Homework 5

due on Wednesday, February 25

Read carefully sections 5.1, 5.2 in the book. Solve problems 4, 8, 9, 13, 19a) in Chapter 5 and the following problem.

Problem 1. Let p be an odd prime number and b a primitive root modulo p.

a) Prove that $b^{(p-1)/2} \equiv -1 (\mod p)$. Conclude that $-b \equiv b^{(p+1)/2} (\mod p)$.

b) Show that the congruence $x^2 \equiv b^k (\mod p)$ is solvable if and only if k is even.

Part a) may be useful for problem 13.