Math 40520 Theory of Number
Homework 4

Due Wednesday, 2015-09-30, in class

Do 5 of the following 8 problems. Please only attempt 5 because I will only grade 5.

1. (This is not a hard exercise, even if it looks very long.) In this exercise you will multiply two positive integers using only doubling, halving and additions. Suppose m and n are two positive integers. Put m and n on the same row in a table with two columns. You will iterate the following operation. Taking the last row of the column, multiply by 2 the left entry and divide by 2 the right entry and put the new values on the next row, forgetting about decimals. When the right row becomes 0, stop the iteration. Eliminate from the column every row in which the right entry is even, then add all the remaining left entries. This sum will then be the product $m \cdot n$. For example

$x \times 2$	$\lfloor x/2 \rfloor$
23	25
~~46~~	~~12~~
~~92~~	~~6~~
184	3
368	1
~~736~~	~~0~~

yield $23 \cdot 25 = 575 = 368 + 184 + 23$.

   (a) Write $m = \overline{m_1 m_2 \cdots m_k}_{(2)}$ and $n = \overline{n_1 n_2 \ldots n_k}_{(2)}$ in base 2. Show that the table, all entries written in base 2, is

$x \times 2$	$\lfloor x/2 \rfloor$
$\overline{m_1 m_2 \cdots m_k}$	$\overline{n_1 n_2 \ldots n_k}$
$\overline{m_1 m_2 \cdots m_k 0}$	$\overline{n_1 n_2 \ldots n_{k-1}}$
$\overline{m_1 m_2 \cdots m_k 00}$	$\overline{n_1 n_2 \ldots n_{k-2}}$
$\vdots$	$\vdots$
$\overline{m_1 m_2 \cdots m_k \underbrace{00\ldots0}_{k-1}}$	$\overline{n_1}$
$\overline{m_1 m_2 \cdots m_k \underbrace{00\ldots0}_{k}}$	0

   (b) Show that the algorithm is correct. [Hint: Write out multiplication in base 2.]

2. Let p be a prime and $n \geq 1$ an integer written in base p as $n = \overline{n_k n_{k-1} \ldots n_1 n_0}_{(p)}$.

   (a) (Optional) Show that

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2 = \binom{2n}{n}$$

   [Hint: Compute the coefficient of x^n in $(1+x)^{2n} = (1+x)^n \cdot (1+x)^n$.]

(b) Writing $i \leq n$ as $i = \overline{i_k \dots i_1 i_0}_{(p)}$ show that

$$\sum_{i=0}^{n} \binom{n}{i}^2 \equiv \sum_{i_k=0}^{n_k} \cdots \sum_{i_0=0}^{n_0} \binom{n_k}{i_k}^2 \cdots \binom{n_1}{i_1}^2 \binom{n_0}{i_0}^2 \pmod{p}$$

[Hint: Use the theorem from class and the fact that $\binom{a}{b} = 0$ unless $b \leq a$.]

(c) Use the previous two parts to deduce that

$$\binom{2n}{n} \equiv \binom{2n_k}{n_k}\binom{2n_{k-1}}{n_{k-1}} \cdots \binom{2n_0}{n_0} \pmod{p}$$

(d) (Optional, but immediate) Show that $p \mid \binom{2n}{n}$ if and only if n, written in base p, has a digit $\geq p/2$.

3. Exercise 4.15 on page 81.

4. Exercise 4.16 on page 81.

5. Exercise 6.17 on page 113. (You have two means of solving this: either primitive roots, or Hensel's lemma.)

6. Let $p > 3$ be a prime number. Find a solution in $\mathbb{Z}_{p^6}$ to the equation

$$x^3 \equiv 1 + p^2 \pmod{p^6}$$

7. Let m and n be two positive integers.

(a) If $m = nq + r$ is division with remainder show that as polynomials $X^m - 1 = (X^n - 1)Q(X) + X^r - 1$ is division with remainder.

(b) Deduce that as polynomials $(X^m - 1, X^n - 1) = X^{(m,n)} - 1$.

8. Show that

$$\sum_{4|k} \binom{781}{k} \equiv 1 \pmod{5}$$

[Hint: What is a base 5 criterion for divisibility by 4?] (This is a special case of a general result of Hermite.)