MATH 4400 – Learning objectives to meet for Exam #1

The exam covers everything up through the lecture on Friday, Feb. 8.

What to be able to state

Basic definitions

You should be able to give complete and precise definitions of each of the following items:

- prime number
- the function $v_p(n)$
- $\gcd(m, n)$ and $\text{lcm}[m, n]$
- congruence modulo m
- the "residue ring" $\mathbb{Z}_m$
- abelian group, and associated terms: order of an element in an abelian group, cyclic group, generator, homomorphism, isomorphism
- Euler's ϕ-function

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 homework, describe the components and main ideas of the proof.

- Division algorithm in $\mathbb{Z}$
- Unique factorization theorem
- Formulas for gcds and lcms in terms of prime factorizations
- Characterization of units in $\mathbb{Z}_m$
- If G is an abelian group of size n, then $g^n = \mathbb{1}$ for all $g \in G$.
- Fermat's little theorem
- Euler's theorem
- If G is an abelian group, and $g \in G$ has order d, then $g^m = \mathbb{1} \iff d \mid m$.
- If G is an abelian group, and $g \in G$ has order n, then the distinct powers of g are $g^0, g^1, \ldots, g^{n-1}$.
- If G is an abelian group and $g \in G$ has order n, then $g^{n/d}$ has order d for every divisor d of n.
- Formula for the order of an element of $\mathbb{Z}_m$, under addition
- Number of elements of a given order in $\mathbb{Z}_m$, under addition
- $\sum_{d|m} \phi(d) = m$.
- If G is an abelian group, and $a, b \in G$ have coprime orders m, n, then ab has order mn.
- If $R \cong S$, then $U(R) \cong U(S)$.

- If m and n are relatively prime, then $U(\mathbf{Z}_{mn}) \cong U(\mathbf{Z}_m \times \mathbf{Z}_n)$.
- $U(\mathbf{Z}_p)$ is a cyclic group for all primes p.
- Characterization of when $U(\mathbf{Z}_m)$ is cyclic
- ϕ is multiplicative
- Every cyclic group is isomorphic to $\mathbf{Z}$ or $\mathbf{Z}_m$, under addition.

What to be able to do

You can expect 5 problems on the exam. At least one will be purely computation-focused; you should know how to use the methods from class for all of the following.

- Calculate gcds or lcms given prime factorizations
- Compute the number of divisors of a given integer, given its prime factorization
- Compute $\phi(m)$ given the prime factorization of m
- Determine whether or not a linear congruence has a solution, and determine the number of solutions
- Calculate a^k modulo m efficiently (as in HW #2, question 2)

I will not ask you to reproduce our proof of when $U(\mathbf{Z}_m)$ is cyclic — but I may ask you questions which test the underlying concepts. You can expect one or more proof-based questions on the theory of finite abelian groups; as a starting point, please make sure you can prove all of the 'big theorems' about them mentioned above.