Math 40520 Theory of Number
Homework 7

Due Wednesday, 2015-11-11, in class

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

   Proof. If $p = 3$ then $p^2 + 2 = 11$ is also a prime. If $p \neq 3$ then $p^2 \equiv 1 \pmod 3$ so $3 \mid p^2 + 2$ and therefore $p^2 + 2 > 3$ is not a prime. $\square$

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, $2^p \equiv 2 \pmod p$.]

   Proof. It suffices to show that $2^{n-1} \equiv 1 \pmod n$. From Fermat's little theorem $2^p \equiv 2 \pmod p$ and so $2^p - 2 = pm$ for some integer m. Thus

   $$2^{n-1} - 1 = 2^{2^p-2} - 1 = 2^{mp} - 1 = (2^p - 1)(2^{p(m-1)} + 2^{p(m-2)} + \cdots + 2^p + 1)$$

   which is clearly divisible by $n = 2^p - 1$ and so $2^{n-1} \equiv 1 \pmod n$. $\square$

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.)

   Proof. Write $n - 1 = 2^{2^k} = 2^{k+1}m$ where $m = 2^{2^k-k-1}$ is an integer as $2^k \geq k + 1$ for every integer $k \geq 1$ (in fact for every real $k \geq 1$). Now

   $$2^{n-1} - 1 = 2^{2^{k+1}m} - 1 = (2^{2^{k+1}} - 1)(2^{2^k(m-1)} + \cdots + 2^{2^k} + 1)$$

   and so $2^{2^{k+1}} - 1 = (2^{2^k} - 1)(2^{2^k} + 1)$ divides $2^{n-1} - 1$ and so $2^{n-1} \equiv 1 \pmod{2^{2^k} + 1}$ as desired. $\square$

4. Suppose $p > q$ are two primes. Show that there exists an integer a such that

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

   Proof. Since $p > q$ then p is odd. If $a^{pq} \equiv a \pmod{pq}$ for all a then in particular the same is true mod p. Thus $a^{pq} \equiv a \pmod p$. As in class take a to be a generator mod p. Then $a^{pq-1} \equiv 1 \pmod p$ implies that the order $p - 1$ of a divides $pq - 1$ so $p - 1 \mid pq - 1$. But $pq - 1 = (p - 1)q + q - 1$ and so we'd need $p - 1 \mid q - 1$ which is impossible as $p - 1 > q - 1$. $\square$

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 $\binom{n}{p}$.]

Proof. In fact we'll show that one single a coprime to n suffices.

If n is a prime then $n \mid \binom{n}{k}$ for all $1 \leq k \leq n-1$ as in class and so $(X+a)^n \equiv X^n + a^n \equiv X^n + a \pmod{n}$ by Fermat's little theorem.

Now suppose that a coprime to n satisfies $(X+a)^n \equiv X^n + a \pmod{n}$ and also suppose that n is not a prime. We seek a contradiction. Expanding the LHS we get that for k between 1 and $n-1$ we need $\binom{n}{k}a^k \equiv 0 \pmod{n}$ and since a is coprime to n we deduce that $n \mid \binom{n}{k}$. If p is the smallest prime divisor of n but $n \neq p$ look at $k = p$. Let k be the exponent of p in n, i.e., $k = v_p(n)$. Then $p^k \mid n \mid \binom{n}{p}$. But

$$\binom{n}{p} = \frac{n(n-1)\cdots(n-(p-1))}{p!}$$

so if $p^k \mid \binom{n}{p}$, as $p \mid p!$, we deduce that $p^{k+1} \mid n(n-1)\cdots(n-(p-1))$. For $1 \leq i \leq p-1$, $p \nmid n-i$ as $p \mid n$ but $p \nmid i$. Thus the only way p^{k+1} can divide $n(n-1)\cdots(n-(p-1))$ is if $p^{k+1} \mid n$ which contradicts the definition of k. $\square$