MAT 312/AMS 351 Fall 2010 Review for Midterm 1

§1.2. Understand how to use induction to prove that a statement $P(n)$ holds for every integer n. Example: $P(n)$ is the statement $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$. Problem 2 p.14. Example: The binomial coefficients $\begin{pmatrix} n \\ k \end{pmatrix}$ are defined for $0 \leq k \leq n$ by $\begin{pmatrix} n \\ 0 \end{pmatrix} = \begin{pmatrix} n \\ n \end{pmatrix} = 1$ and $\begin{pmatrix} n+1 \\ k+1 \end{pmatrix} = \begin{pmatrix} n \\ k \end{pmatrix} + \begin{pmatrix} n \\ k+1 \end{pmatrix}$; and $P(n)$ is the statement that $\begin{pmatrix} n \\ k \end{pmatrix} = \frac{n!}{k!(n-k)!}$ for every $0 \leq k \leq n$.

§1.3 Understand the statement of the division algorithm, especially how to show the uniqueness of the quotient and the remainder. Understand the definition of the *greatest common divisor* d of two positive integers a and b, and the notation $d = (a, b)$. Be able to apply the Euclidean Algorithm to two integers a and b, yielding their g.c.d. d. Be able to use that calculation to express d as an integral linear combination of a and b: $d = j \cdot a + k \cdot b$. Example 1.26 p. 23. Understand the special case: if $(a, b) = 1$, then there exist integers j and k such that $1 = ja + kb$. Understand the proof of Theorem 1.30 (i): it uses that special case. Review assigned exercises on p. 28, 29.

§1.4 Be able to reproduce the definition of *prime number*. Understand the "Fundamental Theorem of Arithmetic" and be able to factorize any integer ≤ 1000 (note that it must be prime, or have a prime factor ≤ 31). Know how to prove that there are infinitely many primes. Given prime factorizations for a and b, be able to immediately write down the factorization of their g.c.d, and be able to calculate their least common multiple from the rule $(\gcd(a, b))(\mathrm{lcm}(a, b)) = ab$. (Corollary 1.40 p.33).

§1.5 Know the proof that $\sqrt{2}$ is not rational.

§1.6 Understand that $\equiv_n$ ("congruence mod n") is an equivalence relation, and that the equivalence classes ("congruence classes") form a system of numbers closed under addition and multiplication. This is modular arithmetic. Be comfortable with calculations in modular arithmetic: know how to represent each congruence class modulo n by a number in the range $0, \ldots, n-1$. Be able to construct addition tables and multiplication tables modulo n. Understand what it means for a class $[a]_n$ to be *invertible*: there exists a class $[b]_n$ such that $[a]_n[b]_n = [1]_n$; equivalently, $ab \equiv_n 1$. Know how to prove that if n is prime, every *nonzero* class mod n is invertible. And know how to show that if n is not prime, then there exist some non-invertible classes: be able to prove that $[a]_n$ is invertible if and only if $(a, n) = 1$. Review homework.