Format and topics for final exam
Math 127

General information. The final will be a little less than twice 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 somewhat emphasize the material listed here from 11A–11C, 4.2–4.3, and 5.1–5.4. As always, 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 may help you understand the theorems. On the other hand, you should defintely spend time memorizing the *statements* of the important theorems in the text.

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

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

Sect. 11A	group	closed
	associativity	cancellation
	solvability	identity
	inverse	commutativity
	abelian group	generalized associativity
	generalized commutativity	U_m
Sect. 11B	subgroup	cyclic subgroup generated by a
	$\langle a \rangle$	cyclic group
	order of a group element	
Sect. 11C	left coset	
4.2	$H \leq G$	C_n
4.3	coset representative	complete set of coset representatives
	partition	
5.2	signal	Discrete Fourier Transform (DFT)
	spectrum	inverse DFT
5.3	convolution of f and g	
5.4	Fast Fourier Transform (FFT)	FFT based on $H_0 \leq \cdots \leq H_n$

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).

Sect. 11A Abstract Fermat Theorem (Thm. 1).

Sect. 11B Order of element equals order of $\langle a \rangle$.

Sect. 11C Cosets are disjoint or equal (Prop. 5) and all the same size (Prop. 6). Lagrange's Theorem (Thm. 7) and corollaries (Cor. 8 and 9).

Sect. 4.2 C_n is a subgroup of $U(\mathbb{C})$; C_k is a subgroup of C_n if k divides n (Thm. 4.2.3).

Sect. 4.3 Cosets partition G (Thm. 4.3.6); picture of cosets partitioning G.

Sect. 5.1 Grade-school multiplication is $O(n^2)$.

Sect. 5.2 Orthogonality Lemma 5.2.5; Inversion Theorem 5.2.6. Matrix notation for DFT (Rems. 5.2.3 and 5.2.7).

Sect. 5.3 Convolution is polynomial multiplication (Thm. 5.3.2). Substitution Lemma 5.3.3; DFT turns convolution into pointwise multiplication (Thm. 5.3.4).

Sect. 5.4 FFT based on $H_0 \le \cdots \le H_n$. Time estimate for FFT (Rem. 5.4.5).

You do not need to memorize the "code" for the FFT. The steps of the FFT will be provided in an abbreviated form that, if you have done the homework, will allow you to go step through the algorithm without having to recite the loop structure and the formulas.

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:

Sect. 11A U_m (units of $\mathbb{Z}/(m)$).
Sect. 11B $U(k)$ (in our notation, C_k). Units $U(R)$ of any ring R. Cyclic subgroups of U_{13}, U_{19}, U_{21}.
Sect. 11C Cosets of cyclic subgroups of U_m (PS10).
Sect. 4.2 C_n: as subgroup of $U(\mathbb{C})$, containing C_k.
Sect. 4.3 Cosets and representatives in U_{13} (Exs. 4.3.4, 4.3.8).
Sect. 5.4 FFT examples: Exs. 5.4.3, 5.4.4, 5.4.6.

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.

Not on exam. (Sect. 11A–11C) All groups and examples where operation is $+$. (Sect. 11B) Props. 3 and 4.

Good luck.