MATH 1020, Review topics for midterm 2

Kiumars Kaveh

November 6, 2018

- The focus of the midterm is on the material covered after midterm 1 until the end of week of November 5.
- The format of midterm 2 is similar to midterm 1.
- No calculators allowed, the questions will be designed so that you do not need one.
- You are responsible to know the homework problems (after midterm 1), some problems in the test will be from homeworks or very similar to them.
- There will be one or two proof problems.
- Definitions: Euler ϕ function, multiplicative function, summatory function, Dirichlet product of two arithmetic functions, Möbius μ function, pseudoprime, Mersenne prime, public key cryptography, order of an element mod n, Möbnius function μ, number of divisors function τ, sum of divisors function σ.
- Skills:
  - Using Fermat/Euler/Wilson's theorems to evaluate/simplify expressions mod n involving large exponents or factorials (Sections 6.1 and 6.3).
  - Computing $\phi(n)$ or number of divisors or sum of divisors of an integer n, using factorization of $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ into product of powers of primes (Sections 7.1, 7.2). For this we use the (non-trivial!) fact that these functions are multiplicative.
  - An application of Möbius inversion formula to some arithmetic functions (Section 7.4, Example 7.17).
  - Encrypting using an affine transformation $aX + b$ mod n, or decrypting such an encryption (Section 8.1, Homeowrk 8, Problems 5, 6).
  - Applying exponentiation encryption for small p (Section 8.3, Example 8.14).
  - Applying RSA algorithm for small number $n = pq$ (Section 8.4, Example 8.16).

  - Applying Diffie-Hellman key exchange algorithm for a small prime p (Section 8.6 only first part).
  - Finding order of an element a mod n.

- Statement of theorems (no proofs):

  - Wilson's theorem (Theorem 6.1).
  - Fermat's little theorem and Euler's theorem (Theorem 6.3, Theorem 6.14).
  - Formula for $\phi(n)$ (Theorem 7.5).
  - Formula for sum and number of divisors of an integer n (Theorem 7.9).
  - Theorem that summatory function of a multiplicative function is also multiplicative (Theorem 7.8).
  - Statement of Möbius inversion formula (Theorem 7.16).

- Proof of theorems:

  - Proof of Fermat's little theorem.
  - Proof of Wilson's theorem.
  - Proof of Euler's theorem: if $(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \mod n$.
  - Proof of $\phi(p^r) = p^r - p^{r-1}$ (Theorem 7.3).
  - Proof of theorem that summatory function of a multiplicative function is also multiplicative (Theorem 7.8).