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 120 minutes in which to complete it and an additional 15 minutes for uploading. It will take place online using our now established Zoom proctoring procedure: write answers on your own paper and scan them into a single PDF. In particular, you are allowed

ONE PAGE OF HANDWRITTEN NOTES (both sides)

and no other aids (books or calculators). Also, the final will (probably) have 13 problems on it, so please prepare 13 sheets of paper by writing $1, \ldots, 13$ on them (large and easily readable, please).

The final will be **cumulative**; in other words, the final will cover the topics on this sheet and also on the previous two review sheets. (Exception: Ch. 4 will not be covered on the final.) However, the exam will somewhat emphasize the material listed here from Sections 8.2–8.5, 9.2–9.4, and 10.1–10.3. 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 definitely spend time memorizing the *statements* of the important theorems in the text.

As usual, 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:

8.2	code of length n over $\mathbf{F}_q$	cyclic code
	polynomial notation	
8.3	generator polynomial of a cyclic code	
8.4	extension field	factoring over a field F
	Frobenius orbit	
9.2	natural primitive Nth root of unity	ω_N, ω
9.3	signal	DFT
	inverse DFT	
9.4	convolution	
10.1	group	abelian group
	subgroup	C_n
	cyclic subgroup generated by a	$\langle a \rangle$
10.2	order of an element	
10.3	left multiplicative coset	coset representative
	partition	complete set of coset representatives

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. 8.2 Cyclic codes are ideals (Thm. 8.2.6).

Sect. 8.3 Cyclic codes are principal ideals $g(x)$, where $g(x)$ divides $x^n - 1$. Basis and dimension for cyclic code $(g(x))$.

Sect. 8.4 Frobenius map is an automorphism (Thm. 8.4.7). Minimal polynomial for $\beta \in E$ (Thm. 8.4.8). Orbit Theorem 8.4.11.

Sect. 8.5 BCH Theorem 8.5.1. BCH Algorithm 8.5.2.

Sect. 9.2 Nth roots of unity are powers of ω_N (Thm. 9.2.3); $1 + \omega_N + \cdots + \omega_N^{N-1} = 0$.

Sect. 9.3 Orthogonality Lemma 9.3.5; Inversion Theorem 9.3.6. Matrix notation for DFT (Rems. 9.3.3 and 9.3.7).

Sect. 9.4 Convolution is polynomial multiplication (Thm. 9.4.2). Substitution Lemma 9.4.3; DFT turns convolution into pointwise multiplication (Thm. 9.4.4).

Sect. 10.1 Subgroup Theorem 10.1.8. Subgroup properties of C_n (Thm. 10.1.10). Cyclic subgroup generated by a really is a subgroup (Thm. 10.1.12).

Sect. 10.2 If order of a is n: a^k depends only on k (mod n) (Thm. 10.2.2); $a^k = 1$ iff n divides k (Cor. 10.2.3); $\langle a \rangle$ contains n elements (Cor. 10.2.4); order of a^k is $n/\gcd(k, n)$ (Thm. 10.2.5).

Sect. 10.3 If $b \in aH$, then $bH = aH$ (Thm. 10.3.3); either $aH = bH$ or $aH \cap bH = \emptyset$ (Cor. 10.3.5). Cosets partition G (Thm. 10.3.7). Order of subgroup divides order of group (Cor. 10.3.11); order of element divides order of group (Cor. 10.3.12).

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. 8.3 Cyclic codes: parity check, repetition, and $\mathcal{H}_7$.

Sect. 8.4 Minimal polynomial for $\alpha \in \mathbf{F}_q$. Factoring over different fields F (Exmp. 8.4.3, 8.4.4). Orbits in $\mathbf{F}_8$.

Sect. 8.5 BCH examples (Exmp. 8.5.3, 8.5.4, 8.5.5).

Sect. 9.3 Explicit expansions in Prob. 9.3.1.

Sect. 10.1 Group of units of a ring R (Ex. 10.1.5). C_n as subgroup of $\mathbf{C}^\times$ (Thm. 10.1.10), as cyclic subgroup (Ex. 10.1.13).

Sect. 10.3 Cosets and representatives in $\mathbf{F}_{13}^\times$ (Exs. 10.3.2, 10.3.9).

Not on exam. Chs. 4 and 11; also Sect. 8.1.

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.

Good luck.