semester will be given next week. The options for scheduling are:

- the regular class period on Wednesday, December 6, or
- Thursday in the late afternoon (say 5 - 7pm). (Unfortunately, I am not available after 7pm that day because of the Festival of Lessons and Carols in the Chapel starting at 8pm. I also have a rehearsal for that on Wednesday night.) (We'll discuss the options on November 29 and decide.) The exam will cover the material we have discussed since the second exam (Problem Sets 7,8), through class on Wednesday, November 29 (convergence of sequences).

1) "Fermat's Little Theorem" (know the statement and proof)
2) RSA public key cryptography (be able to take the public key information m, e for an RSA system, "crack" it by finding the primes p, q with $m = pq$ and the decryption exponent d and decrypt a short message (one or two characters), given an ASCII table for the numerical equivalents of the characters like the one you used for the problem on Problem Set 7.
3) Functions/Mappings, injectivity and surjectivity, direct and inverse images – be able to prove things like the problems from Problem Set 7, *including statements you have not seen before*
4) Properties of the real number systems including the Binomial Theorem, problems like the ones from Problem Set 8, etc. Know especially what Axiom C ("completeness") says and consequences like the facts that the natural numbers are not bounded and given any $\varepsilon > 0$, there exists $n \in \mathbf{N}$ such that $\frac{1}{n} < \varepsilon$.
5) I may ask you to give a proof that a simple sequence like $a_n = 2 + \frac{1}{n}$ or something similar converges.

Review Session

I will be happy to run a review session before the exam. However, Tuesday evening (December 5) is virtually the only time for this for me.

Sample Exam Questions

Note: This list is longer than the actual exam will be to show the range of different kinds of questions that might appear. But the exam questions will be similar in content and format.

I. Consider an RSA public key cryptosystem with public information $m = 143$ and $e = 37$.
A) "Crack the system" by determining the private information p, q and d.

B) You intercept a message encrypted using this system consisting of the numbers $40, 114$. Use your answer to part A and the table on page 102 of the course notes to decrypt the message.

II.

A) Give the statement and proof of "Fermat's Little Theorem."
B) Use part A to compute $3^{177} \bmod 7$.
C) What is the *smallest* positive power k such that $7^k \equiv 1 \bmod 11$? Same question for $5^k \equiv 1 \bmod 11$.

III. Let $f : A \to B$ be a mapping.

A) If $S, T \subseteq A$ and $f(S) \cap f(T) \neq \emptyset$, can you conclude that $S \cap T \neq \emptyset$? (The answer is: No). Why not? Give a counterexample.
B) (continuing from A) Give a condition on f that would imply $S \cap T \neq \emptyset$ under the assumption that $f(S) \cap f(T) \neq \emptyset$. Prove your assertion.
C) If $U, V \subseteq B$ and $f^{-1}(U) \cap f^{-1}(V) \neq \emptyset$, can you conclude that $U \cap V \neq \emptyset$? If so, prove it. If not, give a counterexample.
D) Show that f is surjective if and only if there is a mapping $g : B \to A$ such that $f \circ g = id_B$. ($id_B : B \to B$ is the mapping satisfying $id_B(y) = y$ for all $y \in B$.)

IV.

A) The binomial coefficient $\binom{n}{k}$ is the number of subsets of $A = \{a_1, \ldots, a_n\}$ that contain exactly k elements. Assuming this fact, give (yet another) proof that A has 2^n distinct subsets (including $\emptyset$ and A itself).
B) Show by mathematical induction: For all $u > 0$ in the reals, and all $n \geq 0$,

$$1 + nu + \frac{n(n-1)}{2}u^2 + \frac{n(n-1)(n-2)}{6}u^3 \leq (1+u)^n$$

C) Give a second proof of the statement in part B using the Binomial Theorem.

V.

A) Prove that $\mathbf{N}$ is not bounded above in the real numbers. Use this to deduce that for any $\varepsilon > 0$, there exists $n \neq 0 \in \mathbf{N}$ such that $\frac{1}{n} < \varepsilon$.
B) Use the last statement in part A to prove that the sequence $a_n = 3 - \frac{1}{n}$ converges to $L = 3$.
C) Prove that $a_n = 3 - \frac{1}{\sqrt{n}}$ also converges to $L = 3$.

VI. Let R be the relation on the set of real numbers defined by aRb if and only if $a - b \in \mathbf{Z}$. For example $1.32R(-5.68)$ is true for this relation since $1.32 - (-5.68) = 7 \in \mathbf{Z}$.

A) Show that R is an equivalence relation.
B) Show that the functions $\sin(2\pi x)$ and $\cos(2\pi x)$ are well-defined mod R.
C) Give a subset of $\mathbf{R}$ that contains a *unique* element from each of the equivalence classes for the relation R. (That is, your set should contain a's "hitting" all of the equivalence classes, but each one only once.