

Homework 5, Number Systems

Due Friday October 31st, 2008

The goal of this homework is to prove Fermat's Little Theorem (which is in the book as **Theorem 6.11**). Some things that might be useful are the following:

Definition: Let $p \in \mathbb{N}$. p is a *prime number* if the only integers which divide p are p , $-p$, 1 , and -1 .

Theorem 5.13 (Binomial theorem for integers): If $a, b \in \mathbb{Z}$, and $n \in \mathbb{Z}_{\geq 0}$, then

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

Remember that $\binom{n}{k}$ is defined to be the integer which satisfies the following equation

$$n! = \binom{n}{k} k!(n-k)!$$

You can reference anything we did in class. However, if you use something we didn't do in class, then you need to justify it.

1. Let $m, n \in \mathbb{N}$. Define a set S by

$$S = \{x \in \mathbb{N} \mid \text{There exist two integers } s, t \in \mathbb{Z} \text{ so that } x = ms + nt\}.$$

Note that S is a subset of \mathbb{N} .

- (a) Prove that S is not empty. That means that by the Well Ordering Principle (**Theorem 7.1**) S has a least element.
- (b) Let d be the least element of S . Prove that d divides m and d divides n .

[Hint: Use the Division Algorithm (**Theorem 6.5**) to write $m = dq + r$ where $0 \leq r < d$, and show that $r = 0$. That will show d divides m .]

- (c) Prove that for any $c \in \mathbb{Z}$, if c divides m and c divides n , then c divides d .
- (d) Use part (c) to show that d is the greatest common divisor of m and n . In other words, prove the following: If $c \in \mathbb{Z}$ and c divides m and c divides n , then $c \leq d$.

2. Let $m, n \in \mathbb{N}$ and $p \in \mathbb{N}$ where p is a prime number. Prove the following: If p divides mn , then either p divides m or p divides n .

[Hint: Use Problem 1. Let d be the greatest common divisor of m and p . Then by Problem 1, you have $d = ms + pt$ for some $s, t \in \mathbb{Z}$. Also since d divides p , there aren't that many possibilities for d .]

3. Let $a_1, a_2, \dots, a_n \in \mathbb{N}$ and $p \in \mathbb{N}$ where p is a prime number. Prove the following: If p divides $a_1 a_2 a_3 \cdots a_n$, then p divides a_i for some $1 \leq i \leq n$.

[Hint: Use Problem 2 and induction on n .]

4. Use Problem 3 to prove the following: Let $m, p \in \mathbb{N}$ where p is a prime number and $0 < m < p$. Then $\binom{p}{m}$ is divisible by p .
5. Prove Fermat's Little Theorem. That is prove the following: Let $m \in \mathbb{Z}$ and $p \in \mathbb{N}$ where p is a prime number. Then

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

[Hint: Prove the theorem for $m \geq 0$ by induction on m and using **Theorem 5.13** from above. Then say how this helps you prove the theorem for $m < 0$.]