Math 406 – Fall 2009

Review Sheet for First Midterm

The first midterm exam for Math 406 will be held on **Thursday, October 8**, during class time. The sections in the textbook covered on the midterm are 1-6, the function $d(n)$ from section 7 (we called it $\tau(n)$ in class), and appendix A. You are expected to be familiar with the material as it was covered in class. In particular, you may be asked to give definitions of mathematical concepts or statements of theorems, and do simple proofs as on the homework assignments. No calculators are required or allowed on any Math 406 exam.

Review Questions

1) Use induction to prove that

a) $\sum_{k=1}^{n} k \cdot k! = 1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n+1)! - 1.$

b) $1^2 - 2^2 + 3^2 - \cdots + (-1)^{n-1} n^2 = (-1)^{n-1} n(n+1)/2.$

2) a) Let a and b be two integers with $b > 0$. What are the quotient and the remainder in the division of a by b?

b) Note that $64 = 8^2 = 4^3$ is simultaneously a square and a cube. Show that if n is both a square and a cube, then the remainder in the division of n by 7 must be 0 or 1.

3) If a and b are natural numbers, what is the greatest common divisor of a and b? If x and y are two integers such that $ax + by = \gcd(a, b)$, prove that $\gcd(x, y) = 1$.

4) a) Use the Euclidean algorithm to find $\gcd(481, 299)$.

b) Let f_n be the n-th Fibonacci number. Use the Euclidean algorithm to prove that f_n and f_{n+1} are coprime, for any natural number n.

5) What is a prime number? Prove that the set of all prime numbers is an infinite set. Find all pairs (x, y) of natural numbers such that $x + y$ and xy are both prime numbers.

6) State the Fundamental Theorem of Arithmetic. Write the integer 999000 in the canonical form given by this theorem.

7) Find a natural number n with exactly 60 positive divisors.

8) Solve the linear congruences $25x \equiv 15 \pmod{29}$ and $6x \equiv 15$ (mod 21).

9) State divisibility criteria for the integers $2, 3, 5, 7, 9, 11$.

10) A number is called *palindromic* if it reads the same forwards and backwards, for example 5203773025. The number 11 is a palindromic prime with an even number of digits. Prove that all other palindromic primes, such as 353 or 71317, must have an odd number of digits.

11) Let $F_n = 2^{2^n} + 1$ be the n-th Fermat number. Show that $F_n - 2 = F_{n-1}F_{n-2}\cdots F_0$ for any $n > 0$. Deduce that $\gcd(F_m, F_n) = 1$ whenever $m \neq n$, and thus obtain another proof that there are infinitely many prime numbers.

12) a) When do we say that two integers a, b are congruent modulo n? If $ab \equiv ac \mod n$, does it follow that $b \equiv c \mod n$?

b) If $a \equiv b \mod n$ and $c \equiv d \mod n$, prove that $a + c \equiv b + d \mod n$ and $ac \equiv bd \mod n$.

13) Construct tables for addition and for multiplication modulo 6.

14) True or False: a) If n is both a square and a cube, then there must be an integer x so that $n = x^6$; b) If $n > 1$ then $n^3 + 1$ is always a composite number; c) If $a \equiv b \mod m$ and $c \equiv d \mod n$, then $ac \equiv bd \mod mn$. Why or why not?

15) Use residues to prove that 7 divides $2^{10} + 3^{20} + 4^{30} + 5^{40}$.

16) Show that 100 divides $1^{99} + 2^{99} + \cdots + 99^{99}$.

17) Find the last two digits of the number 3^{100}.

18) Find the digits x and y such that the number $\overline{123xy6789}$ is divisible by 99.

19) State the Chinese remainder theorem. Find an integer that leaves a remainder of 9 when it is divided by either 10 or 11, but that is divisible by 13.

20) Find a natural number n that leaves remainder 1 when divided by 2, remainder 2 when divided by 3, remainder 3 when divided by 4, …, remainder 19 when divided by 20.

21) a) State Fermat's little theorem. b) Find a natural number $n < 11$ such that $1492^{1776} + n$ is divisible by 11.

22) a) State Wilson's theorem.

b) Use Wilson's theorem to prove the following: For any prime number p and any integer k with $0 \leqslant k \leqslant p-1$, we have $k!(p-1-k)! \equiv (-1)^{k+1}$ (mod p). [Hint: Write $(p-1)!$ as $k! \cdot (p-1)(p-2)\cdots(p-(p-k-1))$.]