Homework 6

due on Friday, March 6

Read carefully sections 5.1, 5.2, 5.3 in the book. Solve problem 14 in Chapter 5 and the following problems.

Problem 1. Recall that the exponenet of m is the smallest positive integer k such that $a^k \equiv 1 \pmod{m}$ for every integer a relatively prime to m. Let m, n be integers grater than 1 such that $m|n$.

a) Suppose a is an integer relatively prime to m. Prove that there is an integer b relatively prime to n and such that $a \equiv b \pmod{m}$.

b) Let a, b be as in part a). Prove that $\mathrm{ord}_m a | \mathrm{ord}_n b$.

c) Prove that the exponent of m divides the exponent of n.

Problem 2. Let p be an odd prime. Consider the polynomial

$$f(x) = (x-1)(x-2)\dots(x-(p-1)) - x^{p-1} + 1.$$

a) Compute f for $p = 5$ and $p = 7$.

b) What is the degree of f?

c) What can you say about $f(i) \pmod{p}$ for $i = 1, 2, \dots, p-1$?

d) What does c) and Lagrange's Theorem tell you about the coefficients of f?

e) What is $f(0)$? Now using d) you should get a proof of Wilson's Theorem (different than the one we discussed in class).

Problem 3. Let a, b be integers relatimely prime to $m > 1$. Prove that

a)

$$\mathrm{ord}_m(ab) \left| \frac{\mathrm{ord}_m(a)\mathrm{ord}_m(b)}{\gcd(\mathrm{ord}_m(a), \mathrm{ord}_m(b))} \right. .$$

b) $\mathrm{ord}_m(a) | \mathrm{ord}_m(ab) \cdot \mathrm{ord}_m(b)$.

c)

$$\frac{\mathrm{ord}_m(a)}{\gcd(\mathrm{ord}_m(a), \mathrm{ord}_m(b))} \frac{\mathrm{ord}_m(b)}{\gcd(\mathrm{ord}_m(a), \mathrm{ord}_m(b))} \left| \mathrm{ord}_m(ab) \right.$$