Math 7h	Professor: Padraic Bartlett

Homework 8: Cryptography (Modern) + Groups

Due 11/12/13, at the start of class — *UCSB 2013*

Instructions: Do problems here until you have spent about 90 minutes working seriously on these questions. Have fun!

Homework Problems

1. If you haven't before: prove the binomial theorem! I.e. show that for any positive integer n, and any x, y, we have

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i.$$

2. Here's a second, very pretty proof of Fermat's Little Theorem. Fill in the gaps!

Theorem 1. *Let p be a prime number. Take any $a \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$. Then*

$$a^{p-1} \equiv 1 \mod p.$$

Proof. Suppose you have an alphabet with a letters in it. How many strings of length p can you create?

The answer here is clearly a^p: we have p places to put a letter, and a choices for each letter; therefore, we have $\overbrace{a \cdot a \cdot \ldots \cdot a}^{p \text{ times}} = a^p$ many such strings.

Given any two strings, we say that they are **similar** if we can circularly shift the entries in one string to get the other string. For example, the following four strings are all similar:

$$1121, 1112, 2111, 1211.$$

Stack strings together into piles, where all of the strings in each pile are similar. Show that the following two statements are true:

- There are precisely a strings that consist of the same symbol repeated p times; these correspond to a distinct piles each with one string in them.
- In every other pile, there are precisely p strings. In other words, if you're a string that's not just the same symbol repeated p times, then there are exactly $p-1$ other strings that are similar to you.

Conclude from these two statements that $a^p \equiv a \mod p$, and therefore that $a^{p-1} \equiv 1 \mod p$.

Explicitly perform this grouping operation for $a = 2, p = 5$. (If you're stuck on this proof, start here first!) □

3. A **group** is the following object: a set G along with an operation $\cdot$ that satisfies the following four properties:

- **Associativity**: For all a, b and c in G, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- **Identity element**: There exists an element e in G such that for all a in G, $e \cdot a = a \cdot e = a$.
- **Inverse element**: For each a in G, there is an element b in G such that $a \cdot b = b \cdot a = e$, where e is an identity element.

(a) Show that $\mathbb{Z}/n\mathbb{Z}$ is a group, if we let the group operation be defined as addition mod n.

(b) Show that $\mathbb{Z}/n\mathbb{Z}$ is **not** a group, if we let the group operation be defined as multiplication mod n.

(c) Let $(\mathbb{Z}/n\mathbb{Z})^\times$ denote the set of numbers $\{1, \ldots n-1\}$. Show that this is a group precisely whenever n is a prime number, if we let the group operation be defined as multiplication mod n.

4. Let G be a group with group operation $\cdot$ and identity element e. For any a in this group, let a^k denote the object $\overbrace{a \cdot a \cdot \ldots \cdot a}^{k \text{ times}}$. Let n be the number of elements in this group. Prove that

$$a^n = e.$$

5. (a) Give me three groups that are not equal to $\langle \mathbb{Z}/n\mathbb{Z}, + \rangle$ or $\langle (\mathbb{Z}/n\mathbb{Z})^\times, \cdot \rangle$. For each, explain why they are groups.

   (b) Give me a group not in the above collection, containing only finitely many elements, that is not $\langle \mathbb{Z}/n\mathbb{Z}, + \rangle$ or $\langle (\mathbb{Z}/n\mathbb{Z})^\times, \cdot \rangle$.