Math 223, Spring 2009
Final Exam Preparation

Your final exam is self-scheduled and can be taken any time during the finals period. It is a closed-note, closed-book, open-brain, no-calculator 2.5-hour examination.

The exam is cumulative, and will have the same format as the midterms except it will be roughly twice as long. Later material will be emphasized more heavily. You may be asked to recall some definitions or reproduce statements of theorems or proofs listed on any of the review sheets. You might also see some problems that have already appeared in class, on homework assignments, or quizzes. Another portion of the exam will consist of problems you had not see before, i.e. you will have to solve new problems using techniques you already know. This portion will not comprise the bulk of the exam, and most of it will have the format and difficulty level of an average homework problem.

What follows are some guidelines for studying the portion of the material covered since the second midterm. To study for earlier topics, use review handouts for first and second midterms.

What you need to commit to memory

(1) You must know the definitions of the following.

(a) Quadratic residue and nonresidue
(b) Legendre symbol
(c) Transposition cipher
(d) Substitution cipher
(e) Symmetric/assymetric cipher
(f) Monoalphabetic/polyalphabetic cipher
(g) Unbreakable cipher
(h) One-way function

(2) You must know the statements of the following.

(a) Lagrange's Theorem
(b) Euler Criterion
(c) Quadratic Reciprocity (all parts)

(3) Proofs you must learn.

(a) Proof of Lagrange's Theorem
(b) Proof of the proposition stating that there are exactly $(p-1)/2$ QRs and NRs modulo an odd prime p
(c) Proof of multiplication rules for QRs and NRs
(d) Proof of Euler Criterion
(e) Proof of Quadratic Reciprocity, Part 1
(f) Proof that there are infinitely many primes congruent to 1 mod 4

(4) You must be able to explain the following. In case of ciphers or public-key protocols, you must know how and why encryption and decryption works and be ready to provide all the details.

(a) Frequency analysis
(b) Affine transformation cipher
(c) Vigenère cipher
(d) One-time pad
(e) RSA cryptosystem
(f) Security of RSA
(g) Treaty verification (RSA signature scheme)
(h) Diffie-Hellman key exchange

Topics you must study/Computational problems you must be able to do

(1) Quadratic residues and Quadratic Reciprocity

(2) Determining whether a quadratic congruence has a solution
(3) Computing Legendre symbols using Quadratic Reciprocity
(4) Finding inverses mod n using Euclidean algorithm
(5) Encrypting/decrypting with affine transformation cipher
(6) Encrypting/decrypting with Vigenère cipher
(7) Encrypting/decrypting with RSA cipher
(8) Agreeing on a key using Diffie-Hellman key exchange

How to study for the exam

The exam will be friendly to those who have studied carefully and followed all the instructions on this sheet. Most of the test questions will look familiar. As mentioned above, you will be asked to repeat some definitions, state some theorems, and reproduce some proofs you have seen before. The exam will contain some exercises you have not seen before, but they will not comprise the bulk of the exam, and there will be no questions that only divine intervention will help you solve. You will do poorly if you fail to follow the advice on this preparation sheet.

(1) Read this review sheet thoroughly.
(2) Read and understand your class notes.
(3) Know how to do all the homework and quiz problems. The solutions are on our class conference.
(4) Go to office hours to ask questions.
(5) After you have done all of the above, start on the review questions below.

Review Problems (solutions will be provided later)

(1) Determine whether the following congruences have a solution.
   (a) $x^2 + 1 \equiv 0 \pmod{6911}$
   (b) $x^2 + 6x + 10 \equiv 0 \pmod{19}$

(2) Compute $\left(\frac{84}{103}\right)$ and $\left(\frac{24}{31}\right)$.

(3) Let p be an odd prime and let a be a quadratic residue mod p. Prove that, if $p \equiv 1 \pmod 4$, then $p - a$ is also a quadratic residue mod p, but that, if $p \equiv 3 \pmod 4$, then $p - a$ is a nonresidue mod p.

(4) Show that another way to state the last part of Quadratic Reciprocity is the following: If p and q are distinct odd primes, then

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}.$$

(5) Let p be an odd prime. Prove that there are $\frac{p-1}{2} - \phi(p-1)$ quadratic nonresidues of p that are not primitive roots of p.

(6) Prove that, if p is a Fermat prime, then every quadratic nonresidue of p is also a primitive root of p. (Recall that a Fermat prime has the form $2^{2^n} + 1$ for some $n \in \mathbb{N}$.)

(7) Use Euclidean algorithm to find the inverse of 23 mod 26 and the inverse of 8 mod 13.

(8) Affine transformation cipher $C \equiv 7P + 10 \pmod{26}$ was used to encode a message. The encrypted message is $LJMKGMGMFXQEXMV$. Find the plaintext message. (Use $A = 0$, $B = 1$, ..., $Z = 25$.)

(9) Decode the following using the Vigenère cipher and codeword $BETTERGRADE$:

$$JEVVIGZSRLFFWNGHVXKHHFSMWZIRZDIGRJKAM$$

(10) RSA encryption with public key $(e, n) = (13, 2537)$ was used to encrypt a message. Ciphertext is 009516481410. If you know that the blocklength that was used is 4, find plaintext. (Use the $A = 00$, $B = 01$, ..., $Z = 25$.)

(11) Suppose Alice and Bob want to choose a key using use Diffie-Hellman key exchange. They publicly agree on the prime $p = 7$ and a primitive root $b = 3$. If Alice privately chooses $r = 12$ and Bob privately chooses $q = 9$, what is the key they would agree on?