Information for Midterm 2

November 15, 2019

Work covered: Sections 1 – 15, excluding the section on cryptography and Section 14.

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.

- *order* of $a \pmod m$
- *primitive root* of m
- *quadratic congruence*
- *quadratic residue/nonresidue of* m
- *Legendre symbol* (a/p), where p is an odd prime and $p \nmid a$.
- *Terminating decimal or base* b *expansions*
- *Non-terminating decimal or base* b *expansions*
- *Period* and *length of the non-periodical part* of a non-terminating decimal or base b expansion

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.

- Sections 1 – 8: None
- Section 9: Theorem 9.1
- Section 10: Theorems 10.1, 10.2, 10.5, 10.6, Lemma 10.1
- Section 11: Theorems 11.1, 11.2, 11.5
- Section 12: Theorems 12.2, 12.3
- Section 15: Theorem 15.4

Applications of Theorems

- For integers a and m such that $(a, m) = 1$, determine $\text{ord}_m\, a$.
- Given that a has order $t \pmod m$, use Theorem 10.5 to determine the least residue of $a^{f(t)} \pmod m$, for some given function f of t, or of $f(a) \pmod m$, for some expression $f(a)$ involving a.
- Find a primitive root, if it exists, of a given number. (You must also know which numbers have primitive roots, and how many primitive roots those numbers have – see Theorem 10.7.)
- Given a primitive root g of m, determine all primitive roots of m (where g and m are given specific values).
- Given a primitive root g of the odd prime p, what can you say about $g^{(p-1)/2} \pmod p$?
- Convert a quadratic congruence of the form $ax^2 + bx + c \pmod p$ to one of the form $y^2 \equiv d \pmod p$.
- Use Legendre symbols and the theorems in Section 11 to determine whether a given quadratic congruence $x^2 \equiv a \pmod p$ has a solution. You must know how to manipulate Legendre symbols.
- Solve quadratic congruences.
- Use Theorem 12.3 to show that 2 is a primitive root of a prime of the form $4p + 1$, where p is also prime. Then use Lemma 10.1 or Corollary 10.3 to find the other primitive roots of $4p + 1$.
- Determine the decimal expansion of a rational number r/s.
- Find the period and the length of the non-periodical part of the decimal or base b expansion of a rational number r/s.
- Also look at Assignments 3 – 5.