Format and topics for exam 1
Math 126

General information. Exam 1 will be a timed test of 75 minutes, covering Ch. 1–8 of the text. No books, notes, calculators, etc., are allowed. Most of the exam will rely on understanding the problem sets (including the problems to be done but not to be 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. (Of course, when ideas from those proofs have appeared in the homework, you need to understand those ideas.) On the other hand, you should defintely spend time memorizing the *statements* of the important theorems in the text.

Types of questions. There are four types of questions that may appear on exam 1, namely:

1. Computations;
2. Statements of definitions and theorems;
3. Proofs;
4. True/false with justification.

Computations (with explanation). These will be drawn from computations of the type you've done on the problem sets. You may or may not be asked to explain or justify your answer on a computation; you must always show all your work.

Statements of definitions and theorems. In these questions, you will be asked to recite a definition or the statement of a theorem from the book. You will not be asked to recite the proofs of any theorems from the book, though you may be asked to prove book theorems that you might have been asked to prove on problem sets.

Proofs. These will resemble some of the shorter problems from your homework. You may take as given anything that has been proven in class, in the homework, or in the reading. Partial credit may be given on proof questions, so keep trying if you get stuck (and you've finished everything else). If all else fails, at least try to write down the definitions of the objects involved.

True/false with justification. This type of question may be less familiar. You are given a statement, such as:

- Every odd number greater than 1 is prime.

If the statement is true, all you have to do is write "True". (However, see below.) If the statement is false (like the one above), not only do you have to write "False", but also, you must give a reason why the statement is false. Your reason might be a very specific counterexample:

> False. $9 = 3 \times 3$ is odd and composite.

Your reason might also be a more general principle:

> False. In fact, there are infinitely many odd composite numbers; for example, take any number of the form $3(2n + 1)$ ($n \in \mathbb{N}$).

Either way, your answer should be **as specific as possible** to ensure full credit.

Depending on the problem, some partial credit may be given if you write "False" but provide no justification, or if you write "False" but provide insufficient or incorrect justification. Partial credit may also be given if you write "True" for a false statement, but provide some partially reasonable justification. (In other words, if you have time, it can't hurt to justify "True" answers.)

If I can't tell whether you wrote "True" or "False", you will receive no credit. In particular, please do not just write "T" or "F", as you may not receive any credit.

Definitions. The most important definitions and symbols we have covered are:

Ch. 1	prime	twin primes
	triangle number	
Ch. 2	Pythagorean triple	primitive Pythagorean triple
	PPT	
Ch. 5	divides	$a \mid b$, $a \nmid b$
	divisor	greatest common divisor
	$\gcd(a, b)$	least common multiple
	$\mathrm{LCM}(a, b)$	
Ch. 7	composite	factorization
Ch. 8	a is congruent to b modulo m	$a \equiv b \pmod{m}$
	modulus	

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 correctly. More precisely, you should be able to state any of the theorems, given a reasonable identification of the theorem (either its name or a vague description).

Ch. 1 Formula for triangle numbers.
Ch. 2 Pythagorean triples theorem.
Ch. 3 Theorem: parameterization of rational points on unit circle.
Ch. 5 Euclidean algorithm. Theorem: Euclidean algorithm computes $\gcd(a, b)$.
Ch. 6 Linear Equation Theorem. How to use Euclidean algorithm to compute one solution to $ax + by = \gcd(a, b)$. How to obtain *all* solutions to $ax + by = \gcd(a, b)$.
Ch. 7 $p \mid ab$ lemma, Prime Divisibility Property, Fundamental Theorem of Arithmetic.
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.

Examples. You will also need to be familiar with the key properties of the main examples we have discussed. The most important examples we have seen are:

Ch. 1 Triangle-square numbers (pp. 9–10).
Ch. 2 Pythogrean triples and PPT's.
Ch. 5 Euclidean algorithm examples (pp. 28–29).
Ch. 6 Using Euclidean algorithm to compute one solution to $ax + by = \gcd(a, b)$ (pp. 36–38). Getting *all* solutions to $ax + by = \gcd(a, b)$ (pp. 40–41).
Ch. 7 The $\mathbb{E}$-Zone: Definition and properties of $\mathbb{E}$-divides, $\mathbb{E}$-primes, $\mathbb{E}$-factorization. $\mathbb{M}$-World (PS03): Definition and properties of $\mathbb{M}$-divides, $\mathbb{M}$-primes, $\mathbb{M}$-factorization.
Ch. 8 Examples of solving $ax \equiv c \pmod{m}$, solving higher-degree equations $(\mathrm{mod}\ m)$.

Other. You should have a working familiarity with techniques and strategies for proof and logic tips, to the extent that we have done proofs in the homework. See the handout on "What is a proof?" for more information. You do not need to memorize information from the handout, but you should be able to apply it.

Not on exam. Fermat's Last Theorem stuff (Ch. 4).

Good luck.