MATH 1020, Review topics for midterm 1

Kiumars Kaveh

October 2, 2018

- You are responsible to know the homework problems, some problems in the test will be from homeworks or very similar to them.
- There will be proof problems (like the ones in the homeworks).
- Midterm covers Sections 1.2-1.3, 1.5, 2.1-2.3, 3.1-3.7, 4.1-4.4. More emphasis on Chapters 3 and 4 of course.
- Definitions: divisor, greatest common divisor, least common multiple, prime number, congruence, (modular) inverse, Fermat number, big O notation, Riemann zeta function
- Skills:
  - There will be a question to prove a statement using induction.
  - Be prepared to explain the meaning of polynomial time and give examples of problems that can be solved in polynomial time, and at least one problem for which no polynomial time solution is known (e. g. factorization of an integer into primes).
  - 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, e.g. remainder of 3^{10} mod 5.
  - Fast modular exponentiation (end of Sec. 4.1)
  - Prove that a number is irrational (such as $\sqrt{1+\sqrt{5}}$, see Theorem 3.18)
  - Proving a statement using induction e.g. about Fibonacci numbers (definition of Fibonacci will be given).

  - Solve a system of congruences as in Chinese Remainder Theorem
  - Solve a polynomial equation modulo (small) power of a prime number (as in Sectoin 4.4 ans Hensel's lemma)

- Statement of theorems/conjectures/principles (no proofs required):
  - Well-ordering property (of natural numbers)
  - Division algorithm
  - Prime number theorem (on distribution of primes)
  - Dirichlet's theorem on primes in arithmetic progressions
  - Goldbach's conjecture
  - Fundamental theorem of arithmetic
  - Bertrand's principle that there is a prime between n and $2n$.

- Proof of theorems:
  - Euclid's proof for existence of infinitely many primes
  - $\gcd(a, b)$ is a linear combination of a and b (also called Bezout's theorem), and that every common divisor of a, b divides $\gcd(a, b)$.
  - $a|bc$ and $(a, b) = 1$ implies $a|c$
  - 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 Chinese Remainder Theorem