Format and topics for exam 2
Math 126

General information. Exam 2 will cover Ch. 8–15 of the text. The exam will be cumulative only to the extent that 8–15 rely on previous material; for example, you should still know what it means for a to divide b. 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 divisibility.

As before, most of the exam will rely on understanding the problem sets 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 2 will follows the same ground rules as exam 1 did. 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. 8	a is congruent to b modulo m	$a \equiv b \pmod{m}$
	modulus	
Ch. 9	$n!$	n factorial
Ch. 10	Euler's phi function	$\varphi(m)$
	Carmichael number	
Ch. 13	$\pi(x)$	
Ch. 14	Mersenne prime	
Ch. 15	perfect number	$\sigma(m)$

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. 8 Congruences work like equations (Ex. 8.1). Linear Congruence Theorem. When can we cancel a in $ab \equiv ac \pmod{m}$? (I.e.: When can we divide by $a \pmod{m}$?) Algorithm for solving $ax \equiv c$. Polynomial roots mod p theorem.

Ch. 9: Fermat's Little Theorem.

Ch. 10: Euler's Formula.

Ch. 11: Chinese Remainder Theorem: for 2, 3, and many moduli; in $0 \le x < mn$ version and (mod mn) version. Phi function formulas (esp. multiplicative formula).

Ch. 12: Infinitely Many Primes Theorem. Primes 3 (Mod 4) Theorem. Dirichlet's Theorem on Primes in Arithmetic Progression.

Ch. 13: Prime Number Theorem.

Ch. 14: All primes of the form $a^n - 1$ are Mersenne primes.

Ch. 15: Euclid's Perfect Number Formula; Euler's Perfect Number Theorem. Sigma function formulas.

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, both those to be turned in and those not to be turned in. In addition, you should also know:

Ch. 8: Examples of solving $ax \equiv c \pmod{m}$. Examples of solving higher-degree equations (mod m).

Ch. 9: Using Fermat's Little Theorem (Ex. 9.1, 9.4).
Ch. 10: Using Euler's Theorem (Ex. 11.11).
Ch. 11: Using Phi function formulas to calculate $\varphi(m)$.
Ch. 15: Using Sigma function formulas to calculate $\sigma(m)$.

Not on exam. Ch. 13: Number-theoretic functions other than $\pi(x)$ ($P(x)$, Twin(x), etc.); conjectures (Goldbach, Twin Primes, N^2+1). Ch. 14: Are there infinitely many Mersenne primes? Ch. 15: Odd Perfect Number Quandary.

Good luck.