Math 40520 Theory of Number
Homework 10

Due Friday, 11/30, in class

Do 5 of the following problems.

1. Prove explicitly, using the AKS algorithm, that 31 is a prime. Don't verify all the polynomial congruences, but compute which congruences one needs to check.

2. Compute $\binom{194871}{1610} \mod 385$. [Hint: Use our theorem for binomial coefficients modulo primes (Lucas' theorem) and the Chinese Remainder Theorem.]

3. 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 Mersenne 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, $2^p \equiv 2 \pmod{p}$.]

4. 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 Fermat prime and the point of the exercise is to show this always, whether or not n is a prime.)

5. Suppose $p^m \neq q^n$ are two odd prime powers. Show that there exists an integer a such that

$$a^{p^m q^n} \not\equiv a \pmod{p^m q^n}$$

6. Find integers $a, b > 0$ such that

$$\binom{2401}{400} \equiv a \cdot 7^b \pmod{7^{b+1}}.$$

7. Let p be a prime and $n \geq 1$ an integer written in base p as $n = \overline{n_k n_{k-1} \dots n_1 n_0}_{(p)}$.

   (a) (Optional) Show that

   $$\binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2 = \binom{2n}{n}$$

   [Hint: Compute the coefficient of x^n in $(1+x)^{2n} = (1+x)^n \cdot (1+x)^n$.]

   (b) Writing $i \leq n$ as $i = \overline{i_k \dots i_1 i_0}_{(p)}$ show that

   $$\sum_{i=0}^{n} \binom{n}{i}^2 \equiv \sum_{i_k=0}^{n_k} \cdots \sum_{i_0=0}^{n_0} \binom{n_k}{i_k}^2 \cdots \binom{n_1}{i_1}^2 \binom{n_0}{i_0}^2 \pmod{p}$$

   [Hint: Use the theorem from class and the fact that $\binom{a}{b} = 0$ unless $b \leq a$.]

(c) Use the previous two parts to deduce that

$$\binom{2n}{n} \equiv \binom{2n_k}{n_k}\binom{2n_{k-1}}{n_{k-1}} \cdots \binom{2n_0}{n_0} \pmod{p}$$

(d) (Optional, but immediate) Show that $p \mid \binom{2n}{n}$ if and only if n, written in base p, has a digit $\geq p/2$.

8. Show that

$$\sum_{4|k} \binom{781}{k} \equiv 1 \pmod{5}$$

[Hint: What is a base 5 criterion for divisibility by 4?]