MAT 312/AMS 351 Fall 2010 Review for Midterm 2

§1.7. Understand that if $(a, n) = 1$, then the equation $ax \equiv b \bmod n$ has a unique solution (mod n) and know how to find it. That is the simplest case. Example 1.68 p.45. More generally, understand that if $(a, n) = d$, then the equation $ax \equiv b \bmod n$ has d solutions (mod n) if and only if $d|b$, and that all these solutions are congruent mod n/d. Know how to find them. Example 1.69 p.45.

Know how to apply the proof of the "Chinese Remainder Theorem" to solve a system of congruences. Example 1.71 p.46.

Non-linear congruences will not be covered on the exam.

§1.8. Understand how to prove "Fermat's Little Theorem" (p.51) and how to apply it. More generally, know the definition of $\varphi(n)$ for any positive integer n ("the Euler φ-function"). Know how to calculate $\varphi(n)$ given the prime factor decomposition of n (Theorem 1.86). Know how to apply Euler's theorem: if $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1$ modulo n.

§1.9 Understand the principle behind the RSA method for public-key cryptography: choose two large primes, p, q and publish the product pq along with a number a of your choice, which is relatively prime to $\varphi(pq)$. You keep p and q secret. Without knowing p and q, your competitors cannot calculate $\varphi(pq)$, and so cannot calculate the multiplicative inverse of a mod $\varphi(pq)$. But you can; call it A. Anyone can encode a number n as n^a mod pq, but only you can decode n^a by raising it to the power A. This works since $(n^a)^A = n^{aA} = n^{k\varphi(pq)+1} = n^{k\varphi(pq)} \cdot n = (n^{\varphi(pq)})^k \cdot n \equiv 1 \cdot n \bmod pq$.

§3.1 Understand that a permutation is a one-one function π from a finite set S to itself. If S has n elements, it is standard to label them with the integers $1, 2, 3, \ldots$. Then knowing π is equivalent to knowing $\pi(1), \pi(2), \pi(3), \ldots$. Understand the "two-row matrix" notation (bottom of p. 71). Understand what the inverse π^{-1} of π is, and be able to read it off from the two-row matrix notation. Understand that the product $\pi\sigma$ of two permutations of the same set means the composition of the functions π and σ, so that $\pi\sigma(k) = \pi(\sigma(k))$: be careful to pay attention to the order (page 72, Example 3.3). Understand how cycle notation is more compact, what disjoint permutations are, and be able to write any permutation as a product of disjoint cycles (Theorem 3.11). Be good at multiplying cycles, especially non-disjoint ones. Be able to write the multiplication table for the permutations on three elements using cycle notation (p. 75).

Review homework.