Math 230 D **Fall 2012**
Homework 6 **Drew Armstrong**

Problem 1. For each integer $n \geq 0$, let $P(n)$ be the statement: "any set of size n has 2^n subsets." Use induction to prove that $P(n)$ is true for all $n \geq 0$. [Hint: Let A be an arbitrary set of size n and let $x \in A$ be some fixed element. Then every subset of A either contains x or does not. How many subsets are there of each type? [Hint: By induction, there are 2^{n-1} subsets of A that do **not** contain x, since these are just the subsets of $A \setminus \{x\}$. Show that there are also 2^{n-1} subsets that **do** contain x.]]

Problem 2.

(a) Let $a, b, c \in \mathbb{Z}$ with $\gcd(a, b) = 1$. If $a|c$ and $b|c$, prove that $ab|c$. [Hint: Use Bézout to write $ax + by = 1$ and multiply both sides by c.]

(b) In class we proved *Fermat's little Theorem*, which says that if $p \in \mathbb{Z}$ is prime and $\gcd(a, p) = 1$ (i.e. if p doesn't divide a), then we have $a^{p-1} = 1 \bmod p$. To apply this to cryptography we need a slightly more general result:

> Given integers $a, p, q \in \mathbb{Z}$ with p and q prime and with $\gcd(a, pq) = 1$ (i.e. with $p \not| a$ and $q \not| a$), we have $a^{(p-1)(q-1)} = 1 \bmod pq$.

Prove this result. [Hint: You may assume Fermat's little Theorem. First prove that q divides $a^{(p-1)(q-1)} - 1$. The same argument works for p. Then use part (a).]

Problem 3. Use the Binomial Theorem to prove the following:

(a) $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$ for all $n \geq 1$.

(b) $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n\binom{n}{n} = 0$ for all $n \geq 1$.

(c) $0\binom{n}{0} + 1\binom{n}{1} + 2\binom{n}{2} + \cdots + n\binom{n}{n} = n2^{n-1}$ for all $n \geq 1$.

[Hint: The proofs are one-liners. What is the derivative $\frac{d}{dx}$ of $(1 + x)^n$?]

Problem 4. Note that we can write

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{(n)_k}{k!},$$

where $(n)_k := n(n-1)\cdots(n-(k-1))$. Why would we do this? Because the expression $(z)_k$ makes sense for any positive integer k and *any complex number* $z \in \mathbb{C}$. Thus we can define $\binom{z}{k} := (z)_k/k!$ for any $k \in \mathbb{N}$ and $z \in \mathbb{C}$. Prove that for all $n, k \in \mathbb{N}$ we have

$$\binom{-n}{k} = (-1)^k\binom{n+k-1}{k}.$$

Problem 5. Let $x, z \in \mathbb{C}$ be complex numbers with $|x| < 1$. Newton's Binomial Theorem says that

$$(1 + x)^z = 1 + \binom{z}{1}x + \binom{z}{2}x^2 + \binom{z}{3}x^3 + \cdots$$

where the right hand side is a convergent infinite series. Use this to obtain an infinite series expansion of $(1 + x)^{-2}$ when $|x| < 1$. [Hint: Apply Problem 4.]