Format and topics for exam 2
Math 127

General information. Exam 2 will be a timed test of 75 minutes, covering Sections 5A–5B, 5F, 6A–6E, 8A–8B of Childs, as well as 1.4 and 2.1–2.7 of the class notes. More to the point, the exam will cover PS04–PS06 and the ideas contained therein. No books, notes, calculators, etc., are allowed.

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 and symbols we have covered are:

1.4	$O(f(n))$	$a(n) << b(n)$
	logarithmic-time	polynomial-time
	exponential-time	combinatorial-time
Sect. 5A	a congruent to b (mod m)	$a \equiv b \pmod{m}$
	modulus	least non-negative residue
Sect. 6B	congruence class of a (mod m)	$[a]_m$
	$\mathbb{Z}/m\mathbb{Z}$	
Sect. 6D	complete set of representatives	primitive root (mod p)
Sect. 6E	unit	inverse
	complete set of units	
Sect. 8A	matrix	column vector
	row vector	
Sect. 8B	system of linear equations	homogeneous
	nonhomogeneous	
2.1	message	string
	bit	bitstring
	(noisy) channel	error
	error-correcting code	codeward
	parity check	parity check code
	repetition code	majority logic
2.2	vector	zero vector
	F^n	F-linear combination
	linear combination	
2.3	augmented marrix	row-echelon form
	REF	leading 1
	leading column	reduced row-echelon form
	RREF	leading variable
	free variable	elementary operation
2.4	subspace	zero subspace
	span (noun)	span (verb)
	linearly independent	linearly dependent
	basis	dimension
2.5	linear transformation associated with A	Null(A)
	rank	nullity

2.6	binary linear code	standard framework
	encdoding	decoding
	parity check matrix	generator matrix
	$[n, k, d]$ binary linear code	length
	dimension	minimum distance
2.7	Hamming 7-code	syndrome
	Hamming 8-code	Hamming distance
	$d(\mathbf{x}, \mathbf{y})$	Hamming weight
	$\mathrm{wt}(\mathbf{x})$	nearest neighbor decoding
	floor	

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. 1.4 The Asymptotics Theorem; The Addition Principle.
Sect. 5A Relationship between mod and division with remainder (Prop. 1 and 2)
Sect. 5B Congruence can be treated like equality (Props. 3, 4, and 6)
Sect. 5F When does $ax \equiv b \pmod{m}$ have a solution? (Props. 18–20)
Sect. 6B Relationship between congruence and $[a]_m$ (Props. 1–2).
Sect. 6D Primitive Root Theorem; finding complete sets of representatives (Prop. 4)
Sect. 6E Units in $\mathbb{Z}/m\mathbb{Z}$ (Prop. 5)
Sect. 2.3 Gaussian reduction.
Sect. 2.4 Span is a subspace (Thm. 2.4.4), span calculations (Thm. 2.4.5), linear independence calculations (Thm. 2.4.8), invariance of dimension (Thm. 2.4.10).
Sect. 2.5 Null(A) is a subspace (Thm. 2.5.3); rank-nullity (Thm. 2.5.5, Cor. 2.5.7).
Sect. 2.7 Decoding method for $\mathcal{H}_7$ (discussion before Thm. 2.7.3); $\mathcal{H}_7$ corrects one error (Thm. 2.7.3); $\mathcal{H}_8$ corrects one error and detects two (Thm. 2.7.5). Min distance vs. error correction/detection (Thm. 2.7.11).

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. 1.4 Examples of "big-O" time estimates (e.g., Euclidean Algorithm).
Sect. 5B Computing $a^r \pmod{m}$ (Exs. 1–4).
Sect. 5F Solving $ax \equiv b \pmod{m}$ (Ex. 9).
Sect. 6A Two ways to look at $\mathbb{Z}/2\mathbb{Z}$.
Sect. 6B Working mod 2, 9, 12.
Sect. 6C Working mod m (general discussion).
Sect. 6D Using log table/power table (mod p) (Example 1).
Sect. 6E Units mod 3, 5, 9.
Sect. 8A Modular matrix multiplication examples.
Sect. 8B Solving linear systems.
Sect. 2.1 Parity check code, repetition code.
Sect. 2.3 Solving RREF system (Ex. 2.3.4); Gaussian reduction (Ex. 2.3.7).
Sect. 2.5 Calculating Null(A) (Ex. 2.5.4).
Sect. 2.6 Parity check (Ex. 2.6.3); repetition (Ex. 2.6.4). $[n, k, d]$ (Exs. 2.6.6–2.6.7).
Sect. 2.7 Hamming 7-code example (Ex. 2.7.2). Hamming distance (Ex. 2.7.7).

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. 5B) Prop. 5. (Sect. 5F) Multiple solutions of $ax \equiv b \pmod{m}$. (Sect. 6C) Round robin tournaments. (Sect. 6E) Cor. 6, Euler φ function.

Good luck.