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.]

Proof. To save space I will write $\binom{n}{k}$ instead of $\frac{n!}{k!(n-k)!}$. First suppose that $a = 0$. Then we have

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

If you want to say that $0^0 = 1$ then this is true. If you don't want to say that $0^0 = 1$; fine. Now suppose that $a \neq 0$. Then we can substitute $x = \frac{b}{a}$ into the first equation to get

$$\begin{aligned}
\left(1 + \frac{b}{a}\right)^n &= \sum_{k=0}^{n} \binom{n}{k} \left(\frac{b}{a}\right)^k \\
\left(\frac{a+b}{a}\right)^n &= \sum_{k=0}^{n} \binom{n}{k} \left(\frac{b}{a}\right)^k \\
\frac{(a+b)^n}{a^n} &= \sum_{k=0}^{n} \binom{n}{k} \frac{b^k}{a^k} \\
a^n \frac{(a+b)^n}{a^n} &= a^n \sum_{k=0}^{n} \binom{n}{k} \frac{b^k}{a^k} \\
(a+b)^n &= \sum_{k=0}^{n} \binom{n}{k} \frac{a^n b^k}{a^k} \\
(a+b)^n &= \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.
\end{aligned}$$

□

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 $p \mid \frac{p!}{k!(p-k)!}$ because p divides the numerator but p does not divide the denominator. You will need Euclid's Lemma.]

Proof. Let $a, b, p \in \mathbb{Z}$ with p prime. The binomial theorem says that

$$(a+b)^p = a^p + \binom{p}{1} ab^{p-1} + \binom{p}{2} a^2 b^{p-2} + \cdots + \binom{p}{p-1} ab^{p-1} + b^p.$$

We will be done if we can show that each of the terms on the right side except a^p and b^p is divisible by p (and hence $\equiv 0 \bmod p$). In fact we will show that p divides $\binom{p}{k}$ for all $1 \leq k \leq p-1$. Recall that we proved

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!}.$$

The expression on the right does not look like an integer, but it is an integer because $\binom{p}{k}$ is an integer. This means that if we factor the numerator $p!$ and denominator $k!(p-k)!$ into primes, each of the primes in the denominator will cancel with some prime in the numerator. Note that p divides $p!$, so p occurs in the prime factorization of the numerator. We will be done if we can show that p does **not** occur in the prime factorization of the denominator. Suppose for contradiction that we have

$$p | k(k-1)(k-2)\cdots 3 \cdot 2 \cdot 1 \cdot (p-k)(p-k-1)\cdots 3 \cdot 2 \cdot 1.$$

Since p is prime Euclid's Lemma then implies that p must divide one of the factors on the right. But since $1 \leq k \leq p-1$ each of these factors is smaller than p. Contradiction. We conclude that after cancellation, a p remains in the prime factorization of $\binom{p}{k}$. □

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.]

Proof. Given an integer $n \geq 0$ consider the statement $P(n) =$ "$n^p \equiv n \pmod{n}$". We want to show that $P(n) = T$ for all $n \geq 0$. First we observe that the base case $P(0)$ is true because $0^p = 0$, so clearly $0^p \equiv 0 \pmod{p}$. Now fix an arbitrary $k \geq 0$ and **assume for induction** that $P(k) = T$. That is, assume that $k^p \equiv k \pmod{p}$. In this case we want to show that $P(k+1)$ is true. Using the Freshman's Dream, we have

$$(k+1)^p \equiv k^p + 1^p \equiv k+1 \pmod{p}.$$

[In the last equation we used the fact that $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$ imply $a+b \equiv a'+b' \pmod{n}$, which you proved on a previous homework. In our case we used that $k^p \equiv k \pmod{p}$ and $1^p \equiv 1 \pmod{p}$ imply $k^p + 1^p \equiv k+1 \pmod{p}$.] By induction we conclude that $P(n) = T$ for all $n \geq 0$.

The question also mentions that $a^p \equiv a \pmod{p}$ for negative integers a. How can we show this? First note that if a is negative then we always have $a \equiv n \pmod{p}$ for some positive n. Then we have

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

[Here we used the fact that $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{p}$ imply $ab \equiv a'b' \pmod{n}$, which you also proved on a previous homework.] □

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 $p \not| a$ and $q \not| a$. 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).]

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

$$\begin{aligned} ax + by &= 1 \\ acx + bcy &= c \\ ab\ell x + baky &= c \\ ab(\ell x + ky) &= c. \end{aligned}$$

We conclude that $ab|c$.

For part (b) consider $a, p, q \in \mathbb{Z}$ with p, q prime and $\gcd(a, pq) = 1$. This implies that $p \not| a$ since otherwise p would be a common divisor of a and pq. Similarly we have $q \not| a$. Now we want to show that

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

First note that $q \not| a^{p-1}$. If it did then we would have

$$q | aaa \cdots a.$$

Then since q is prime, Euclid's Lemma says that q must divide one of the factors on the right, i.e. we must have $q|a$. Contradiction. Now since $q \not| a^{p-1}$ and q is prime, Fermat's little Theorem says that

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

In other words, q divides $(a^{p-1})^{q-1} - 1 = a^{(p-1)(q-1)} - 1$. Using exactly the same argument we can show that p divides $a^{(p-1)(q-1)} - 1$. Then since p and q both divide $a^{(p-1)(q-1)} - 1$ and since $\gcd(p, q) = 1$, part (a) says that

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

In other words, $a^{(p-1)(q-1)} \equiv 1 \pmod{p}$. $\square$