Midterm 2 Review

Due: April 6/7, 2016

All homeworks are due at 12:55 PM in the CS22 bin on the CIT second floor, next to the Fishbowl.

Include our cover sheet or equivalent, write your Banner ID (but not your name or your CS login) on each page of your homework, label all work with the problem number, and staple the entire handin before submitting.

Be sure to fully explain your reasoning and show all work for full credit. Consult the style guide for more information.

Problem 1

Suppose \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \).

Show that

a. \( ac \equiv bd \pmod{m} \)

b. \( a^n \equiv b^n \pmod{m} \) for any non-negative integer \( n \)

Problem 2

Let \( k \) be an integer and let \( R_k \) be the set of equivalence classes mod \( k \). For example \( R_k = 0, 1, 2, 3, 4 \). We say that \( a \in R_k \) is nilpotent if there is some \( n \geq 1 \) such that \( a^n \equiv 0 \pmod{9} \).

a. Suppose \( a, b \in R_k \) are nilpotent. Show that \( ab \) is nilpotent.

b. Suppose \( a, b \in R_k \) are nilpotent. Show that \( a + b \) is nilpotent.

c. Let \( l \geq 1 \) and \( p \) be a prime. Let \( a \) be an arbitrary integer. Show that either \( a \) has an inverse mod \( p^l \) or there exists an \( n \) such that \( a^n = 0 \pmod{p^l} \).

Problem 3

Use induction to prove the following generalization of one of De Morgan’s laws:

\[ \neg(p_1 \land p_2 \land p_3 \land \ldots \land p_n) = \neg p_1 \lor \neg p_2 \lor \ldots \lor \neg p_n \]

for \( n \in \mathbb{Z}^+, n \geq 2 \).
Problem 4

In this problem, you will sketch another proof of Fermat’s Little Theorem using the Binomial Theorem and modular arithmetic.

As a reminder, Fermat’s Little Theorem states that for any integer $a$ relative to a prime number $p$,

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

and the Binomial Theorem states that, for any integers $a$, $b$, and $n$:

$$(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$

a. Prove that, for any prime number $p$ and any integer $0 < i < p$,

$p$ divides $\binom{p}{i}$.

b. Prove that, for integers $a$ and $b$ and a prime number $p$, $(a + b)^p \equiv a^p + b^p \pmod{p}$.

c. Complete this proof with an induction on $a$, substituting 1 for $b$.

Problem 5

Prove that for all $n \in \mathbb{Z}^+$,

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2$$

Problem 6

Dwight, eager for revenge in the office’s ongoing prank war, desperately needs to get into Jim’s computer. Jim’s computer, however, is password-protected! Dwight has as many guesses as he needs, and he won’t stop until he obtains access to all of Jim’s files. Fortunately, Jim is a little predictable, and Dwight is certain that his password is an anagram of “JELLOSTAPLER”.

a. If Dwight knows nothing else about the password, how many possibilities must she try to guarantee that she guesses the password correctly? Your answer can be left as an expression containing factorials.

b. Dwight knows that Jim is a simple fellow who only knows simple words. How many possible passwords contain the word “SPOT” in them?
c. Dwight guesses all of the anagrams of “JELLOSTAPLER”, but he’s still locked out of Jim’s computer! After awkwardly questioning Pam, Dwight discovers that Jim’s password is actually three words, separated by spaces. Each word in the password must consist of at least 1 character, and the non-space characters still form an anagram of “JELLOSTAPLER”. How many possible passwords are there for Dwight to try now?