# 18.781 Introduction to Number Theory

**Prof. A. De Sole**

**Mid Term Exam 2**

**April 24, 2014**

**First and Last Name:**  
Alberto De Sole

**MIT ID number:**  
1234567890

<table>
<thead>
<tr>
<th>Problem #</th>
<th>Total Points</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Total</td>
<td>60</td>
<td>60</td>
</tr>
</tbody>
</table>

Justify your answers!
Problem 1. Determine how many solutions each of the following congruences has

(a) $x^{48} \equiv 9 \pmod{17}$

(b) $x^{11} \equiv 9 \pmod{17}$

Solution:
Recall that, for an odd prime $p$, the equation $x^n \equiv a \pmod{p}$ either has $(n, p - 1)$ solutions, if $a^{\frac{p-1}{(n, p-1)}} \equiv 1 \pmod{p}$, or it has no solutions, if $a^{\frac{p-1}{(n, p-1)}} \not\equiv 1 \pmod{p}$.

In case (a), we have $(48, 16) = 16$, and $9^{\frac{16}{16}} \equiv 9 \not\equiv 1 \pmod{17}$, hence there are no solutions.

In case (b), we have $(11, 16) = 1$, and $9^{\frac{16}{16}} \equiv 1 \pmod{17}$ (by Fermat Little Thm), hence there is 1 solution.

Answer:

(a) number of solutions: $0$
(b) number of solutions: $1$
Problem 2. (a) Prove that \( g = 5 \) is a primitive root modulo \( m = 54 \).

(b) Solve the equation \( x^7 \equiv 25 \pmod{54} \).

Solution:

To prove that 5 is a primitive root, we just need to check that \( 5^k \not\equiv 1 \) for \( 1 \leq k < \phi(54) = 18 \). Since \( 5^{18} \equiv 1 \pmod{54} \) (by Euler-Fermat Thm), and since the prime divisors of 18 are 2 and 3, it is enough to check that \( 5^{18/2} = 5^9 \not\equiv 1 \pmod{54} \), and \( 5^{18/3} = 5^6 \not\equiv 1 \pmod{54} \).

We have \( 5^6 = 125^2 \equiv 17^2 \equiv 289 \equiv 19 \not\equiv 1 \pmod{54} \), and \( 5^9 = 125^3 \equiv 17^3 \equiv 17 \cdot 19 = 323 \equiv -1 \not\equiv 1 \pmod{54} \). Hence, 5 is a primitive root modulo 54.

Letting \( x = 5^u \), the equation reduces to \( 7u \equiv 2 \pmod{18} \). The solution is \( u = [7]_{18}^{-1} \cdot 2 = 13 \cdot 2 = 26 \equiv 8 \pmod{18} \). Hence, \( x = 5^8 = 625^2 \equiv 31^2 = 961 \equiv 43 \).

Answer:

(b) \( x = \boxed{43} \)
Problem 3. Find all the primes \( p \) such that \( n = 7 \) is a square residue modulo \( p \).

Solution:
First, for \( p = 2 \), \( n = 7 \equiv 1 = 1^2 \) is a square mod \( p \), and for \( p = 7 \), \( n = 7 \equiv 0 = 0^2 \) is also a square mod \( p \).

Let us next assume that \( p \) is an odd prime coprime to 7. We need to find all the primes \( p \) such that \( \left( \frac{7}{p} \right) = 1 \). By quadratic reciprocity, we have \( \left( \frac{7}{p} \right) = (-1)^{\frac{p-1}{2}} \left( \frac{p}{7} \right) \). Hence, we need to find all odd \( p \) such that \( \left( \frac{p}{7} \right) = (-1)^{\frac{p-1}{2}} \).

We have:
\[
\begin{align*}
\left( \frac{1}{7} \right) &= +1, \\
\left( \frac{-1}{7} \right) &= -1, \\
\left( \frac{2}{7} \right) &= -1, \\
\left( \frac{-2}{7} \right) &= +1, \\
\left( \frac{3}{7} \right) &= (\cdot -1)^2 \left( \frac{-1}{7} \right) = -1, \\
\left( \frac{4}{7} \right) &= +1, \\
\left( \frac{5}{7} \right) &= +1, \\
\left( \frac{-5}{7} \right) &= -1, \\
\left( \frac{6}{7} \right) &= -1.
\end{align*}
\]
We thus have the following table:

<table>
<thead>
<tr>
<th>( p ) mod 7</th>
<th>( \left( \frac{p}{7} \right) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>+1</td>
</tr>
<tr>
<td>2</td>
<td>+1</td>
</tr>
<tr>
<td>3</td>
<td>-1</td>
</tr>
<tr>
<td>4</td>
<td>+1</td>
</tr>
<tr>
<td>5</td>
<td>-1</td>
</tr>
<tr>
<td>6</td>
<td>-1</td>
</tr>
</tbody>
</table>

Therefore, the solutions to equation (1) are: the primes \( p \) such that:
(a) \( p \equiv 1 \) (4), and \( p \equiv 1, 2 \) or 4 mod 7,
(b) or \( p \equiv 3 \) (4), and \( p \equiv 3, 5 \) or 6 mod 7.

These cases are equivalent, respectively, to: \( p \equiv 1, 9, 25, 3, 19, 27 \) mod (28).

Answer:

Primes:

\( p \equiv 1, 3, 9, 19, 25, 27 \) (28)
Problem 4. Consider the following binary quadratic form: \( f(x, y) = 3x^2 - 4xy + 2y^2 \).

(a) Find the discriminant \( d \) of \( f \).

(b) Find a reduced form of \( f \).

(c) Compute the class number of \( d \).

Solution:
(a) \( d = (-4)^2 - 4 \cdot 3 \cdot 2 = -8 \).

(b) We have
\[
\begin{align*}
f &= 3x^2 - 4xy + 2y^2 \\
&\xrightarrow{y\rightarrow x} 2x^2 - 4xy + 3y^2 \\
&\xrightarrow{y\rightarrow x+y} 2x^2 + y^2 \\
&\xrightarrow{y\rightarrow x+y} x^2 + 2y^2.
\end{align*}
\]

(c) We need to count the number of reduced positive definite* forms of discriminant \( d = -8 \), namely the solutions \((a, b, c)\) of the equations
\[
0 \leq b \leq a \leq c, \quad b^2 - 4ac = -8.
\]

(* Note: depending on the reference, we can consider \( f \) and \( -f \) equivalent or not, and in class I was deliberately a bit vague about this point. So I consider valid both types of answers.) From the second equation we get \( a, c > 0, ac \geq 2 \), and using the inequalities, we also have \(-8 = b^2 - 4ac \leq -3ac\), which implies \( ac \leq \frac{8}{3} \). Hence, it must be \( ac = 2 \), and the only solution is \( a = 1, b = 0, c = 2 \). Therefore, \( H(d) = 1 \).

Answer:

(a) \( d = \boxed{-8} \) \hspace{1cm} (b) reduced form: \( x^2 + 2y^2 \) \hspace{1cm} (c) \( H(d) = \boxed{1} \)
Problem 5. Find all values of the parameter $a, b \in \mathbb{Z}$ for which the following system of linear equations admits integer solutions

$$\begin{align*}
3x + 6y - 9z &= 3 \\
6x - 3z &= b \\
12y - 15z &= a
\end{align*}$$

Solution:

We perform elementary row and column operations to the complete matrix (since we don’t need to find solutions, we don’t add the extra rows to keep track of the changes of variables):

$$\begin{pmatrix}
3 & 6 & -9 & 3 \\
6 & 0 & -3 & b \\
0 & 12 & -15 & a
\end{pmatrix} \begin{array}{c}
r_2 \rightarrow -2r_1 \\
+ r_2 \rightarrow -2r_1, c_3 + 3c_1 \\
+ r_3 \rightarrow -2r_1 \\
+ r_2 \rightarrow -2r_1, c_3 + 3c_1 \\
+ r_3 \rightarrow -2r_1
\end{array} \begin{pmatrix}
3 & 0 & 0 & 3 \\
0 & -12 & 15 & b - 6 \\
0 & 12 & -15 & a \\
0 & -12 & 15 & b - 6 \\
0 & 12 & -15 & a
\end{pmatrix}$$

Hence, in the new variables, the system becomes

$$\begin{align*}
3x' &= 3 \\
3y' &= b - 6 \\
0 &= a + b - 6
\end{align*}$$

and it has solutions if and only if $3 \mid b$, and $a + b = 6$.

Answer:

Values of $a$ and $b$: $3 \mid b$ and $a + b = 6$
**Problem 6.** Find all integer solutions of the following equation

\[ x^4 + 2x^3 + 2x^2 + 2x + 5 = y^2. \]

**Solution:**

We have

\[ P(x) = x^4 + 2x^3 + 2x^2 + 2x + 5 = (x^2 + x)^2 + x^2 + 2x + 5 > (x^2 + x)^2 \text{ for all } x, \]

and

\[ P(x) = x^4 + 2x^3 + 2x^2 + 2x + 5 = (x^2 + x + 1)^2 - (x^2 - 4) < (x^2 + x + 1)^2 \text{ if } |x| > 2. \]

Hence, if \(|x| > 2\), letting \(n = x^2 + x \in \mathbb{Z}\), we have \(n^2 < y^2 < (n + 1)^2\), which is impossible. It remains only to consider the cases when \(|x| \leq 2\), i.e. \(x = -2, -1, 0, 1, 2\). We have

\[
\begin{array}{ccc}
 x & P(x) & y \\
-2 & 9 & \pm 3 \\
-1 & 4 & \pm 2 \\
0 & 5 & \text{imp.} \\
1 & 12 & \text{imp} \\
2 & 49 & \pm 7 \\
\end{array}
\]

**Answer:**

\[(x, y) = (-2, \pm 3), (-1, \pm 2), (2, \pm 7)\]