MAT 312/AMS 251 FALL 2015
REVIEW FOR MIDTERM I

General

The exam will be in class on Thursday, October 1. It will consist of 5 problems and will be a closed book exam: no books, notes, laptops, tablets, cell phones, etc. The exam will cover all material in Chapter 1, except for the public key codes in §1.6. The list of covered topics and expected skills is given below.

Material covered

§1.1 Understanding of the division algorithm, especially the uniqueness of the quotient and the remainder. Understand the definition of the *greatest common divisor* of two positive integers a and b, and the notation $d = (a, b)$. Know how to apply the Euclidean algorithm to find the g.c.d of two integers a and b. Be able to use this calculation in a matrix form to express d as an integral linear combination of a and b,

$$d = as + bt, \quad s, t \in \mathbb{Z}.$$

Do Examples 1 and 2 and understand the special case $(a, b) = 1$. Understand the statement and the proof of Theorem 1.6.1, and review assigned exercises on p. 15.

§1.2 Understand how to use induction to prove that the statement $P(n)$ holds for every integer n. Go over all examples and assigned exercises on pp. 23-25.

§1.3 Be able to reproduce the definition of the prime number. Understand the Sieve of Eratosthenes and the Unique Factorization Theorem and be able to factorize every integer ≤ 1000: it is either a prime or contains a prime factor ≤ 31 (the largest prime number less than $\sqrt{1000}$). Understand Lemma 1.3.2: if a p is a prime that divides the product $a_1 a_2 \cdots a_r$, than p divides at least one of the factors $a_1, a_2, \ldots, a_r$. Know how to prove that there are infinitely many primes. Given a prime factorization of a and b, be able to immediately write down the prime factorizations of their g.c.d. and l.c.m.

§1.4 Understand the relation of congruence $\mod n$ and that elements in $\mathbb{Z}_n$ — the congruence classes $\mod n$ — can be added and multiplied. This is called the modular arithmetic. Be comfortable with all calculations in modular arithmetic, know how to represent each congruence class by a number in the range $0, 1, \ldots, n-1$. Be able to construct addition and multiplication tables for $\mathbb{Z}_n$. Understand what it means for a class $[a]_n$ to be *invertible*: there is a class $[b]_n$ such that $[a]_n[b]_n = [1]_n$. Equivalently,

$$ab \equiv 1 \mod n.$$

Know how to prove that $[a]_n$ is invertible if and only if $(a, n) = 1$ and how to find $[a]_n^{-1}$. Understand the definition of $G_n = \mathbb{Z}_n^*$ — the set of invertible elements in $\mathbb{Z}_n$ — and be able to prove Theorem 1.4.7: the product of two elements in G_n is in G_n. Review the homework.

§1.5 Understand that the congruence

$$ax \equiv b \mod n$$

in $\mathbb{Z}_n$ only has solutions if $d = (a, n)$ divides b and in this it has d distinct solutions $\mod n$ (this is Theorem 1.5.1). Understand how to apply Chinese Remainder Theorem to solving simultaneous congruencies with respect to relatively prime moduli m and n, and that solution is unique modulo mn. Understand how this allows extension to the third congruence modulo l provided $(l, m) = (l, n) = 1$.

§1.6 Understand the definition of the Euler φ-function: $\varphi(n)$ is the number of invertible elements in $\mathbb{Z}_n$, that is, the cardinality of G_n. In other words, it is the number of elements $1, 2, \dots, n$ which are relatively prime to n. Understand why if p is a prime $\varphi(p) = p - 1$ and $\varphi(p^n) = p^n - p^{n-1}$. Be able to use $\varphi(ab) = \varphi(a)\varphi(b)$, along with the factorization into primes, to calculate $\varphi(n)$ for any integer n.

Understand the concept of the *multiplicative order* of $a \mod n$, know how to prove Fermat and Euler Theorems:

$$a^{p-1} \equiv 1 \mod p \quad \text{if} \quad (a, p) = 1,$$

p is a prime, and

$$a^{\varphi(n)} \equiv 1 \mod n \quad \text{if} \quad (a, n) = 1.$$

Understand Corollaries 1.6.4 and 1.6.8 and how to use them to simplify large powers of a number $\mod n$ in Examples 1 and 2 on pages 65 and 69.

Sample practice problems

1) Find the g.c.d. of $12n + 1$ and $30n + 2$.
2) Compute $(935, 272)$ and write it as $935x + 272y$ for integer x and y.
3) Let F_n be the Fibonacci sequence, defined as F_1, $F_2 = 1$ and for every $n > 2$, $F_n = F_{n-1} + F_{n-2}$. Prove that
$$F_1 + F_3 + \dots + F_{2n-1} = F_{2n}.$$
4) Let a_n be the sequence defined as follows: $a_1 = 1$ and $a_{n+1} = 2a_n + 1$. Guess the formula for a_n and prove it using induction.
5) Let a, b and c be positive integers such that $a^2 + b^2 = c^2$. Prove that at least one of them is divisible by 3.
6) Compute multiplicative inverses (if they exist) of the following congruence classes: $[11]_{73}, [15]_{25}, [18]_{23}, [18]_{46}, [29]_{31}$.

7) Find the minimal positive integer which has a remainder 4 when divided by 7 and remainder 5 when divided by 12.
8) Solve the system of congruence equations

$$\begin{aligned} x &\equiv 4 \mod 17 \\ x &\equiv 1 \mod 13 \end{aligned}$$

9) Solve the following system of congruence equations

$$\begin{aligned} 5x &\equiv 7 \mod 13 \\ x &\equiv 4 \mod 11 \\ 3x &\equiv 6 \mod 9 \end{aligned}$$

10) Find $3^{392} \mod 5$, $3^{288} \mod 11$, $3^{99} \mod 21$.
11) Compute $\varphi(244)$.
12) Find the last two digits of 1221^{122}.