Math 4000 – Learning objectives to meet for Exam #1

The exam will cover §1.1–§2.1 of the course notes. §2.2, on the construction of the 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 $\mathbf{Z}$ (including the ring axioms, order axioms, well ordering principle)
- 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 (i.e., tell me what its elements are) and as a ring (tell me what the operations on the set are)
- the terms integral domain and field
- 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.

- there are no integers between 0 and 1
- 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
- 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
- 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 (we didn't ever prove this explicitly, but you should be able to fashion a proof from results we did talk about in class), 6, 21

§1.3: 2, 9, 13, 17, 18, 20(b,d,f,h), 21(a,f), 34(a)

§1.4: 1, 15 (this is related to 9(b) from your last HW), 20

§2.1: 3 (do this for any ordered field), 4 (you more or less did this already), 8, 12 and 13 (but without finding the fields of quotients)

Here are some more problems to try.

1. Let p be a prime. Suppose R is a commutative ring in which $\overbrace{1 + 1 + 1 + \cdots + 1}^{p \text{ times}} = 0$. ($\mathbf{Z}_p$ is one example of such a ring, but there are many others.) Show that for any $x, y \in R$, we have
$$(x + y)^p = x^p + y^p.$$
More generally, show that for any natural number n,
$$(x + y)^{p^n} = x^{p^n} + y^{p^n}.$$

2. Let R be an integral domain. If there is a natural number n with $\overbrace{1+1+1+\cdots+1}^{n \text{ times}} = 0$, then the smallest such n is called **the characteristic of** R. If no such n exists, we say R has characteristic 0. For example, $\mathbf{Z}$ has characteristic 0, while $\mathbf{Z}_3$ has characteristic 3.

   Show that if R is finite, then (a) R has nonzero characteristic, and (b) if p is the characteristic of R, then p is a prime number.

   Hint for (a): There must be (why?) distinct positive integers $n < m$ with

$$\overbrace{1+1+1+\cdots+1}^{n \text{ times}} = \overbrace{1+1+1+\cdots+1}^{m \text{ times}}.$$

   Remark: The converse of (a) is not true; there are infinite integral domains with positive characteristic. One example is the ring of one-variable polynomials over $\mathbf{Z}_p$, which we will study later in the course.

3. Let F be an ordered field. Show that F has characteristic 0. Conclude that every ordered field is infinite.

4. Let F be a field of characteristic 0. To avoid cumbersome notation, for each natural number n, the element

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

   of F will be denoted simply by n, and the element

$$\underbrace{(-1)+(-1)+(-1)+\cdots+(-1)}_{n \text{ times}}$$

   by $-n$. We continue to use 0 to denote the additive identity of F.

   (a) For an integer n, show that $n = 0$ in F if and only if $n = 0$ in $\mathbf{Z}$.

   (b) Show that for every nonzero $n \in \mathbf{Z}$, the element n of F is a unit.

   (c) Find an embedding of $\mathbf{Q}$ into F. In other words, describe a map $\iota\colon \mathbf{Q} \to F$ which is one-to-one and operation preserving: $\iota(\alpha+\beta) = \iota(\alpha)+\iota(\beta)$ and $\iota(\alpha\beta) = \iota(\alpha)\iota(\beta)$.

5. (Continuation)

   (a) Now assume F is an ordered field. Show that the map ι you wrote down in 4(c) is "order-preserving", in the following sense: If $\alpha > 0$ in $\mathbf{Q}$, then $\iota(\alpha) > 0$ in F, and vice versa.

   (b) Assume F is an ordered field. Show that if $\alpha, \beta \in F$ and $\alpha < \beta$, then there is a $\gamma \in F$ with $\alpha < \gamma < \beta$.

6. Let R be a ring, not necessarily commutative. If $x^{100} = 0$, show that $1 - x$ and $1 + x$ are units in R.