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.]

Proof. (a): In base 2 multiplication by 2 is adding a 0 whereas dividing by 2 means shifting the decimal point one place to the left. Forgetting about decimals this means dropping the last digit.

(b): Summing up the left entries where the right entries are odd means, using part (a), that

$$S = \sum_{0 \le i \le k, n_i = 1} \overline{m_1 \ldots m_k \underbrace{00\ldots0}_{i}}$$

which can be rewritten as

$$
\begin{aligned}
S &= \sum_{i=0}^{k} \overline{m_1 \dots m_k \underbrace{00\dots0}_{i}} \cdot n_i \\
&= \sum_{i=0}^{k} m \cdot n_i 2^i \\
&= m \sum_{i=0}^{k} n_i 2^i \\
&= m \cdot n
\end{aligned}
$$

$\square$

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

   (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 $\geq p/2$.

Proof. (a): $\binom{2n}{n}$ is the coefficient of x^n in $(1+x)^{2n} = (1+x)^n \cdot (1+x)^n$. Expanding we seek the coefficient of x^n in

$$\sum_{i=0}^{n} \binom{n}{i} x^i \sum_{j=0}^{n} \binom{n}{j} x^j = \sum_{0 \leq i,j \leq n} \binom{n}{i}\binom{n}{j} x^{i+j}$$

thus the coefficient is

$$
\begin{aligned}
\binom{2n}{n} &= \sum_{i+j=n} \binom{n}{i}\binom{n}{j} \\
&= \sum_{i=0}^{n} \binom{n}{i}\binom{n}{n-i} \\
&= \sum_{i=0}^{n} \binom{n}{i}^2
\end{aligned}
$$

as $\binom{n}{n-i} = \binom{n}{i}$.

(b): We know that

$$\binom{n}{i} \equiv \binom{n_k}{i_k} \cdots \binom{n_0}{i_0} \pmod{p}$$

and this is zero whenever $i_j > n_j$ for some j. Thus

$$\begin{aligned}
\sum_{i=0}^{n} \binom{n}{i}^2 &\equiv \sum_{\overline{i_k \ldots i_0} \leq \overline{n_k \ldots n_0}} \binom{n_k}{i_k}^2 \cdots \binom{n_1}{i_1}^2 \binom{n_0}{i_0}^2 \pmod{p} \\
&\equiv \sum_{\overline{i_k \ldots i_0} \leq \overline{n_k \ldots n_0}, i_0 \leq n_0, \ldots, i_k \leq n_k} \binom{n_k}{i_k}^2 \cdots \binom{n_1}{i_1}^2 \binom{n_0}{i_0}^2 \pmod{p}
\end{aligned}$$

If $i_k \leq n_k, \ldots, i_0 \leq n_0$ then automatically $\overline{i_k \ldots i_0} \leq \overline{n_k \ldots n_0}$ so part (b) follows.

(c): We factor the RHS of part (b) to get

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

where the last line follows from part (a).

(d): From part (c) we have $\binom{2n}{n} \equiv 0 \pmod{p}$ iff $\binom{2n_j}{n_j} \equiv 0 \pmod{p}$ for some digit n_j. If $n_j < p/2$ then $2n_j < p$ and so in the expression $\binom{2n_j}{n_j} = \dfrac{(2n_j)!}{(n_j!)^2}$ the factor p does not appear at all in the numerator so it cannot be divisible by p. If $n_j \geq p/2$ then $2(p-1) \geq 2n_j \geq p$ so the base p expansion of $2n_j$ is $2n_j = \overline{1a}_{(p)}$ where $a = 2n_j - p$. Then $\binom{2n_j}{n_j} \equiv \binom{1}{0}\binom{a}{n_j} \pmod{p}$. But $a = 2n_j - p < n_j$ and so $\binom{a}{n_j} = 0$. ☐

3. Exercise 4.15 on page 81.

Proof. First note that any solution mod 5^2 yields a solution mod 5. So we first solve $x^3+4x^2+9x+1 \equiv 0 \pmod{5}$. But $x^3 + 4x^2 + 9x + 1 \equiv x^3 - x^2 - x + 1 \equiv (x^2 - 1)(x - 1) = (x - 1)^2(x + 1) \pmod{5}$ so the two solutions are $x = \pm 1$. To solve the equation modulo 5^2 we apply Hensel's lemma to each of the two solutions modulo 5.

Starting with $x_1 = -1$, $P(-1) = -15$ and $P'(-1) \equiv -1 \pmod{5}$ with inverse -1 mod 5. Thus Hensel implies that $x_2 = x_1 - P(x_1) \cdot (-1) = -1 - (-15) \cdot (-1) = -16$ is the only solution of $P(X) \equiv 0 \pmod{5^2}$ with $X \equiv -1 \pmod{5}$.

Next, we start with $x_1 = 1$, $P(1) = 25$ and $P'(1) \equiv 0 \pmod{5}$. Applying Hensel's lemma again we note that $5 \mid P(1)/5$ and so there are exactly 5 solutions to $P(X) \equiv 0 \pmod{5^2}$ with $X \equiv 1 \pmod{5}$. Thus we seek solutions to the equation $Q(y) = P(1 + 5y) \equiv \pmod{5^2}$. We know that there are 5 such solutions but in $\mathbb{Z}_{5^2}$ there are exactly 5 elements of the form $1 + 5y$ and so $1, 6, 11, 16, 21$ are all solutions to $P(X) \equiv 0 \pmod{5^2}$ with $X \equiv 1 \pmod{5}$.

Thus the solutions are $1, 6, 11, 16, 21, -16 \equiv 9 \pmod{25}$. ☐

4. Exercise 4.16 on page 81.

Proof. Case $e = 1$. We solve $x^3 - x - 1 \equiv 0 \pmod 5$ and note by brute force that only $x = 2$ is a solution mod 5.

Case $e = 2$. Any solution is a lift of $x = 2 \pmod 5$. Note that $P(2) = 5$ and $P'(2) = 11$ with inverse 1 mod 5. Thus Hensel implies that $x_2 = 2 - 5 \cdot 1 = -3$ is the only solution mod 25.

Case $e = 3$. We lift again using Hensel's lemma. The only solution mod 125 is $x_3 = -3 - P(-3) = -3 + 25 = 22$.

□

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

Proof. **First solution:** Recall that $\mathbb{Z}_{32}^\times = \{\pm 1, \pm 3, \pm 3^2, \pm 3^3, \ldots, \pm 3^7\}$ as $32 = 2^5$. Note that the order of 7 must be a power of 2 so we check: $7^2 = 49 \equiv 17 \pmod{32}$ and $7^4 \equiv 17^2 \equiv 1 \pmod{32}$ so 7 has order 4. From the previous homework we know that there are 4 elements of order 4 in $\mathbb{Z}_{32}^\times$. Since 3 has order 8 these four elements are of the form $\pm 3^{2r}$ where r is odd and so they are $\pm 3^2 \equiv \pm 9$ and $\pm 3^6 = \pm 7$. Checking we get that $7 = -3^6 \pmod{32}$. Finally, we need to solve $x^{11} =\equiv 7 \equiv -3^6 \pmod{32}$ and we know that $x = \pm 3^r$. Thus we need $\pm 3^{11r} \equiv -3^6 \pmod{11}$.

Immediately the sign must be $-$ and so we need $3^{11r} \equiv 3^6 \pmod{32}$. As 3 has order 8 this is equivalent to $11r \equiv 6 \pmod 8$. 11 is invertible mod 8 and has inverse 3 so this is equivalent to $r \equiv 3 \cdot 6 \equiv 18 \equiv 2 \pmod 8$. As $0 \leq r \leq 7$ this implies that $r = 2$. Thus the equation has exactly one solution, namely $x = -3^2 = -9$.

Second solution: Clearly $(-1)^{11} \equiv 1 \pmod 2$ so we may use Hensel's lemma to lift solutions to mod 32. Since $P'(-1) = 11$ with inverse 1 Hensel's lemma implies the uniqueness of lifts to mod 2^n for all exponents n. As $P(-1) = -8 \equiv 0 \pmod{2^3}$ we may even start Hensel at $x_3 = -1$. Then $x_4 = x_3 - P(x_3) = -1 - (-8) = 7$ and $x_5 = x_4 - P(x_4) = 7 - (7^{11} - 7) \equiv -9 \pmod{32}$ which is then the unique solution. □

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

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

Proof. **First solution:** Again we may use Hensel's lemma because mod p there's the easy solution $x = 1$ with $P'(1) = 3$ invertible mod p. Since $P(1) \equiv 0 \pmod{p^2}$ we may start at $x_2 = 1$. Then $x_3 = x_2 - P(x_2)/3 = 1 + p^2/3$. Note that $P(x_3) = (1 + p^2/3)^3 - 1 - p^2 \equiv 0 \pmod 4$ so $x_4 = x_3$. Since $P(x_4) = P(1 + p^2/3) = p^4/3 + p^6/27$ we get $x_5 = x_4 - P(x_4)/3 = 1 + p^2/3 - (p^4/3 + p^6/27)/3 = 1 + p^2/3 - p^4/9 - p^6/27$. Then x_5 is the unique solution modulo p^5 lifting $1 \mod p$ but a simple verification shows that even modulo p^6 we have $P(x_5) \equiv P(1 + p^2/3 - p^4/9) = (1 + p^2/3 - p^4/9)^3 - 1 - p^2 \equiv (1 + p^2/3)^3 - (1 + p^2/3)p^4/3 \pmod{p^6} \equiv 1 + p^2 + p^4/3 - p^4/3 - 1 - p^2 \equiv 0 \pmod{p^6}$ so $1 + p^2/3 - p^4/9$ is the unique solution modulo p^6 lifting $1 \pmod p$.

Second solution: Let's try Taylor expansions and hope things make sense. Then

$$\begin{aligned} x &\equiv (1 + p^2)^{1/3} \pmod{p^6} \\ &\equiv 1 + \binom{1/3}{1} p^2 + \binom{1/3}{2} p^4 + \cdots \pmod{p^6} \end{aligned}$$

Note that

$$\binom{1/3}{k} = \frac{\frac{1}{3}(\frac{1}{3} - 1) \cdots (\frac{1}{3} - (k-1))}{k!} = \frac{(-1)^{k-1}(3k-4)(3k-7) \cdots 5 \cdot 2}{k! 3^k}$$

so

$$\binom{1/3}{k}p^{2k} = \frac{(-1)^{k-1}(3k-4)(3k-7)\cdots 5\cdot 2}{3^k}\frac{p^{2k}}{k!}$$

and the exponent of p in $k!$ is certainly less than k. In fact it is less than $k(1/p+1/p^2+\cdots) = k/(p-1)$. Thus every term in the sum makes sense modulo p^6 and we may in fact truncate after $k=6$. Thus

$$\begin{aligned} x &\equiv 1 + p^2/3 - p^4/3^2 + 5p^6/3^4 - 10p^8/3^5 + 22p^{12}/3^6 \pmod{p^6} \\ &\equiv 1 + p^2/3 - p^4/9 \pmod{p^6} \end{aligned}$$

as $p > 3$. □

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 $(X^m-1, X^n-1) = X^{(m,n)} - 1$.

Proof. (a):

$$\begin{aligned} X^m - 1 &= X^{nq+r} - 1 \\ &= X^{nq+r} - X^r + X^r - 1 \\ &= X^r(X^{nq}-1) + X^r - 1 \\ &= X^r(X^n-1)(1 + X^n + \cdots + X^{n(r-1)}) + X^r - 1 \\ &= (X^n-1)Q(X) + X^r - 1 \end{aligned}$$

where $\deg(X^r-1) < \deg(X^n-1)$.

(b): Suppose $m \geq n$. We'll do by induction on n. The base case is $n=0$ in which case immediately $X^m - 1 \mid X^n - 1 = 0$ and so the gcd is $X^m - 1 = X^{(m,0)} - 1$. We know that $(m,n) = (n,r)$ from the Euclidean algorithm for $\mathbb{Z}$. Part (a) and the Euclidean algorithm for polynomials also implies that $(X^m-1, X^n-1) = (X^n-1, X^r-1)$. As $r < n$ we can apply the inductive hypothesis to deduce that $(X^m-1, X^n-1) = X^{(n,r)} - 1 = X^{(m,n)} - 1$. □

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.)

Proof. In base a, a number is divisible by $a-1$ iff the sum of its base a digits are divisible by $a-1$. (Think divisibility by 9 in base 10.)

Since $781 = 11111_{(5)}$ we need to find

$$S = \sum_{k=\overline{k_4k_3k_2k_1k_0}_{(5)}, 4|k_0+\cdots k_4} \binom{11111_{(5)}}{\overline{k_4k_3k_2k_1k_0}_{(5)}} \equiv \sum_{k=\overline{k_4k_3k_2k_1k_0}_{(5)}, 4|k_0+\cdots k_4} \binom{1}{k_4}\cdots\binom{1}{k_0} \pmod 5$$

In the RHS the only way to get a nonzero term is if k_0, k_1, k_2, k_3, k_4 are either 0 or 1 or else the binomial factor in the product is 0. Thus the sum $k_0 + \cdots + k_4$ is either 0 or 4. In the former case all digits of k are 0 while in the later four are 1 and one is 0. There are 5 such possibilities. Therefore

$$S \equiv \binom{1}{0}^5 + \binom{11111}{01111} + \binom{11111}{10111} + \binom{11111}{11011} + \binom{11111}{11101} + \binom{11111}{11110} \equiv 1 + 5\binom{1}{1}^4\binom{1}{0} \equiv 1 \pmod 5$$

□