Format and topics for exam 1
Math 127

General information. Exam 1 will be a timed test of 75 minutes, covering Sections 3A–3F, 7A, 7C, 13A–13C, and 14A–14B of Childs, as well as 1.1–1.4 of the class notes. No books, notes, calculators, etc., are allowed. Most of the exam will rely on understanding the problem sets (including the problems to be done but not to be 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. (Of course, when ideas from those proofs have appeared in the homework, you need to understand those ideas.) On the other hand, you should defintely spend time memorizing the *statements* of the important theorems in the text.

Types of questions. There are four types of questions that may appear on exam 1, namely:

1. Computations;
2. Statements of definitions and theorems;
3. Proofs;
4. True/false with justification.

Computations (with explanation). These will be drawn from computations of the type you've done on the problem sets. You may or may not be asked to explain or justify your answer on a computation; you must always show all your work.

Statements of definitions and theorems. In these questions, you will be asked to recite a definition or the statement of a theorem from the book. You will not be asked to recite the proofs of any theorems from the book, though you may be asked to prove book theorems that you might have been asked to prove on problem sets.

Proofs. These will resemble some of the shorter problems from your homework. You may take as given anything that has been proven in class, in the homework, or in the reading. Partial credit may be given on proof questions, so keep trying if you get stuck (and you've finished everything else). If all else fails, at least try to write down the definitions of the objects involved.

True/false with justification. This type of question may be less familiar. You are given a statement, such as:

- Every commutative ring is a field.

If the statement is true, all you have to do is write "True". (However, see below.) If the statement is false (like the one above), not only do you have to write "False", but also, you must give a reason why the statement is false. Your reason might be a very specific counterexample:

> False. The integers $\mathbb{Z}$ are a commutative ring, but they are not a field, since $\dfrac{1}{2}$ is not an integer.

Your reason might also be a more general principle:

> False. In fact, if m is not prime, then $\mathbb{Z}/m$ is a ring with zero divisors, and therefore, not a field.

Either way, your answer should be **as specific as possible** to ensure full credit.

Depending on the problem, some partial credit may be given if you write "False" but provide no justification, or if you write "False" but provide insufficient or incorrect justification. Partial credit may also be given if you write "True" for a false statement, but provide some partially reasonable justification. (In other words, if you have time, it can't hurt to justify "True" answers.)

If I can't tell whether you wrote "True" or "False", you will receive no credit. In particular, please do not just write "T" or "F", as you may not receive any credit.

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

1.1	natural numbers $\mathbb{N}$	integers $\mathbb{Z}$
	rational numbers $\mathbb{Q}$	complex numbers $\mathbb{C}$
	complex numbers	complex plane
	modulus	absolute value
	conjugate	complex exponential e^z
	argument	nth root of unity
	primitive nth root of unity	
1.2	divides	common divisor
	greatest common divisor	
Sect. 3A	divisor	dividend
	quotient	remainder
Sect. 3B	coprime	relatively prime
Sect. 7A	ring (with identity)	zero element 0
	negative	commutative ring
	subring	unit
	field	
Sect. 7C	zero divisor	NZD property
	complementary zero divisor	
1.3	$\mathbb{Z}/n$ (informal)	
Sect. 13A	polynomial	
Sect. 13B	ring of polynomials $R[x]$	degree
	leading coefficient	
Sect. 14A	monic polynomial	
Sect. 14B	greatest common divisor	associates
	coprime (polynomials)	relatively prime (polynomials)
1.4	$O(f(n))$	$a(n) << b(n)$
	logarithmic-time	polynomial-time
	exponential-time	combinatorial-time

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. 1.1 Properties of absolute values (Thm. 1.1.4), Euler's formula, deMoivre's formula.
Sect. 1.2 Naive algorithm for $\gcd(a, b)$.
Sect. 3A Division theorem and uniqueness.
Sect. 3C Euclidean algorithm.
Sect. 3D Bezout's identity.
Sect. 3E $ax + by = e$ has solution iff $\gcd(a, b)$ divides e.
Sect. 7C Cancellation holds in NZD rings (Prop. 7). Units are never zero divisors (Prop. 11). Elements of $\mathbb{Z}/m$ (units vs. zero divisors) (Thm. 12); $\mathbb{Z}/m$ is a field iff m prime (Cor. 13).
Sect. 13B $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$ (Prop. 1).
Sect. 14A Division theorem (polynomials); Remainder Theorem, Root Theorem, d'Alembert's Theorem (degree n has at most n roots).
Sect. 14B Euclidean Algorithm and Bezout's Identity for polynomials.
Sect. 1.4 The Asymptotics Theorem; The Addition Principle.

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. 1.1 n roots of unity and primitive nth roots of unity for arbitrary n.
Sect. 3C Examples of computing gcd by Euclidean algorithm.

Sect. 3D Solving $ax + by = \gcd(a, b)$. Coprime iff $ax + by = 1$; common divisors divide gcd (Cor. 7).

Sect. 7A Non-rings: $\mathbb{N}$, $\mathbb{R}_+$. Commutative rings: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/m$. Fields: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{Z}/p$.

Sect. 13C Multiplying polynomials.

Sect. 14B Examples of Euclidean Algorithm and Bezout.

Sect. 1.4 Examples of "big-O" time estimates (e.g., Euclidean Algorithm).

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. 3A) Numbers written in different bases. (Sect. 3D) You can use the "solve for remainders" version of the EEA; you do not need to know the EEA matrix. Cor. 8 and Prop. 9. (Sect. 3E) Multiple solutions of $ax + by = c$. (Sect. 7A) Group, abelian group. (Sect. 7C) Prop. 9, Thm. 14. (Sect. 13C) You have to know how to multiply polynomials, but you can either use the notation of "detaching the coefficients" or the notation where the x^k are written explicitly. (Notes 1.3) Calendar trick.

Good luck.