Format and topics for exam 1
Math 127

General information. Exam 1 will be a timed test of 75 minutes, covering Sections 2.1–2.6 and 3.1–3.6 of the class notes/text. No books, notes, calculators, etc., are allowed. The exam will mainly 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. (Of course, when ideas from those proofs have appeared in the homework, you need to understand those ideas.) On the other hand, you should definitely spend time memorizing the *statements* of the important theorems in the text.

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

1. Computations;
2. Statements of definitions and theorems;
3. Proofs;
4. Explanations/problem solving;
5. 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 proof 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.

Explanations/problem solving. These will resemble the "Explain" problems or open-ended problems from the homework. However, instead of having to do an open-ended problem on an exam, you will just have to understand the homework problems you actually did and do something similar (perhaps very similar) on the exam.

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 $\frac{1}{2}$ 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:

2.1	divides	divisor
	associates	up to associates
2.2	common divisor	greatest common divisor
2.6	$T(n) = O(f(n))$	Big O notation
	$f(n) << g(n)$	asymptotic domination
3.1	k reduced mod m	$\mathbb{Z}/(m)$
	integers (mod m)	modulus
	congruent (mod m)	primitive element (mod p)
	quadratic residue (mod p)	quadratic nonresidue (mod p)
3.2	multiplicative inverse	inverse
	unit	field
	$\mathbb{F}_p = \mathbb{Z}/(p)$	field of order p
	$GF(p)$	fraction $\frac{a}{b}$
3.3	$R[x]$	polynomials with coefficients in R
	zero polynomial	coefficient ring of $R[x]$
	degree	leading coefficient
	leading term	zero factor property
3.5	divides	common divisor
	greatest common divisor	associates
	up to associates	irreducible
	reducible	

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. 2.1 Basic properties of divisibility (Probs. 2.1.1–2.1.4).

Sect. 2.2 Naive Algorithm 2.2.9 for computing GCD, and refinement (Prob. 2.2.2).

Sect. 2.3 Division Theorem (Thm. 2.3.1), Signed Division Theorem (Thm. 2.3.4).

Sect. 2.4 Euclidean Algorithm (Alg. 2.4.1). EA works (Thm. 2.4.4), common divisors divide GCD (Cor. 2.4.5). Signed Euclidean Algorithm (Alg. 2.4.6); SEA works (Thm. 2.4.8).

Sect. 2.5 Bezout's Identity (Thm. 2.5.1) and Corollary (Thm. 2.5.6). Euclidean Rewriting (Alg. 2.5.2).

Sect. 2.6 Asymptotics Theorem (Thm. 2.6.4), Addition Principle (Thm. 2.6.5). SEA and EA are $O(\log n)$ (Thms. 2.6.6, 2.6.7).

Sect. 3.1 Congruent Substitution Principle, $m = 0$ Principle.

Sect. 3.2 Solving $ax = b$ in $\mathbb{Z}/(m)$ (Cor. 3.2.2), $ax = 1$ in $\mathbb{Z}/(p)$ (Cor. 3.2.4), units in $\mathbb{Z}/(m)$ (Cor. 3.2.5). $\mathbb{Z}/(p)$ is a field (Cor. 3.2.8).

Sect. 3.3 Degrees add (Thm. 3.3.8), at least one factor must have small degree (Cor. 3.3.9). Units of $R[x]$ are constant polynomials that are units of R (Cor. 3.3.10).

Sect. 3.4 Division Theorem for Polynomials (Thm. 3.4.4). Remainder Theorem (Cor. 3.4.7) and Factor Theorem (Cor. 3.4.7). Degree n has $\leq n$ roots (Cor. 3.4.9).

Sect. 3.5 Euclidean Algorithm for polynomials (Alg. 3.5.4). EA works (Thm. 3.5.6), common divisors divide GCD (Cor. 3.5.7). GCD unique up to associates (Cor. 3.5.9). Unique Factorization for polynomials (Thm. 3.5.12).

Sect. 3.6 Bezout's Identity for polynomials (Thm. 3.6.1). Euclidean Reduction for polynomials (Alg. 3.6.2). Linear equations in $F[x]$ (Cor. 3.6.4).

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. 2.1 Divisors of 12 (Exmp. 2.1.5).
Sect. 2.4 Euclidean Algorithm (Exmp. 2.4.2), Signed EA (Exmp. 2.4.7).
Sect. 2.5 Euclidean Rewriting example (Exmp. 2.5.3).
Sect. 2.6 Big O estimates from homework problems.
Sect. 3.1 Names for $\mathbb{Z}/(m)$ elements (Exmp. 3.1.5), $\mathbb{Z}/(2)$ and $\mathbb{Z}/(3)$ tables (Exmp. 3.1.6), fractions and negatives in $\mathbb{Z}/(m)$ (Exmp. 3.1.7). Primitive and non-primitive elements in $\mathbb{Z}/(7)$ (Exmp. 3.1.10).
Sect. 3.2 Solving $ax = b$ (Exmp. 3.2.3).
Sect. 3.3 Multiplying polynomials (Exmp. 3.3.4). Failure of degrees adding (Exmp. 3.3.6).
Sect. 3.4 Long division of polynomials (right before Ask Yourself 3.4.3); fractions in $\mathbb{F}_5$ (Rem. 3.4.6).
Sect. 3.5 Euclidean Algorithm (Exmp. 3.5.5).
Sect. 3.6 Euclidean Rewriting example (Exmp. 3.6.3).

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. (2.3) Definition of floor.

Good luck.