MATH 1020, Review topics for final exam

Kiumars Kaveh

December 6, 2018

- The focus of the exam is on the material covered in the second half of the course although of course there will be questions from the first half too.
- The format is similar to the midterms.
- No calculators allowed, the questions will be designed so that you do not need one.
- You are responsible to know midterm problems and the homework problems, some problems in the test will be from homeworks or similar to them. It is also useful to try the suggested practice problems from textbook posted in the webpage.
- There will be one or two proof problems.
- Definitions: greatest common divisor, least common multiple, prime number, congruence, (modular) inverse, Euler ϕ function, multiplicative arithmetic function, summatory function, Dirichlet product of two arithmetic functions, Möbius μ function, pseudoprime, Mersenne prime, perfect number, public key cryptography, primitive root, order of an element mod n, discrete logarithm, quadratic residue, Legendre symbol.
- Skills:
  - Calculate greatest common divisors using Euclid's algorithm, and express the gcd of two numbers as a linear combination of the two numbers.
  - Base conversion
  - Solve linear Diophantine equations
  - Calculate inverses mod n
  - Solve linear congruences
  - Calculating the remainder of an expression mod n
  - Proving a statement using induction
  - Solving a system of linear congruences (as in Chinese remainder theorem Section 4.3).

- Using Fermat/Euler/Wilson's theorems to evaluate/simplify expressions mod n involving large exponents or factorials (Sections 6.1 and 6.3)
- O Solving a polynomial equation modulo (small) power of a prime number (as in Section 4.4 and Hensel's lemma)
- Fast modular exponentiation (end of Sec. 4.1)
- Prove that a number is irrational (such as $\sqrt{1+\sqrt{5}}$, see Theorem 3.18)
- 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.
- A simple application of Möbius inversion formula to some arithmetic functions (Section 7.4, Example 7.17).
- Encrypting using an affine transformation $aX+b \bmod n$, or breaking such an encryption (Section 8.1, Homeowrk 8, Problems 5, 6).
- Applying exponentiation encryption for small p (Section 8.3, Example 8.14).
- O 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 $a \bmod n$, and verifying if a is a primitive root (Section 9.1, Examples 9.3, 9.4, 9.6, 9.7. 9.9).
- O Determine whether a given number is a quadratic residue modulo a prime number (equivalently determine a Legendre symbol) using properties of Legendre symbol such as multiplicativity, Euler's criterion or the quadratic reciprocity. Usually the quadratic reciprocity is a more efficient way than Euler's criterion.
- O Given n and a, determine whether an equation $x^2 \equiv a \ (mod\ n)$ has a solution by factoring n into product of powers of primes, using Chinese remainder theorem, Hensel's lemma and quadratic reciprocity.

• Statement/content of theorems (no proofs):

- Prime number theorem (on distribution of primes)
- Dirichlet's theorem on primes in arithmetic progressions
- Fundamental theorem of arithmetic
- Bertrand's principle that there is a prime between n and $2n$.
- 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).
- Chinese remainder theorem (Theorem 4.13).
- 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).
- Existence of primitive roots for primes and powers of primes (Corollary 9.8.1).
- Properties of order of an element mod n (Theorem 9.3, Theorem 9.4, Corollary 9.4.1, Theorem 9.5, Theorem 9.8).
- Properties of quadratic residues and Legendre symbol (Lemma 11.1, Theorem 11.1, Theorem 11.2, Theorem 11.4, Theorem 11.5, Theorem 11.6).
- Statement of Euler's criterion (Theorem 11.3) and Gauss's Lemma (Lemma 11.2)
- Statement of Theorem of Quadratic Reciprocity (Theorem 11.7).

- Proof of theorems:
  - Euclid's proof for existence of infinitely many primes
  - The greatest common divisor (a, b) is a linear combination of a and b (Theorem 3.8 also called Bezout's theorem), and that every common divisor of a, b divides (a, b).
  - Characterization of inverses in terms of gcd, i.e. $ax \equiv 1 \bmod n$ has a solution if and only if $(a, n) = 1$.
  - Proof of Fermat's little theorem.
  - Proof of Wilson's theorem.
  - Proof of Euler's theorem: if $(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \bmod n$.
  - Proof of the fact that for any $0 < a < n$, $\mathrm{ord}_n(a)$ divides $\phi(n)$ (Theorem 9.1 and Corollary 9.1.1).
  - Proof of theorem that summatory function of a multiplicative function is also multiplicative (Theorem 7.8).
  - Proof of Euler's criterion (Theorem 11.3).