Format and topics for exam 3
Math 126

General information. Exam 3 will cover chapters 16–22 of the text. The exam will be cumulative only to the extent that these chapters rely on previous material; for example, you should still know what $a \equiv b \pmod{m}$. However, there will not be any questions on the exam that only cover old material; for example, you will not be asked to recite the definition of mod m. One slight exception is that you should review Fermat's Little Theorem and Euler's Formula, since they are used so often in Chs. 16–22.

As before, most of the exam will rely on understanding the problem sets (including the problems to be done but not written up or turned in) and the definitions and theorems that lie behind them. If you can do all of the homework, and you know and understand all of the definitions and the statements of all of the theorems we've studied, you should be in good shape. You should not spend time memorizing proofs of theorems from the book, though understanding those proofs does help you understand the theorems. On the other hand, you should defintely spend time memorizing the *statements* of the important theorems in the text.

Exam 3 will follows the same ground rules as the previous exams. In particular, no books, notes, or calculators are allowed, and there will be the same four types of questions: computations, statements of definitions and theorems, proofs, and true/false with justification.

Definitions. The most important definitions we have covered are:

Ch. 16	binary expansion	
Ch. 18	encryption	decryption
	RSA encryption	
Ch. 19	witness	Carmichael number
	Rabin-Miller witness	
Ch. 20	quadratic residue mod p	quadratic nonresidue mod p
	QR, NR	Legendre symbol
	$\left(\frac{a}{p}\right)$	
Ch. 22	Jacobi symbol	$\left(\frac{a}{b}\right)$

Theorems, results, algorithms. The most important theorems, results, and algorithms we have covered are listed below. You should understand all of these results, and you should be able to state any theorem clearly and precisely. You don't have to memorize theorems by number or page number; however, you should be able to state a theorem, given a reasonable identification of the theorem (either a name or a vague description).

Ch. 16: Method of successive squaring; successive squaring works.
Ch. 17: How to compute kth roots mod m; why kth root algorithm works (conditions where algorithm may be applied).
Ch. 18: Setup of RSA encryption; RSA encryption works.
Ch. 19: Korselt's Criterion for Carmichael numbers; Rabin-Miller test for composite numbers.
Ch. 20: Half QR, half NR (Thm. 20.1); Quadratic Residue Multiplication Rules (Thms. 20.2 and 20.3).
Ch. 21: Euler's Criterion; Quadratic Reciprocity parts I and II (a.k.a. parts (-1) and 2); Primes 1 (mod 4) Theorem.
Ch. 22: Law of Quadratic Reciprocity (especially part III); Generalized Law of Quadratic Reciprocity (Thm. 22.2). Computing Legendre symbols: Method using factoring, method using Jacobi symbols.

Examples. You will also need to be familiar with the key properties of the main examples we have discussed. Most of the important examples we have encountered have appeared in the assigned problems. In addition, you should also know:

Ch. 16: Application: Fermat's Little Theorem and primality testing.
Ch. 17: Solving $x^k \equiv b \bmod m$.
Ch. 18: Decryption examples from text and class and HW.
Ch. 19: Examples of false witnesses (a such that $a^n \equiv a \pmod{n}$ but n composite). Examples of Carmichael numbers.
Ch. 20: Lists of QR, NR (mod p).
Ch. 22: Computing Legendre and Jacobi symbols (pp. 164–167).

Good luck.