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 $n < 0$.]

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).]

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.