Format and topics for exam 3
Math 127

General information. Exam 2 will be a timed test of 75 minutes, covering Sections 23A–23C, 14C, and 24B–24C of Childs, as well as 3.1–3.7 of the class notes. More to the point, the exam will cover PS07–PS09 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 3 will follows the same ground rules as the previous exams. 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:

Sect. 14C	irreducible polynomial	
Sect. 23B	congruent mod $m(x)$	congruence class
	$[a(x)]_{m(x)}$	$F[x]/m(x)$
	representative of a congruence class	complete set of representatives
Sect. 23C	$[a(x)]_{m(x)} + [b(x)]_{m(x)}$	$[a(x)]_{m(x)}[b(x)]_{m(x)}$
	simple field extension	
3.1	burst error	information rate
	error-correction rate	
3.2	linear code over $\mathbb{F}_q$	codeword
	cyclic code	polynomial notation for codewords
	ideal	
3.3	zero ideal	principal ideal
	ideal (a) generated by a	ideal (a, b) generated by a and b
	minimal polynomial (of an ideal)	
3.4	generator polynomial of a cyclic code	
3.5	extension field	primitive root (of a field)
	minimal polynomial (of β over $\mathbb{F}_q$)	$m_i(x)$
	Frobenius orbit of β	
3.6	BCH code	designed distance δ of a BCH code
3.7	Reed-Solomon code	designed $\mathbb{F}_q$-distance Δ
	byte (in an R-S code)	bit (in an R-S code)
	$[N, K, D]$ code	

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. 14C Polynomials can be factored uniquely into irreducibles (Thms. 10, 12, 13).

Sect. 23B Congruence mod $m(x)$ is an equivalence class, and is same as mod (Props. 1 and 2); order of $F[x]/(m(x))$.

Sect. 23C Operations mod $m(x)$ are well-defined; $\mathbb{F}[x]/(m(x))$ is a field if and only if $m(x)$ is irreducible.

Sect. 24B–24C Every finite field has form $\mathbb{F}_p[x]/(m(x))$ (Thm. 4); there exists a field of order n if and only if $n = p^d$ (Thms. 5 and 6), and that field is essentially unique (Thm. 8).

Sect. 3.2 $\mathcal{C}$ is cyclic if and only if it is an ideal of $\mathbb{F}_q[x]/(x^n - 1)$ (Thm. 3.2.6).

Sect. 3.3 Every ideal of $F[x]$ or $\mathbb{Z}$ is principal (Thm. 3.3.8). Minimal polynomial of $(a(x), b(x))$ is GCD (Euclidean algorithm) (Thm. 3.3.10).
Sect. 3.4 Every ideal of $F[x]/(x^n - 1)$ is generated by $g(x)$ dividing $x^n - 1$ (Thm. 3.4.1). Basis and dimension of cyclic code from generator $g(x)$ (Thm. 3.4.3). Encoding and reading codewords in a cyclic code.
Sect. 3.5 Finite field facts (Thm. 3.5.5), especially: Every finite field has a primitive root. Polynomials with β as a root are an ideal (Thm. 3.5.6). **The Orbit Theorem** (Thm. 3.5.9).
Sect. 3.6 The BCH Theorem (Thm. 3.6.1). Recipe for BCH codes (Thm. 3.6.2).
Sect. 3.7 Recipe for Reed-Solomon codes. Reed-Solomon burst correction (Thm. 3.7.3).

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. 14C Irreducibles in $\mathbb{F}_2[x]$ up to degree 4.
Sect. 23A $\mathbb{C}$ as $\mathbb{R}[i]$; $\mathbb{F}_2[x]/(x^3 + x + 1)$.
Sect. 23B $F_3[x]/(x^3 + 1)$; $\mathbb{F}_2[x]/(x^4 + x + 1)$; $\mathbb{C} = \mathbb{R}[x]/(x^2 + 1)$.
Sect. 24B Finite fields of order up to 16.
Sect. 3.1 Burst problem (Prob. 3.1.1).
Sect. 3.3 Examples of ideals of R: Even integers, zero ideal, R. $m\mathbb{Z}$, $(m(x))$, principal ideal (a), ideal (a, b) generated by a and b.
Sect. 3.4 Examples of cyclic codes: Parity check, repetition, Hamming 7-code.
Sect. 3.5 $\mathbb{F}_q$ $(q = 2^e)$ is an extension of $\mathbb{F}_2$ and itself. Computing Frobenius orbits (Ex. 3.5.10).
Sect. 3.6 Constructing BCH codes (Exs. 3.6.3 and 3.6.5).
Sect. 3.7 Constructing a Reed-Solomon code (Exs. 3.7.2).

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. 14C) Prop. 9, Thm. 11. (Sect. 23A) $\mathbb{Q}[\sqrt[3]{2}]$. (Sect. 23B) $\mathbb{Q}[\sqrt{5}]$. (Sect. 24C) Cors. 7 and 9. (Sect. 3.5) Proof of Orbit Theorem. (Sect. 3.6) Vandermonde matrices; proof of BCH Theorem.

Good luck.