The exam will be given in class on Tuesday, April 16. If, due to an emergency, you are unable to take the exam then, it is your responsibility to notify me at the earliest possible time.

You should know the axioms, definitions, and results from the textbook and class, and be able to use them in answering questions and doing proofs. I may ask you to state definitions, theorems, etc., and to prove things. I won’t ask you to give proofs of theorems proved in the textbook, but you should be able to use the techniques used in those proofs. The homework is a good general guide to the kind of problems you’ll see, though some of the homework problems are probably too long for an in-class exam. So make sure you have gone through the posted solutions to homework problems.

What do I mean by “you should know” things like definitions and results? I don’t mean that you should necessarily be able to refer to Exercise 32 or Definition 17 by number. And you don’t need to be able to quote things with exactly the same wording used in the book. But you need to know what the definitions, etc., actually say and you need to know it precisely and completely in the sense of the mathematical content.

For example, the book says

Let \( n \in \mathbb{N} \). If \( a \) and \( b \) are integers, then we say that \( a \) is congruent to \( b \) modulo \( n \) provided that \( n \) divides \( a - b \).

If the test asks you for the definition of “congruence modulo \( n \)”, you don’t need to quote this word for word, using the same letters, etc. But you would need to give a definition that is mathematically equivalent to the one in the book. So it would be fine to say something like

Two integers are congruent modulo \( n \) if their difference is divisible by \( n \).

But saying it means \( a \equiv b \pmod{n} \) won’t get you any credit.

For proofs, you can use results from the book, homework problems, or discussion in class, but you need to cite those results. You don’t need to cite theorems by the number in the book, but you should say “A theorem in the book says that . . . ” or something like that which makes it clear exactly what result your referring to.

You’ll have the whole class period (but people who come late won’t get extra time without a very good reason). No notes, books, or electronic devices can be used during the exam.

I strongly suggest that you go through the Chapter Summaries in the text. Make sure that you know the “Important Definitions” precisely and completely. There will be some questions on the exam that ask you for definitions, and you must know the definitions precisely to be able to use them in proofs. If I ask you to prove, for instance, that a certain function is a bijection, you’re unlikely to get
much credit (or even be able to think of a way to approach the problem) if you
don’t know for sure what a bijection is. And certainly review the “Important
Theorems” and proof methods (if any) and make sure you understand them
(which will probably depend on knowing and understanding the definitions!).

The exam covers the material in the text in Chapters 5, 6, 7, and 8. So I
won’t ask you a question that’s entirely on material from earlier chapters. But
the material in this course is extremely cumulative. So you still need to know
and be able to use the material that was covered on the first exam. For instance,
there won’t be a question that’s just on induction proofs, but I expect you to
be able to use induction to prove things about, say, greatest common divisors.

You’re responsible for the material in the textbook and everything we’ve
done in class. Here’s a bit more detail on the topics (though the fact that
something is listed here doesn’t mean it will necessarily be on the exam and
the fact that something isn’t mentioned here doesn’t mean it won’t be on the
exam).

Chapter 5: This chapter covers the basic definitions of set, element, subset,
containment, etc. You should know these definitions, and the basic operations
on sets, such as intersection, union, and complement. The most important note
to make about proof techniques is that showing two sets are equal is usually
done by separately showing that the first is a subset of the second and that the
second is a subset of the first. Of course, the most basic way to show that one
set is a subset of another is to show that, for all elements $x$ of the first set, $x$
is also an element of the second; and proving a universally quantified statement
usually starts by choosing an “anonymous” element of the set.

You also need to know the properties of the operations, including De Mor-
gan’s Laws, the distributive properties of union and intersection, etc.

An important construction in this chapter is the Cartesian product of two
sets.

The chapter also talks about operations involving indexed families of sets.
I think most of Section 5.5 is pretty straightforward and you shouldn’t worry
about it too much, but notice the introduction of the “big” union and intersec-
tion symbols that function like the large $\Sigma$ we use for adding indexed collections
of numbers.

Chapter 6: Chapter 6 defines functions and establishes properties of certain
classes of functions. Presumably you already knew about functions; the first
section of the chapter just reviews that definition and establishes some termin-
ology (domain, codomain, range, etc.). Note that the definition of a function $f: A \rightarrow B$ includes the domain and codomain; for two functions to be equal,
they must have the same domain and codomain. In class, we talked about for-
mally defining the function $f: A \rightarrow B$ a special kind of subset of the Cartesian
product $A \times B$; the book doesn’t discuss this until Section 6.5, but I think it’s
important for you to have this in mind as the way we make precise sense out of
the somewhat vague idea of “a rule that associates” an element of the codomain with each element of the domain.

Section 6.2 is mostly about examples of functions. Section 6.3 defines injections, surjections, and bijections (which you’ve probably encountered previously under the names “one-to-one functions”, “onto functions”, and “one-to-one and onto functions”). You need to know the definitions and be able to prove that particular functions are injective or surjective or bijective. Section 6.4 introduces composition of functions, which is also something you’ve encountered before. The definition here is the same as the one you’ve used in, e.g., calculus (but make sure you understand how composition works if we define a function as a subset of the Cartesian product). The book states some theorems about the composition of injections, etc. (though some of the proofs are left to the exercises). You should know these results and be able to prove things like them (or provide counterexamples for the versions which aren’t true). You should also know about the special identity function $I_A$ from a set $A$ to itself that maps each element to itself. (As a subset of the Cartesian product $A \times A$, it’s just the diagonal, the set $\{ (a, a) \mid a \in A \}$.)

Section 6.5 is about inverse functions. The main result here is that a function $f : A \to B$ has an inverse function $f^{-1} : B \to A$ if and only if $f$ is a bijection (in which case $f^{-1}$ is also a bijection), but I think the book’s presentation is a little confusing. This is where the book introduces the idea of a function as a set of ordered pairs. Given a function $f : A \to B$, not necessarily bijective, the book defines a subset of $B \times A$ it calls “the inverse of $f$” and denotes by $f^{-1}$. The key point is that this will just be a relation and not a function unless $f$ is bijective. (I think it’s confusing to call this “the inverse of $f$” when it’s not a function; it’s the inverse relation in a sense that’s not exactly the same as the inverse of a function, and the section is called “Inverse Functions”, so I’m not surprised if some of you had a little trouble sorting this out.)

In class, I gave a definition of an invertible function and the inverse of a function in terms of the identity functions on sets. If $f : A \to B$ and $g : B \to A$ satisfy the conditions that $g \circ f = I_A$ and $f \circ g = I_B$, we say that $f$ and $g$ are invertible and that $g = f^{-1}$ and $f = g^{-1}$. Such a $g$ exists exactly when $f$ is bijective and, in this case, we already know $g$ is a function, and we saw that it has to be the same as the book’s definition: $f^{-1}(b)$ is the unique $a$ (which has to exist and be unique because $f$ is bijective) that has $f(a) = b$. (So the difference here is that the book is willing to call something “the inverse of $f$” even when that thing is not a function and $f$ is not invertible.) The book’s Corollary 6.28 is essentially the condition about the compositions being the identity functions in my definition of invertible.

Section 6.6 talks about images and preimages of subsets of the domain and codomain under a function $f$. This is the part where I said we were extending the notation, so that if $f : A \to B$ is a function, we can talk about $f(a)$ for an element $a \in A$ and $f(X)$ for a set $X \subseteq A$. And we use the $f^{-1}(Y)$ notation for the preimage of a set $Y \subseteq B$ (though usually not for an element $b \in B$ unless $f$ really has an inverse function). The theorems in this section are pretty easy to sort out; you mainly just need to remember that things like these exist.
Chapter 7: The focus of Chapter 7 is equivalence relations. It starts with a definition of a general relation in 7.1 and gets to equivalence relations in 7.2. You certainly need to know the definition of equivalence relation, and what reflexivity, symmetry, and transitivity are. (Note that these are all at least implicitly universally quantified; if you need to prove that a relation is symmetric, you need to consider all pairs \(a, b\) with \(aRb\) and show that \(bRa\).) The most important nontrivial example of an equivalence relation discussed here is congruence modulo \(n\) on \(\mathbb{Z}\), but the section text and exercises give some additional examples. The importance of equivalence relations comes from the equivalence classes they define. You need to know the definition of equivalence classes and the fact that the equivalence classes of an equivalence relation form a partition of the set the relation is defined on. (So you need to know what a partition is.) Partitions and equivalence relations are different ways of describing the same thing: given a partition, we can construct a unique equivalence relation whose classes are the parts of the partition; and given an equivalence relation, we get a unique partition whose parts are the equivalence classes.

We went through several examples of equivalence relations where we can define operations on the set of equivalence classes. The book has a whole section on modular arithmetic and in class and on the homework, we constructed the integers from the whole numbers and the rationals from the integers, including describing the standard operations. The key point is that the operations are things that take two classes and return a class, but the way we define these operations depends on choosing elements from the classes, and so looks like it might give different results depending on which elements we take. So we need to check that our operations are well-defined, meaning that we end up with the same class no matter which elements we choose from the starting classes.

Chapter 8: Chapter 8 looks at some basic results in number theory, involving the arithmetic of \(\mathbb{Z}\). We defined the greatest common divisor (also called the greatest common factor) of two integers, not both of which are 0. We then showed how the Euclidean algorithm can be used to find the greatest common divisor efficiently (I told you about the efficiency, though we didn’t really prove that), and how the work carried out in the algorithm can be easily extended to write the greatest common divisor as a linear combination (with integer coefficients) of the two numbers. You need to be able to do this for the exam.

We can use this description of the gcd as a linear combination to prove Euclid’s lemma that if a prime divides a product \(ab\) it must divide at least one of the factors, and then to prove the uniqueness part of the Fundamental Theorem of Arithmetic. You should be able to use properties of prime factorizations to prove things about integers (and understand how one could use prime factorizations to find greatest common divisors without the Euclidean Algorithm; this is useful for proving things, but computationally the Euclidean Algorithm is much more efficient in general than having to find the prime factorizations).

We also showed how the linear combination description of the gcd can be used to find the solutions (if any exist) of a linear Diophantine equation \(ax + by = c\).
in the two variables $x$ and $y$. For us, the most important application of this is to solve linear congruences modulo $n$: If $ax \equiv c \pmod{n}$, then $ax = c + kn$ for some $k \in \mathbb{Z}$, and hence $ax - ky = c$, a linear Diophantine equation of the type we studied. (Equivalently, we can solve equations like $[a][x] = [c]$ in $\mathbb{Z}_n$.) You should know Theorem 8.22 and be able to apply it.