MAT 312/AMS 351 Spring 2014 Review for Midterm 1, Lecture 1 (Kirillov)

General

The exam will be in class on Th, Feb 27. It will consist of 5 problems. It will be closed book: no books or notes allowed. Calculators are allowed (but are useless). Of course, no cell phones and no laptops, tablets, or other electronic devices can be used.

The exam will cover material up to and including Section 1.6 (except for public key cryptography). For your convenience, a listing of topics covered and skills expected of you is given below.

Material covered

§1.1 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: $d = s \cdot a + t \cdot b$. Examples, pp. 10, 11. Understand the special case: if $(a, b) = 1$, then there exist integers j and k such that $1 = s \cdot a + t \cdot b$. Understand the proof of Theorem 1.1.6, p. 13: it uses that special case. Review assigned exercises on p. 15.

§1.2. Understand how to use induction to prove that a statement $P(n)$ holds for every integer n. Example (p. 17): $P(n)$ is the statement $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$. Problem 2 p.14. Example (see Theorem 1.2.1): The binomial coefficients $\left(\begin{array}{c} n \\ k \end{array} \right)$ are defined for $0 \leq k \leq n$ by $\left(\begin{array}{c} n \\ 0 \end{array} \right) = \left(\begin{array}{c} n \\ n \end{array} \right) = 1$ and $\left(\begin{array}{c} n+1 \\ k+1 \end{array} \right) = \left(\begin{array}{c} n \\ k \end{array} \right) + \left(\begin{array}{c} n \\ k+1 \end{array} \right)$; and $P(n)$ is the statement that $\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{n!}{k!(n-k)!}$ for every $0 \leq k \leq n$.

§1.3 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). Understand Lemma 1.3.2 (p. 27; it uses Theorem 1.3.1): if p is prime and divides the product $a_1 a_2 \cdots a_r$ then p must divide at least one of the factors. 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 1.3.5 p. 27).

§1.4 Understand the relation of congruence mod n (p. 36); and that the congruence classes mod n form a system of numbers closed under addition and multiplication. This is modular arithmetic. Be comfortable with calculations in modular arithmetic (Theorem 1.4.1); 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 more generally know how to show that $[a]_n$ is invertible if and only if $(a, n) = 1$. Know the definition of $\mathbb{Z}_n^* = G_n$, the set of invertible classes mod n. Be able to prove that for $n \geq 2$, the product of any two elements of G_n is also in G_n (Theorem 1.4.7, p. 47) Review homework.

§1.5 Understand that the congruence equation

$$ax \equiv b \bmod n$$

only has solutions if $d = (a, n)$ divides b; in case $d|b$, understand why there are d distinct solutions, and be able to calculate them in examples. (Theorem 1.5.1, p. 50). Understand how to apply the "Chinese Remainder Theorem" (1.5.2, p. 54) to solve simultaneous congruences mod relatively prime moduli m and n. Note that the solution is unique mod mn. This allows extension to a third congruence ℓ as long as $(\ell, m) = (\ell, n) = 1$ (Example, page 56, bottom).

§1.6 Understand the definition of the Euler ϕ-function: $\phi(n)$ is the number of integers between 1 and n which are relatively prime to n. (Note that 1 counts!). Understand why if p is prime, then $\phi(p) = p - 1$. Be able to use the identities $\phi(p^n) = p^n - p^{n-1}$ (p prime) and $\phi(ab) = \phi(a)\phi(b)$ (a, b relatively prime), along with factorization into primes, to calculate $\phi(n)$ for any integer n.

Understand the concept of the *multiplicative order* of a mod n.

Know how to prove Fermat's Theorem (1.6.3): if p is prime, and a is not divisible by p, then $a^{p-1} \equiv 1 \bmod p$ and Euler's Theorem:

$$\text{if } (a, n) = 1 \text{ then } a^{\phi(n)} \equiv 1 \bmod n.$$

Use this and 1.6.2 to deduce Corollary 1.6.4: with p and a as above, the multiplicative order of a mod p must divide $p - 1$. Be able to find remainders of large powers of a number mod n (e.g., $5^{2014} \bmod 7$).

Practice problems

(1) Compute $\gcd(935, 272)$ and write it in the form $935x + 272y$.
(2) Compute the multiplicative inverses of the following numbers in modular arithmetic:
    11 mod 73
    18 mod 46
    29 mod 31
(3) Let the sequence a_n be defined by the rule $a_1 = 3$, $a_{n+1} = 2a_n + 1$. Guess the formula for a_n and prove it using induction. Be certain to write your arguments carefully.
(4) Solve the system of congruences

$$x \equiv 4 \mod 17$$
$$x \equiv 1 \mod 13$$

(5) Find $3^{942} \bmod 5$.
(6) Compute $\phi(244)$.