Homework 7

due on Wednesday, February 21

Read section 5.1, 5.2 in the book. Solve problems 4, 7, 8, 13, 19a) in Chapter 5. Also solve problem 58 in Chapter 2 and the following problems.

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.

Problem 2. We proved that if $\gcd(m, n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$ by showing that the map $U_{mn} \longrightarrow U_m \times U_n$ sending $a \in U_{mn}$ to the pair $(a(\mod m), a(\mod n))$ is a bijection. Verify "by hand" that this is indeed a bijection when $m = 3$, $n = 7$.