Math 230 D **Fall 2015**
Homework 6 **Drew Armstrong**

Problem 1. Generalized Binomial Coefficients. Let $C(n,k)$ denote the coefficient of $a^k b^{n-k}$ in the expansion of $(a+b)^n$. We proved in class that

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

for all relevant values of n and k.

(a) It seems that the above formula only makes sense when $n,k \in \mathbb{Z}$ with $0 \leq k \leq n$. However, if we rewrite the formula as

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

where $(n)_k := n(n-1)(n-2)\cdots(n-(k-1))$, then we can define $C(z,k)$ for any integer $k \geq 0$ and for **any number** z **whatsoever**. Use this definition to prove that

$$C(-n,k) = (-1)^k \cdot C(n+k-1,k)$$

for all integers $n,k \in \mathbb{Z}$ with $k \geq 0$.

(b) If z is any number and k is a negative integer then we will define $C(z,k) = 0$. Use induction and the result from part (a) to prove that for all integers $n,k \in \mathbb{Z}$ (even for negative integers) we have

$$C(n,k) = C(n-1,k-1) + C(n-1,k).$$

[Hint: You already know this is true for $n \geq 0$. Use induction to prove it for $n < 0$.]

Proof. For part (a), first note that when $n,k \geq 0$ we have

$$\begin{aligned} C(n,k) &= \frac{n!}{k!(n-k)!} \\ &= \frac{n(n-1)(n-2)\cdots(n-k+1)(n-k)(n-k-1)\cdots 3\cdot 2\cdot 1}{k!(n-k)(n-k-1)\cdots 3\cdot 2\cdot 1} \\ &= \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} \end{aligned}$$

The first expression makes no sense when n is negative, but the final expression **does** make sense. If $n \geq 0$ then using the formula gives

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

For part (b) I apologize that the hint was unhelpful and slightly wrong. Actually, we don't need induction to prove this. We want to show that for all $n, k \in \mathbb{Z}$ we have

$$C(n,k) = C(n-1,k-1) + C(n-1,k).$$

We already know that this statment is true when $n \geq 1$ (we **don't** know it yet when $n = 0$). So we need to show that for all $n \geq 0$ we have

$$C(-n,k) = C(-n-1,k-1) + C(-n-1,k).$$

Next, note that this statment is true when $k \leq 0$. Indeed, if $k < 0$ then both sides are zero by definition and if $k = 0$ then $C(-n-1,-1) = 0$ by definition and we have $C(-n,0) = 1 = C(-n-1,0)$. Next, suppose that $n = 0$ and $k \geq 1$. Then the left hand side is $C(0,k)$ and using the formula from (a) gives

$$\begin{aligned} C(-1,k-1) + C(-1,k) &= (-1)^{k-1}C(1+(k-1)-1,k-1) + (-1)^k C(1+k-1,k) \\ &= (-1)^{k-1}C(k-1,k-1) + (-1)^k C(k,k) \\ &= (-1)^{k-1} + (-1)^k \\ &= 0. \end{aligned}$$

Finally, suppose that $n, k \geq 1$. Then since $n + k - 1 \geq 0$ we know from the usual Pascal Recurrence that

$$C(n+k,k) = C(n+k-1,k-1) + C(n+k-1,k).$$

Combining this with the formula from part (a) gives $C(-n-1,k-1) + C(-n-1,k) =$

$$\begin{aligned} &= C(-(n+1),k-1) + C(-(n+1),k) \\ &= (-1)^{k-1}C((n+1)+(k-1)-1,k-1) + (-1)^k C((n+1)+k-1,k) \\ &= (-1)^{k-1}C(n+k-1,k-1) + (-1)^k C(n+k,k) \\ &= (-1)^{k-1}C(n+k-1,k-1) + (-1)^k [C(n+k-1,k-1) + C(n+k-1,k)] \\ &= [(-1)^{k-1} + (-1)^k]C(n+k-1,k-1) + (-1)^k C(n+k-1,k) \\ &= (0)C(n+k-1,k-1) + (-1)^k C(n+k-1,k) \\ &= (-1)^k C(n+k-1,k) \\ &= C(-n,k). \end{aligned}$$

□

[Remark: What did we just do here? Recall the picture of the extended Pascal Triangle from class:

```
                0       0       0       0       1
            0       0       0       0       1       -3
        0       0       0       0       1       -2      3
    0       0       0       0       1       -1      1       -1
        0       0       0       1       0       0       0
            0       0       1       1       0       0
                0       1       2       1       0
                    1       3       3       1
```

Part (a) proved that the upper triangle is a rotated version of the lower triangle with some negative signs mixed in. Part (b) proved that the whole picture obeys the Pascal Recurrence. And why do we care? Because Isaac Newton proved that the upper part of the picture tells us the power series expansion of $(1+x)^n$ when n is negative and x is small.]

Problem 2. Generalization of Fermat's little Theorem.

(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 $ax + by = 1$ for some $x, y \in \mathbb{Z}$ and multiply both sides by c.]

(b) The RSA cryptosystem is based on the following generalization of Fermat's little Theorem: For all integers $a, p, q \in \mathbb{Z}$ with $p \neq q$ prime and $\gcd(a, pq) = 1$ we have

$$[a^{(p-1)(q-1)}]_{pq} = [1]_{pq}.$$

Prove this. [Hint: The condition $\gcd(a, pq) = 1$ implies that $p \nmid a$ and $q \nmid a$. We want to show that pq divides $a^{(p-1)(q-1)} - 1$. First observe that q does not divide a^{p-1} otherwise Euclid's Lemma implies that $q|a$. Then Fermat's little Theorem implies that q divides $(a^{p-1})^{q-1} - 1 = a^{(p-1)(q-1)} - 1$. A parallel argument shows that p divides $a^{(p-1)(q-1)} - 1$. Now use part (a).]

Proof. For part (a), consider $a, b, c \in \mathbb{Z}$ with $\gcd(a, b) = 1$. By Bézout's Identity there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Now assume that $a|c$ (say $c = ak$) and $b|c$ (say $c = b\ell$). Then multiplying both sides of $ax + by = 1$ by c gives

$$\begin{aligned} ax + by &= 1 \\ c(ax + by) &= c \\ cax + cby &= c \\ (b\ell)ax + (ak)by &= c \\ ab(\ell x + ky) &= c, \end{aligned}$$

as desired.

For part (b), consider $a, p, q \in \mathbb{Z}$ with p, q prime and with $\gcd(a, pq) = 1$ (i.e. $p \nmid a$ and $q \nmid a$). In this case we want to prove that

$$pq \left| \left(a^{(p-1)(q-1)} - 1 \right) \right.$$

First recall that Fermat's little Theorem says that $q|(b^q - b) = b(b^{q-1} - 1)$ for any integer b. If we also know that $\gcd(b, q) = 1$ (i.e. $q \nmid b$) then it follows from Euclid's Lemma that $q|(b^{q-1} - 1)$. Since we know that $q \nmid a$, Euclid's Lemma also implies that $q \nmid a^{p-1}$. Finally, we can take $b = a^{p-1}$ in Fermat's little Theorem to obtain

$$q \left| \left(\left(a^{(p-1)} \right)^{(q-1)} - 1 \right) = \left(a^{(p-1)(q-1)} - 1 \right) \right.$$

A parallel argument gives

$$p \left| \left(a^{(p-1)(q-1)} - 1 \right) \right.$$

and then since $\gcd(p, q) = 1$ the result follows from part (a). □

[Remark: It's sort of amazing that this little theorem of number theory is the foundation of digital security. You use it every day.]

Problem 3. RSA Cryptosystem. You set up an RSA cipher with public key $(23, 55)$ and private key $(7, 55)$. I sent you the following message using the numbers 1-26 for letters of the alphabet, 27 for period, 28 for space, and 29 for exclamation point:

> [25, 17, 1, 49, 11, 39, 7, 51, 20, 2, 7, 23, 15, 1, 2, 49, 14, 49, 13, 7, 1, 8, 20, 21,
> 25, 7, 1, 8, 39, 25, 2, 1, 27, 25, 7, 52, 1, 25, 17, 15, 52, 1, 25, 14, 27, 39, 48, 17,
> 1, 33, 15, 7, 1, 7, 13, 2, 15, 1, 25, 7, 12, 14, 49, 25, 15, 2, 7, 8, 2, 15, 1, 11, 24]

Decrypt the message.

To decrypt the message we raise each number to the power 7 and reduce it mod 55. For example, decrypting the first character gives

$$[25^7]_{55} = [20]_{55}.$$

This translates to "t", which is the 20th letter of the alphabet. Here is the full message:

> [t, h, a, n, k, s, space, f, o, r, space, l, e, a, r, n, i, n, g, space, a, b, o, u, t, space,
> a, b, s, t, r, a, c, t, space, m, a, t, h, e, m, a, t, i, c, s, period, h, a, v, e, space,
> a, space, g, r, e, a, t, space, w, i, n, t, e, r, space, b, r, e, a, k, exclamation]