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

The exam will cover Chapter 1, i.e., the material covered in class through 2/8.

## What to be able to state

### Basic definitions

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

- properties of $\mathbf{Z}$ 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
- $\mathbf{Z}_m$; know how to describe $\mathbf{Z}_m$ 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

### 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 $\mathbf{Z}^+$
- binomial theorem
- division algorithm for integers
- 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
- basic facts about congruences, such as "congruence mod $m$ is an equivalence relation" and "congruences to the same modulus are preserved under 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 $\mathbf{Z}_m$ is a field $\iff$ $\mathbf{Z}_m$ is an integral domain $\iff$ $m = p$ is prime

- for natural numbers $m$, the ring $\mathbf{Z}_m$ is a field $\iff$ $m = p$ is prime; the same with "field" replaced by "integral domain"
- fields are integral domains
- finite integral domains are fields

### What to be able to compute

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
- solve 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.

## Extra 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, 13, 17, 18, 20(b,d,f,h), 21(a,f), 34(a)

§1.4: 1, 7, 10, 14, 15