Format and topics for final exam
Math 126

General information. The final will be a little more than 1.5 times as long as our in-class exams, with 135 minutes in which to complete it. It will take place in our usual room.

The final will be cumulative; in other words, the final will cover the topics on this sheet and also on the previous three review sheets. However, the exam will somehwat emphasize the material listed here (Chapters 20–22, 24–25, 31–31). As always, 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.

The usual ground rules apply: No books or notes allowed, and four types of questions, namely, computations, statements of definitions and theorems, proofs, and true/false with justification.

Definitions. The most important definitions we have covered are:

Ch. 20	quadratic residue mod p	quadratic nonresidue mod p
	QR, NR	Legendre symbol
	$\left(\frac{a}{p}\right)$	
Ch. 22	Jacobi symbol	$\left(\frac{a}{b}\right)$
Ch. 32	Pell equation	

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. 20: Half QR, half NR (p. 158); a is QR if and only if $I(a)$ is even; Quadratic Residue Multiplication Rules (both versions on pp. 160–162).
Ch. 21: Euler's Criterion, Gauss' Lemma, Quadratic Reciprocity parts I and II; Primes 1 (mod 4) Theorem.
Ch. 22: Law of Quadratic Reciprocity (especially part III); Generalized Law of Quadratic Reciprocity (from text and from handout). Computing Legendre symbols: Method using factoring, method using Jacobi symbols.
Ch. 24: Sum of Two Squares Theorem For Primes. Fermat descent procedure.
$(u^2+v^2)(A^2+B^2) = (uA+vB)^2 + (vA-uB)^2$.
Ch. 25: Sum of Two Squares Theorem (part (a) only). Procedure for solving $n = a^2 + b^2$.
Ch. 31: Square-Triangular Number Theorem.
Ch. 32: Pell's Equation Theorem.

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. 22: Examples of computing $\left(\frac{a}{p}\right)$.
Ch. 24: Examples of solving $p = a^2 + b^2$.
Ch. 25: Examples of solving $n = a^2 + b^2$.
Ch. 31: Using approximation $x_k \approx \frac{(3+2\sqrt{2})^k}{2}$, similar for y_k.

Not on exam. Ch. 24: Sums of squares and complex numbers. Ch. 25: Part (b) of Sum of Two Squares Theorem; Pythagorean Hypotenuse Proposition. Chs. 33–34: All.

Good luck.