

MCS 425 Exercise Set #2 — Spring Semester, 2008

This assignment covers Chapter 3, sections 1–5, of the textbook (*Trappe and Washington, 2nd Ed.*). Page and section numbers refer to the textbook. This assignment is due on Friday, Feb 22.

Sec 3.13, exercises 1, 4, 10.

Use Euclid's extended algorithm in exercise 1.

Sec 3.14, exercises 5, 6.

These don't require a computer, though you will probably want to use a calculator. Show your work.

Exercise C Use the Chinese Remainder Theorem to find all solutions of $x^2 \equiv 1 \pmod{63}$.

Exercise D Show how to compute $a^{123} \pmod{m}$ using 11 modular multiplications. Be sure to show where each multiplication is used.

Exercise E Approximately how many primes are there between 10^{300} and 1.0001×10^{300} ?