Math 230 E **Fall 2013**
Exam 3 — Mon Dec 9 **Drew Armstrong**

There are 3 problems, worth 7 points each. This is a closed book test. Anyone caught cheating will receive a score of **zero**.

Problem 1.

(a) Accurately state the Binomial Theorem.

For all integers $n \geq 0$ and all numbers a and b we have

$$(a+b)^n = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!}\, a^k\, b^{n-k}.$$

(b) Use Pascal's Triangle to compute the coefficient of x^5 in $(1+x)^7$.

$$\begin{array}{ccccccccccccccc}
&&&&&&&1&&&&&&& \\
&&&&&&1&&1&&&&&& \\
&&&&&1&&2&&1&&&&& \\
&&&&1&&3&&3&&1&&&& \\
&&&1&&4&&6&&4&&1&&& \\
&&1&&5&&10&&10&&5&&1&& \\
&1&&6&&15&&20&&15&&6&&1& \\
1&&7&&21&&35&&35&&\boxed{21}&&7&&1
\end{array}$$

(c) Use the formula $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ to compute the coefficient of x^5 in $(1+x)^7$.

$$\binom{7}{5} = \frac{7!}{5!2!} = \frac{7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1}{5\cdot 4\cdot 3\cdot 2\cdot 1\cdot 2\cdot 1} = \frac{7\cdot 6}{2} = 21.$$

(d) Use the formula $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ to prove that for all $1 \leq k \leq n-1$ we have

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

Proof. Applying the formula gives

$$\begin{aligned}
\binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{k!(n-k-1)!} + \frac{(n-1)!}{(k-1)!(n-k)!} \\
&= \frac{(n-1)!}{k!(n-k-1)!}\cdot\frac{(n-k)}{(n-k)} + \frac{k}{k}\cdot\frac{(n-1)!}{(k-1)!(n-k)!} \\
&= \frac{(n-k)(n-1)!}{k!(n-k)!} + \frac{k(n-1)!}{k!(n-k)!} \\
&= \frac{(n-k)(n-1)! + k(n-1)!}{k!(n-k)!} \\
&= \frac{[(n-k)+k](n-1)!}{k!(n-k)!}
\end{aligned}$$

$$
\begin{aligned}
&= \frac{n(n-1)!}{k!(n-k)!} \\
&= \frac{n!}{k!(n-k)!} \\
&= \binom{n}{k}.
\end{aligned}
$$

$\square$

Problem 2. Fix a nonzero integer $0 \neq n \in \mathbb{Z}$.

(a) If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$ prove that $a + b \equiv a' + b' \pmod{n}$.

Proof. Let $a, b \in \mathbb{Z}$ and assume that $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$. That is, assume that there exist integers k, ℓ such that $a - a' = nk$ and $b - b' = n\ell$. Then we have

$$
\begin{aligned}
(a + b) - (a' + b') &= (a - a') + (b - b') \\
&= nk + n\ell \\
&= n(k + \ell),
\end{aligned}
$$

and it follows that $a + b \equiv a' + b' \pmod{n}$. $\square$

(b) If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$ prove that $ab \equiv a'b' \pmod{n}$.

Proof. Let $a, b \in \mathbb{Z}$ and assume that $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$. That is, assume that there exist integers k, ℓ such that $a - a' = nk$ and $b - b' = n\ell$. Then we have

$$
\begin{aligned}
ab - a'b' &= ab - ab' + ab' - a'b' \\
&= a(b - b') + (a - a')b' \\
&= ank + n\ell b' \\
&= n(ak + \ell b'),
\end{aligned}
$$

and it follows that $ab \equiv a'b' \pmod{n}$. $\square$

(c) Accurately state the Principle of Induction.

Let $P(n)$ be a logical statement depending on an integer n. If
- $P(b) = T$, and
- For all integers $k \geq b$ we have $P(k) \Rightarrow P(k+1)$,

then it follows that $P(n) = T$ for all $n \geq b$.

(d) Suppose that $a \equiv b \pmod{n}$ and for all $k \geq 0$ let $P(k)$ be the statement that "$a^k \equiv b^k \pmod{n}$". Use induction to prove that $P(k) = T$ for all $k \geq 0$. [Hint: You will need to quote the result of part (b).]

Proof. First note that the statement $P(0) =$ "$a^0 \equiv b^0 \pmod{n}$" is obviously true. Now fix some integer $k \geq 0$ and assume for induction that $P(k)$ is true. In this case we will show that $P(k+1)$ is also true. Indeed, since $a \equiv b \pmod{n}$ (by assumption) and $a^k \equiv b^k \pmod{n}$ (by $P(k)$), we conclude from part (b) that

$$\begin{aligned} a \cdot a^k &\equiv b \cdot b^k \pmod{n} \\ a^{k+1} &\equiv b^{k+1} \pmod{n}. \end{aligned}$$

By the Principle of Induction we conclude that $P(n)$ is true for all $n \geq 0$. □

Problem 3.

(a) If $a|c$ and $b|c$ with $\gcd(a,b) = 1$, prove that $ab|c$. [Hint: Bézout.]

Proof. Let $a|c$ and $b|c$ so that $c = ak$ and $c = b\ell$ for some $k, \ell \in \mathbb{Z}$. Since $\gcd(a,b) = 1$, Bézout's Identity says that there exist $x, y \in \mathbb{Z}$ with $ax + by = 1$. Then multiplying both sides of this equation by c gives

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

and hence $ab|c$ as desired. □

(b) Accurately state Fermat's little Theorem.

Let $b, p \in \mathbb{Z}$ with p prime and $p \nmid b$. Then we have $b^{p-1} \equiv 1 \pmod{p}$.

(c) Suppose that $a, p, q \in \mathbb{Z}$ with p prime. If $p \nmid a$ show that $a^{(p-1)(q-1)} \equiv 1 \pmod{p}$. [Hint: Use Fermat's little Theorem and Problem 2(d).]

Proof. Since $p \nmid a$, Euclid's Lemma implies that $p \nmid a^{q-1}$. Then by Fermat's little Theorem (with $b = a^{q-1}$) we have

$$a^{(p-1)(q-1)} = \left(a^{q-1}\right)^{p-1} \equiv 1 \pmod{p}$$

□

[Remark: I wrote this problem in 2013 and I wrote the solution in 2015. I have no idea why Problem 2(d) is necessary for this proof.]

(d) Now suppose that $a, p, q \in \mathbb{Z}$ with p and q both prime. If $p \nmid a$ and $q \nmid a$, use parts (a) and (c) to prove that

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

Proof. Since $p \nmid a$, part (b) shows that $p \,\big|\, \left(a^{(p-1)(q-1)} - 1\right)$ and since $q \nmid a$ the same argument shows that $q \,\big|\, \left(a^{(p-1)(q-1)} - 1\right)$. Then since $\gcd(p,q) = 1$, part (a) implies that

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

as desired. □