

Study guide for Exam 3

This section is one of the more difficult, and it is not reasonable to remember how to do all the proofs in the class notes and the in the exercises. Here is a more specific guide of what to expect on the exam.

1. Basic definitions and properties. You do not have to reproduce the proofs in the notes and exercises for these. But know the basic definitions, properties and ideas.

- even numbers, odds, rationals, irrationals, reals
 - e.g. mn is odd iff m and n are odd (is this true?)
- basic properties of modular arithmetic
 - e.g. $x = x'$ and $y = y' \Rightarrow xy = x'x'y'$
- prime factorizations, including use of common prime sets
- gcd, lcm and relationship to prime factorizations.

2. Countability

- we proved two basic results: countability of the rationals, and non-countability of the reals. There was a central idea in the proofs for each of these
 - rationals: a special way of grouping them so a listing could be defined
 - reals: a way to define a real that is not in a supposed list of all reals
- be able to give short descriptions of these basic ideas

3. Euclid's algorithm

- how to use it to compute the gcd of a couple of numbers
- use the augmented form of it to determine a and b in
$$\gcd(m,n) = am + bn$$

4. Crypto

- the two main results we looked at were Diffie-Hellman for computing a shared key, and RSA for the two-part public key encryption.
- given a set of basic parameters (e.g. base and prime modulus, etc) compute the shared key, doing this for both A and B to make sure they come out the same
- given a set of basic parameters for RSA, encrypt a message M using the basic steps in RSA, and then decrypt using the steps in RSA (to get the original message M back)