Math 104A - Fall 2014 - Midterm II

Name: __________________________________________

Student ID: ________________________________

Instructions:

Please print your name, student ID.

During the test, you may not use books, calculators or telephones.

Read each question carefully, and show all your work. Answers with no explanation will receive no credit, even if they are correct.

There are 4 questions which are worth 10 points each. You have 50 minutes to complete the test.

<table>
<thead>
<tr>
<th>Question</th>
<th>Score</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>40</td>
</tr>
</tbody>
</table>
Problem 1. [10 points.]

Solve the system of linear congruences
\[ x \equiv 9 \mod 12, \ x \equiv 51 \mod 75, \ x \equiv 36 \mod 90. \]

Solution:

(i) The moduli are not coprime:

\[ 12 = 2^2 \cdot 3, \ 75 = 3 \cdot 5^2, \ 45 = 3^2 \cdot 5. \]

We reduce the equations modulo powers of primes. We obtain

- for the powers of 2:

\[ x \equiv 9 \mod 2^2 \equiv 1 \mod 2. \]

- for the powers of 3:

\[ x \equiv 9 \mod 3 \equiv 0 \mod 3, \]
\[ x \equiv 51 \mod 3 \equiv 0 \mod 3, \]
\[ x \equiv 36 \mod 3^2 \equiv 0 \mod 3^2. \]

- for the powers of 5:

\[ x \equiv 51 \mod 5^2 \equiv 1 \mod 5, \]
\[ x \equiv 36 \mod 5 \equiv 1 \mod 5. \]

These equations are all compatible. We throw away the redundant equations to obtain

\[ x \equiv 1 \mod 4, \ x \equiv 0 \mod 9, \ x \equiv 1 \mod 25. \]

(ii) We combine the first and last equations into \( x \equiv 1 \mod 100. \) We need to solve

\[ x \equiv 0 \mod 9, \ x \equiv 1 \mod 100. \]

Thus

\[ x = 9k = 1 + 100\ell \]

which means

\[ 9|1 + 100\ell \implies 9|1 + \ell \implies \ell \equiv 8 \mod 9 \implies x \equiv 801 \mod 900. \]
Problem 2. [10 points.]

Solve the quadratic congruence
\[ x^2 - x - 9 \equiv 0 \mod 7^2. \]

Solution:

(i) We apply the quadratic formula to find the solutions mod 7. We have
\[
x_{1,2} = \frac{1 + \sqrt{37}}{2} = \frac{1 + 3}{2} = \frac{1 + 3}{2} = \frac{2}{2} = 2, -1.
\]

Alternatively, we can factor in \( \mathbb{Z}_7[x] \)
\[
x^2 - x - 19 = x^2 - x - 2 = (x - 2)(x + 1),
\]
to find the same solutions \( x = 2 \) and \( x = -1 \) in \( \mathbb{Z}_7 \).

(ii) We find the solutions mod \( 7^2 \). Let
\[
f(x) = x^2 - x - 9 \implies f'(x) = 2x - 1.
\]

We analyze two cases:

- \( x \equiv 2 \mod 7 \). The solution mod \( 7^2 \) is given by the formula proved in class
\[
x \equiv 2 - f(2) \cdot (f'(2))^{-1} \mod 7^2.
\]
Since \( f(2) = -7, f'(2) = 3 \implies (f'(2))^{-1} = 5 \) we obtain
\[
x \equiv 2 + 7 \cdot 5 \equiv 37 \mod 7^2.
\]

- \( x \equiv -1 \mod 7 \). The solution mod \( 7^2 \) is given by the formula proved in class
\[
x \equiv -1 - f(-1) \cdot (f'(-1))^{-1} \mod 7^2.
\]
Since \( f(-1) = -7, f'(-1) = -3 \implies (f'(-1))^{-1} = 2 \) we obtain
\[
x \equiv -1 + 7 \cdot 2 \equiv 13 \mod 7^2.
\]

Thus, there are two solutions: 37 and 13 mod \( 7^2 \).
Problem 3. [10 points.]

Let $p$ be a prime and consider the equation $x^p - px - 1 \equiv 0 \mod p^2$. Show that the equation has no solutions.

Solution:

(i) We reduce the equation mod $p$. It becomes

$$x^p - 1 \equiv 0 \mod p.$$

Using Fermat,

$$x^p \equiv x \mod p$$

so that

$$x \equiv 1 \mod p.$$

(ii) We next solve the equation mod $p^2$. We look for solutions $x = 1 + pt$. By Taylor, we have

$$f(x) = f(1) + pt \cdot f'(1) \mod p^2.$$

Note that

$$f(1) = -p, f'(1) = 0$$

so that from Taylor we obtain

$$f(x) \equiv -p \mod p^2.$$

The original equation has no solutions.
Problem 4. [10 points.]

Let \( p > 2 \) be a prime. Assume that the congruence \( x^4 \equiv -1 \mod p \) has a solution.

(i) Show that \( p \equiv 1 \mod 8 \).

(ii) Show that the equation \( x^4 \equiv -1 \mod p^n \) also has a solution for all \( n \).

(iii) Extra credit: prove that the converse of (i) is true.

Solution:

(i) Since \( x^4 \equiv -1 \mod p \) has a solution \( x_0 \), it follows that \( y^2 \equiv -1 \mod p \) has solution \( y_0 = x_0^2 \). By a result proved in class, we must have \( p \equiv 1 \mod 4 \).

Now, since \( x_0^4 \equiv -1 \mod p \), it follows that \( x_0 \) is coprime to \( p \). Raising the congruence to power \((p - 1)/4\) (which is an integer by the above discussion), we obtain

\[
x_0^{p-1} \equiv (-1)^{\frac{p-1}{4}} \mod p.
\]

The left hand side equals \( x_0^{p-1} \equiv 1 \mod p \) by Fermat. Thus,

\[
(-1)^{\frac{p-1}{4}} = 1 \mod p \implies \frac{p-1}{4} = 2k \implies p = 1 + 8k \implies p \equiv 1 \mod 8.
\]

(ii) Let \( f(x) = x^4 + 1, f'(x) = 4x^3 \). We use induction on \( n \). For \( n = 1 \) we know a solution exists by hypothesis. For the inductive step, assume that a solution \( x_n \) of the equation \( f(x) \equiv 0 \mod p^n \) exists. We wish to construct a solution \( x_{n+1} = x_n + p^n t \) for the equation

\[
f(x) \equiv 0 \mod p^{n+1}.
\]

Existence is guaranteed provided we show \( x_n \) is a non-singular solution of the equation \( f(x) \equiv 0 \mod p^n \). For a contradiction, assume we are in the singular case. Then

\[
f'(x_n) \equiv 0 \mod p \implies 4x_n^3 \equiv 0 \mod p.
\]

Since \( p > 2 \), we would get

\[
x_n \equiv 0 \mod p \implies f(x_n) = x_n^4 + 1 \not\equiv 0 \mod p
\]

contradiction.

(iii) Let \( a \) be a non-quadratic residue \( \mod p \). Then

\[
a^{\frac{p-1}{2}} \equiv -1 \mod p.
\]

Set

\[
x_0 = a^{\frac{p-1}{2}},
\]

which is well-defined since \( p \equiv 1 \mod 8 \). We compute

\[
x_0^4 = a^{\frac{p-1}{2}} \equiv -1 \mod p.
\]