Math 40520 Theory of Number
Homework 7

Due Wednesday, 2015-11-11, in class

1. Exercise 2.17 on page 35. [Hint: Mod 3.]

2. (Restatement of first part of Exercise 4.6 on page 74) Show that if p is a prime and $n = 2^p - 1$ then $2^n \equiv 2 \pmod{n}$. (This would be a consequence of Fermat's little theorem if n were a prime and the point of the exercise is to show this always, whether or not n is a prime.) [Hint: Use the fact that, since p is a prime, $2^p \equiv 2 \pmod{p}$.]

3. (Restatement of second part of Exercise 4.6 on page 74) Show that if k is a positive integer and $n = 2^{2^k} + 1$ then $2^n \equiv 2 \pmod{n}$. (This would be a consequence of Fermat's little theorem if n were a prime and the point of the exercise is to show this always, whether or not n is a prime.)

4. Suppose $p > q$ are two primes. Show that

$$q^{pq} \not\equiv q \pmod{pq}$$

5. Show that an integer n is a prime if and only if

$$(X + a)^n \equiv X^n + a \pmod{n}$$

for all integers a. [Hint: If p is the smallest prime factor of n but $p \neq n$ show that n cannot possibly divide $\binom{n}{p}$.]