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

The exam will cover §1.1–§2.1 of the course notes. §2.2, on the properties of real numbers, is not examinable.

What to be able to state

Basic definitions

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

- basic properties of $\mathbf{Z}$ (all properties on the handout)
- greatest common divisor of two integers
- congruences modulo m
- ring, commutative ring
- definition of exponentiation
- $\mathbf{Z}_m$; know how to describe $\mathbf{Z}_m$ both as a set (i.e., tell me what its elements are) and as a ring (tell me what the operations on the set are)
- the terms unit, zero divisor, integral domain, field
- ordered integral domain
- construction of $\mathbf{Q}$ from $\mathbf{Z}$

Big theorems

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

- 1 is the smallest positive integer
- binomial theorem
- division algorithm for integers
- 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
- description of solutions to a linear congruence $ax \equiv b \pmod{m}$
- simple identities that hold in every ring, like $a \cdot 0 = 0$, $(-1)a = -a$, etc.

- $\mathbf{Z}_m$ is a ring for every positive integer m
- 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
- $\mathbf{Q}$ (as constructed from $\mathbf{Z}$ in class) is an ordered field

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, 3, 5, 6, 21

§1.3: 2, 3 (look at the last j decimal digits), 9, 13, 17, 18, 20(b,d,f,h), 21(a,f), 34(a)

§1.4: 1, 5, 7, 15, 20

§2.1: 3 (do this for any ordered field), 4 (you more or less did this already), 8, 12 (without finding the fields of quotients), 14