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.]]

Proof. We wish to show that $P(n) = T$ for all $n \geq 0$. First note that $P(0) = T$ because there is only one set of size 0 — the empty set $\emptyset$ — and it has exactly $2^0 = 1$ subset — itself. Now fix an arbitrary $k \geq 0$ and (OPEN MENTAL PARENTHESIS. suppose that $P(k) = T$. In this case we wish to show that $P(k+1) = T$. So let A be an arbitrary set of size $k+1$ and fix some element $x \in A$. Each subset of A either contains x or does not. The subsets of A that do **not** contain x are precisely the subsets of $A \setminus \{x\}$, and since $P(k) = T$ we know there are 2^k of these. On the other hand, for each subset of A that does not contain x there is a unique subset that does — namely, we just add x. Hence there are **also** 2^k of these. We conclude that A has $2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$ subsets, hence $P(k+1) = T$. CLOSE MENTAL PARENTHESIS.) We have shown that $P(0) = T$ and $P(k) \Rightarrow P(k+1)$ for all $k \geq 0$. By induction we conclude that $P(n) = T$ for all $n \geq 0$. □

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 $p \nmid a$ and $q \nmid a$), 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).]

Proof. To prove (a) suppose that $a|c$ and $b|c$ (say $c = ak$ and $c = b\ell$) with a, b coprime. By Bézout, there exist integers $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Multiply both sides by c to get

$$\begin{aligned} ax + by &= 1 \\ (ax + by)c &= c \\ axc + byc &= c \\ axb\ell + byak &= c \\ ab(x\ell + yk) &= c, \end{aligned}$$

hence $ab|c$. To prove (b) consider $a, p, q \in \mathbb{Z}$ with p and q prime and with $\gcd(a, pq) = 1$ (i.e. with $p \nmid a$ and $q \nmid a$). We wish to show that pq divides $a^{(p-1)(q-1)} - 1$. To see this, first note that q does **not** divide a^{p-1} since if it did then q would also divide a (by the Extended Euclid's Lemma HW5.2), contradiction. Hence by Fermat's little Theorem we conclude that q divides $(a^{p-1})^{q-1} - 1 = a^{(p-1)(q-1)} - 1$. Similarly we see that p divides $a^{(p-1)(q-1)} - 1$. Then since p and q are coprime (indeed, they are both prime), part (a) implies that pq divides $a^{(p-1)(q-1)} - 1$, as desired. □

[I agree, it doesn't seem that this should be the foundation of modern cryptography, but it is.]

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 $(1+x)^n$?]

Proof. Recall the Binomial Theorem:

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n. \tag{1}$$

Since this is an equation of *polynomials*, it remains true if we substitute any value for x. Putting $x = 1$ in equation (1) yields

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

and putting $x = -1$ in equation (1) yields

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

We may also differentiate equation (1) by x to get another equation of polynomials:

$$n(1+x)^{n-1} = 0\binom{n}{0} + 1\binom{n}{1} + 2\binom{n}{2}x + \cdots + n\binom{n}{n}x^{n-1}. \tag{2}$$

Then putting $x = 1$ in equation (2) yields

$$n2^{n-1} = 0\binom{n}{0} + 1\binom{n}{1} + 2\binom{n}{2} + \cdots + n\binom{n}{n}.$$

□

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

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

Proof. Let $n, k \in \mathbb{N}$ be positive integers. Then we have

$$\begin{aligned}\binom{-n}{k} = \frac{(-n)_k}{k!} &= \frac{(-n)(-n-1)(-n-2)\cdots(-n-(k-1))}{k!} \\ &= \frac{(-1)^k(n)(n+1)(n+2)\cdots(n+(k-1))}{k!} \\ &= (-1)^k \frac{(n+k-1)(n+k-2)\cdots(n+2)(n+1)(n)}{k!} \\ &= (-1)^k \frac{(n+k-1)_k}{k!} = (-1)^k \binom{n+k-1}{k}.\end{aligned}$$

□

[One could alternatively show that $\binom{-n}{k}$ satisfies the correct recurrence and initial conditions.]

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.]

By Problem 4, we know that

$$\binom{-2}{k} = (-1)^k \binom{2+k-1}{k} = (-1)^k \binom{k+1}{k} = (-1)^k(k+1)$$

for all $k \in \mathbb{N}$. Then for any $x \in \mathbb{C}$ with $|x| < 1$, Newton tells us that

$$\frac{1}{(1+x)^2} = 1 - 2x + 3x^2 - 4x^3 + \cdots = \sum_{k \geq 0} (-1)^k (k+1) x^k,$$

where the infinite series on the right is convergent. We could alternatively get this by differentiating the well-known geometric series

$$\frac{1}{1+x} = 1 - x + x^2 - x^3 + x^4 - \cdots.$$

What do you get if you integrate the geometric series? Answer:

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots.$$

The geometric series is useful.