Information for Midterm 1

October 11, 2019

Work covered: Sections 1 – 8

Definitions and Notations

Make sure you understand and know all definitions and notations. Suggestion: make a list of all the following definitions, and learn them from your list.

- *a is congruent to b modulo m*, $a \equiv b \pmod{m}$
- *least residue* of $a \pmod{m}$
- *linear* congruence
- *solution* to a congruence
- $d(n)$: number of positive divisors of n
- $\sigma(n)$: sum of the positive divisors of n
- write down $d(n)$ and $\sigma(n)$ if $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$
- *multiplicative* function
- *perfect* number
- *Mersenne* prime, *Mersenne* number (a composite number $m = 2^p - 1$, where p is prime)

Theorems

You must know the statements of all the theorems. Suggestion: make a separate list of the statements of all the theorems, and learn them from your list.

You need to know the proofs of the following theorems.

- Section 1: Corollaries 1.1 – 1.3 (they are really just exercises)
- Section 2: Lemmas 2.1 – 2.5, Theorems 2.1, 2.2

- Section 3: None
- Section 4: Theorems 4.1 – 4.5
- Section 5: None
- Section 6: Lemmas 6.1 – 6.3, Theorems 6.1, 6.2
- Section 7: None
- Section 8: Theorem 8.1. (The rest is for next time.)

Applications of Theorems

- Various problems concerning prime numbers.
- Use the definition and equivalent formulations of the statement "$a \equiv b \pmod{m}$" interchangeably.
- Various results about congruences and least residues.
- Determine whether a linear congruence has a solution (e.g., by using the Euclidean algorithm and Theorem 5.1), and if so, find all solutions.
- Use linear congruences to solve linear Diophantine equations.
- Use the Chinese Remainder Theorem to solve a congruence $\pmod{m}$, where m is composite.
- Use Fermat's Theorem and Corollary 6.2 to find the least residue of $a^{f(p)} \pmod{p}$, where p is prime and $f(p)$ is some function of p. Learn to use the available theorems to do this, not calculators. A calculator cannot determine the remainder when a^{162} is divided by 163 when the specific value of a is not given, nor the least residue of $8888^{8888} \pmod{9}$.
- Use the Chinese Remainder Theorem in combination with Fermat's Theorem to find the least residue of $a^{f(m)} \pmod{m}$, where m is composite.
- Use Wilson's Theorem to determine the least residue of $(f(p))! \pmod{p}$ for some function $f(p)$ of the prime number p.
- Determine $d(n)$ and $\sigma(n)$ for a given integer n.
- **Look at the assignment problems and their solutions as well.**
- If it says in an assignment to remember a certain result, then it might just be a good idea to well, uhm ... **remember the result!**