Math 230 E | **Fall 2013**
Homework 6 | **Drew Armstrong**

Problem 1 (Binomial Theorem). We proved in class that for all $n \geq 0$ we have

$$(1+x)^n = \sum_{k=0}^{n} \frac{n!}{k!\,(n-k)!}\, x^k.$$

Use this to prove that for all integers $a, b \in \mathbb{Z}$ we have

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

[Hint: Show directly that the result holds when $a = 0$. When $a \neq 0$, substitute $x = \frac{b}{a}$ then then multiply both sides by a^n.]

Problem 2 (Freshman's Dream). Formally write up the proof of the "Freshman's Dream". That is, for all $a, b, p \in \mathbb{Z}$ with p prime, prove that

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

[Hint: Use the Binomial Theorem and show that for all $0 < k < p$ we have $p | \frac{p!}{k!(p-k)!}$ because p divides the numerator but p does not divide the denominator. You will need Euclid's Lemma.]

Problem 3 (Fermat's little Theorem). Formally write up Euclid's 1736 proof of "Fermat's little Theorem". That is, for all $a, p \in \mathbb{Z}$ with p prime, prove that

$$a^p \equiv a \pmod{p}.$$

[Hint: Let p be prime and let $P(n)$ be the statement that "$n^p \equiv n \pmod{p}$". Use induction to prove that $P(n) = T$ for all $n \geq 0$. The induction step will use the Freshman's Dream.]

Problem 4 (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 $ax + by = 1$ and multiply both sides by c.]

(b) Fermat's little Theorem can be stated as follows: for all $a, p \in \mathbb{Z}$ with p prime and $\gcd(a, p) = 1$ we have $a^{p-1} \equiv 1 \pmod{p}$. To apply this to cryptography we need a slightly more general result: For all $a, p, q \in \mathbb{Z}$ with p and q prime and $\gcd(a, pq) = 1$, we have

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

Prove this. [Hint: The condition $\gcd(a, pq) = 1$ implies $p \nmid a$ 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} since otherwise Euclid's Lemma implies that q divides a. Then Fermat's little Theorem says that q divides $(a^{p-1})^{q-1} - 1 = a^{(p-1)(q-1)} - 1$, and similarly p divides $a^{(p-1)(q-1)} - 1$. Now use part (a).]