18.781 Problem Set 2

Thursday, February 23.

Collaboration is allowed and encouraged. However, your writeups should be your own, and you must note on the front the names of the students you worked with.

Extensions will only be given for extenuating circumstances.

1. Let p be a prime, and n, k natural numbers. Show that the power of p dividing $\binom{n}{k}$ is the number of carries when adding k to $n-k$ in base p.

2. (a) Let m, n, k be positive integers. Show the identity

$$\binom{m+n}{k} = \sum_{i=0}^{m} \binom{m}{i}\binom{n}{k-i}.$$

   by combinatorial reasoning.

   (b) Now prove this identity by considering the coefficient of x^k in $(1+x)^m(1+x)^n$.

   (c) Show that

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}.$$

   (d) Show that

$$\sum_{k=0}^{2n} (-1)^k \binom{2n}{k}^2 = (-1)^n \binom{2n}{n}.$$

3. Let p be a prime.

   (a) Show the polynomial identity

$$(1+x)^p \equiv 1 + x^p \pmod{p}$$

   and more generally, that

$$(1+x)^{p^k} \equiv 1 + x^{p^k} \pmod{p}.$$

   Note: this means that the difference of the two polynomials has coefficients divisible by p, which is stronger than saying that it holds if you plug in any integer for x. For instance, $x^p \equiv x \pmod{p}$ is false as a polynomial identity, even though it's true for every integer value of x.

   (b) Let $a = a_r p^r + \cdots + a_0$ and $b = b_r p^r + \cdots + b_0$ be the base p expressions of two positive integers. Show that

$$\binom{a}{b} \equiv \binom{a_r}{b_r} \cdot \binom{a_{r-1}}{b_{r-1}} \cdots \binom{a_0}{b_0} \pmod{p}.$$

   Hint: Simplify $(1+x)^a$ modulo p using the previous part, and calculate the coefficient of x^b.

4. Let $n > 1$ be a positive integer. Show that the polynomial identity

$$(x-a)^n \equiv x^n - a \pmod{n}$$

holds for every integer a if and only if n is prime. (For this problem, you may use the result of problem 1.)

5. Show that

$$\frac{n^7}{7} + \frac{n^{11}}{11} + \frac{59n}{77}$$

is an integer, for all integers n.

6. Let p be a prime, and $e \geq 1$. Find all the solutions of $x^2 \equiv 1 \pmod{p^e}$.

7. (a) Show that $\binom{x}{k}$ is a polynomial in x of degree k and with leading coefficient $1/k!$. Now let $p(x)$ be an arbitrary polynomial with complex coeficients and degree at most n. Show that there exist complex numbers $c_0, \ldots, c_n$, such that

$$p(x) = \sum_{k=0}^{n} c_k \binom{x}{k}$$

and that the c_k are uniquely determined.

(b) For any function $f : \mathbb{N} \to \mathbb{C}$ of the natural numbers, we can define another function Δf by $\Delta f(n) = f(n+1) - f(n)$. (Note: Δ is called the difference operator; it's a discrete analogue of the derivative). Show that $\Delta\binom{x}{k} = \binom{x}{k-1}$. Show that if $p(x)$ is as above, then

$$\Delta p(x) = \sum_{k=1}^{n} c_k \binom{x}{k-1}.$$

(c) Show that $p(n)$ is an integer for all integers n if and only if all the c_k are integers. Such polynomials are called *numerical polynomials*.

8. (Bonus problem) Let p be an odd prime. How many p-element subsets of $\{1, 2, \ldots, 2p\}$ have the sum of their elements divisible by p? Generalize to kp instead of $2p$.

18.781 Theory of Numbers
Spring 2012