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

The exam will cover all of Chapter 1 as well as §2.1, up to but **not** including the material on ordered fields. There will be at most one problem from Chapter 2.

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
- congruences modulo 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
- Division Algorithm/Division Theorem for $\mathbb{Z}$
- $\gcd(a, b)$ is a linear combination of a, b
- the "fundamental gcd lemma" ($a \mid bc$ and $\gcd(a, b) = 1 \Longrightarrow a \mid c$)
- Euclid's lemma
- unique factorization theorem for natural numbers
- 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
- 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 field $\iff$ m is prime
- fields are integral domains
- if m is prime, then $\mathbb{Z}_m$ is a field
- 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 simultaneous congruences

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) What does it mean to say that a positive integer is a **prime number**?

   (b) **Carefully** state the Unique Factorization Theorem (alternatively called the Fundamental Theorem of Arithmetic).

   (c) Let p be a prime number. Suppose a is a positive integer for which $p \mid a^{2022}$. Prove that $p^{2022} \mid a^{2022}$.

2. (a) Let m be a positive integer. What is meant by $\mathbb{Z}_m$? Tell me both the elements of the set $\mathbb{Z}_m$ and the definition of additions and multiplication. If you use the bar notation, you must define it.

   (b) Is there a nonzero element x of $\mathbb{Z}_{15}$ with $x^{100} = 0$ in $\mathbb{Z}_{15}$? If so, give an example. If not, prove that none exist.

   (c) Is there a nonzero element x of $\mathbb{Z}_{45}$ with $x^{100} = 0$ in $\mathbb{Z}_{45}$? If so, give an example. If not, prove that none exist.

3. (a) List the distinct cubes in $\mathbb{Z}_7$.

   (b) Show that if x, y, z are integers satisfying the equation $x^3+y^3 = z^3$, then 7 divides at least one of x, y, or z.

4. A ring R is said to have **finite characteristic** if there exists a positive integer n such that

$$0 = \underbrace{1 + 1 + 1 + \cdots + 1}_{n \text{ times}}$$

   in R. In that case, the smallest such n is called the characteristic of R.

   (a) Give an example of a ring of characteristic 7.

   (b) State carefully the definition of an **integral domain**.

   (c) Show that an integral domain cannot have characteristic 6.

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

   (b) Show that every element of $\mathbb{Q}$ can be written in the form a/b where $\gcd(a, b) = 1$.

6. (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) Let R be a ring and suppose $x \in R$ has $x^2 = 0$. Show that $1 - x$ is a unit in R.

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

Textbook problems

You should carefully review the solutions to all of the assigned homework. In addition, I recommend looking at the following problems from your textbook:

§1.2: 1, 5, 6, 21

§1.3: 9, 18, 20(b,d,f,h), 21(a,f)

§1.4: 1, 7, 10, 14