MATH 4000/6000 – Learning objectives to meet for Exam #1

The exam will cover all of the material this semester through what is covered in lecture on Monday, 2/17.

What to be able to state

Basic definitions

You should be able to give precise descriptions of all of the following:

- properties of $\mathbb{Z}$ from the handout (know, for instance, what "commutativity of addition" means, and what the "well-ordering principle" says)
- greatest common divisor of two integers
- $a \equiv b \pmod{m}$
- ring, commutative ring
- $\mathbb{Z}_m$; know how to describe $\mathbb{Z}_m$ both as a set (tell me what its elements are, including what we mean when we write $\bar{a}$) and as a ring (tell me how we define $+$ and $\cdot$)
- the terms unit, zero divisor, integral domain, and field
- construction of $\mathbb{Q}$ from $\mathbb{Z}$, including the definition of a/b as an equivalence class

Big theorems

Give full statements of each of the following results, making sure to indicate all necessary hypotheses. For results proved in class or on HW, describe the components and main ideas of the proof.

- 1 is the least element of $\mathbb{Z}^+$
- Binomial Theorem, in $\mathbb{Z}$ and in any commutative ring
- Division Algorithm for $\mathbb{Z}$
- $\gcd(a, b)$ is a $\mathbb{Z}$-linear combination of a, b
- the "Fundamental gcd Lemma" ($a \mid bc$ and $\gcd(a, b) = 1 \implies a \mid c$)
- Euclid's Lemma
- unique factorization theorem for natural numbers (Fun. Theorem of Arithmetic)
- basic facts about congruences, such as "congruence mod m is an equivalence relation" and "congruences to the same modulus play nice with addition and multiplication"
- Chinese remainder theorem (both parts: so you should know how to describe all solutions to $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ whenever m and n are relatively prime)
- simple identities that hold in every ring, like $a \cdot 0 = 0$, $(-1)a = -a$, etc.

- for natural numbers m, the ring $\mathbb{Z}_m$ is a domain $\iff$ m is prime
- for natural numbers m, the ring $\mathbb{Z}_m$ is a field $\iff$ m is prime
- fields are integral domains
- if $\gcd(a, m) = 1$, then $\bar{a}$ is a unit in $\mathbb{Z}_m$, and conversely
- finite integral domains are fields (proved on HW)

What to be able to compute

The first problem on the exam will assess your computational abilities and will have multiple parts. You are expected to know how to use the methods described in class to solve the following problems.

- compute greatest common divisors using Euclid's algorithm
- given integers a and b, compute integers x and y with $ax + by = \gcd(a, b)$
- compute all solutions x to a congruence of the form $ax \equiv b \pmod{m}$ or prove that no such solution exists
- determine all solutions to a system of two simultaneous congruences when the moduli are relatively prime

What else?

This is a proofs-based class. As such, there will be questions which are neither computational nor definitional, requiring you to assemble ideas in fresh ways to establish statements that you have not already seen before. The proof problems on your HW are representative of the sorts of proofs you might be asked for on an exam, although I will be more sensitive to time constraints for exam problems.

Practice problems

1. (a) Determine $\gcd(33, 18)$ by using the Euclidean algorithm. **Show your steps.** You must use the Euclidean algorithm to receive credit.

   (b) **Using the method of backtracking and your work in (a)**, find a pair of integers X and Y with $33X + 18Y = \gcd(33, 18)$. You must use the backtracking method to receive credit.

   (c) What are *all* integer solutions x to the congruence $18x \equiv 15 \pmod{33}$? I am looking for the answer only; no proof necessary.

2. Let R be a ring. (Do not assume R is commutative!)

   (a) What does it mean to say that an element $x \in R$ is a **zero divisor** in R?

   (b) Let a be a nonzero element of R. Suppose that a^2 is a zero divisor in R. Prove that a is a zero divisor in R.

3. Let $m \in \mathbb{Z}^+$.

   (a) What is meant by $\mathbb{Z}_m$? Tell me both the elements of the set $\mathbb{Z}_m$ and the definitions of addition and multiplication. If you use the bar notation, you must define it.

   (b) List the squares in the ring $\mathbb{Z}_8$.

   (c) Explain why it is impossible to write 800007 in the form $a^2 + b^2 + c^2$ for integers a, b, and c.

4. (a) If R is a ring, what does it mean to say that u is a **unit** in R? If you use the term **multiplicative inverse**, you must define that. Make sure your definition does not assume R is commutative.

   (b) Suppose $x \in R$ satisfies $x^{10} = 0$. Show that $1 - x$ is a unit in R.

   (c) Determine, **with proof**, all $x \in \mathbb{Z}_{44}$ that satisfy $x^{10} = 0$. [You should *not* need or want to use your answer to part (a) for this!]

5. (a) State precisely and completely the equivalence class definition of "a/b" introduced when defining $\mathbb{Q}$.

   (b) Prove that every element of $\mathbb{Q}$ can be written in the form a/b where $\gcd(a, b) = 1$. You may use any results proved in class or on homework.