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>Total</td>
<td>50</td>
<td>50</td>
</tr>
</tbody>
</table>

Justify your answers!
Problem 1. Check that 259 is invertible modulo 1815, and find its multiplicative inverse \( [259]_{1815}^{-1} \).

Solution:
We have, by the Euclidean argument:

\[
1815 = 259 \times 7 + 2 \\
259 = 2 \times 129 + 1
\]

Hence, \((259, 1815) = 1\), proving that 259 is invertible modulo 1815. To find the multiplicative inverse, we go backwards:

\[
1 = 259 - 2 \times 129 = 259 - (1815 - 259 \times 7) \times 129 = 259 \times (1 + 7 \times 129) - 1815 \times 129 = 259 \times 904 - 1815 \times 129
\]

Hence, \(259 \times 904 \equiv 1 \mod (1815)\).

Answer:

\[ [259]_{1815}^{-1} = 904 \]
Problem 2. Let $m, n \in \mathbb{N}$ be positive integers which are sums of two square, and assume that $m|n$. Is $\frac{n}{m} \in \mathbb{N}$ a sum of two squares?

Solution:
By the theorem proved in class, $m$ and $n$ are sums of two squares if and only if their prime factorizations are as follows,

\[
m = 2^\ell p_1^{i_1} \cdots p_s^{i_s} q_1^{2j_1} \cdots q_t^{2j_t}
\]
\[
n = 2^\ell p_1^{h_1} \cdots p_s^{h_s} q_1^{2k_1} \cdots q_t^{2k_t}
\]

where $p_1, \ldots, p_s$ are primes $\equiv 1 \pmod{4}$, and $q_1, \ldots, q_t$ are primes $\equiv 3 \pmod{4}$. To say that $m|n$ means that $\ell \leq r$, $i_1 \leq h_1, \ldots, i_s \leq h_s, j_1 \leq k_1, \ldots, j_t \leq k_t$. But then

\[
\frac{n}{m} = 2^{r-\ell} p_1^{h_1-i_1} \cdots p_s^{h_s-i_s} q_1^{2(k_1-j_1)} \cdots q_t^{2(k_t-j_t)}
\]

which implies that $\frac{n}{m}$ is again a sum of two squares.

Answer:

Is $\frac{n}{m} \in \mathbb{N}$ a sum of two squares? (circle) YES
Problem 3. (a) Compute the remainder of $132^{1601}$ in the division modulo 125.
(b) Compute the last three digits of the number $132^{1601}$.

Solution:
(a) We have $125 = 5^3$, so that $\phi(125) = 4 \cdot 5^2 = 100$. Also, 132 is clearly not divisible by 5, so that $(132, 125) = 1$. Hence, by the Euler-Fermat Theorem, we have $132^{100} \equiv 1 \pmod{125}$. But then

$$132^{1601} = 132^{100+16+1} = (132^{100})^{16} \cdot 132^1 \equiv 132 \equiv 7 \pmod{125}$$

Hence, the remainder of $132^{1601}$ in the division modulo 125 is 7.

(b) We want to solve for $x \equiv 132^{1601} \pmod{1000}$, with $0 \leq x \leq 999$. Since $1000 = 2^3 \cdot 5 \cdot 3$, this is equivalent to solve the Cinese system

$$\begin{cases}
    x \equiv 132^{1601} \equiv 7 \pmod{125} \\
    x \equiv 132^{1601} \equiv 0 \pmod{8}
\end{cases}$$

The solution is

$$x = \frac{1000}{125} \cdot [\frac{1000}{125}]^{-1} \cdot 7 + \frac{1000}{8} \cdot [\frac{1000}{8}]^{-1} \cdot 8 = 8 \cdot [8]^{-1}_{125} \cdot 7 = 8 \cdot 47 \cdot 7 = 2632 \equiv 632 \pmod{1000}$$

Answer:
(a) Remainder: \boxed{7}  
(b) Last three digits of $132^{1601}$: \boxed{6} \boxed{3} \boxed{2}
**Problem 4.** Solve the following congruence equation

\[ x^2 + 2x + 3 \equiv 0 \mod (18) \]

**Solution:**
We have \( 18 = 2 \times 3^2 \). First, we solve the equation modulo 2:

\[ x^2 + 2x + 3 \equiv x^2 + 1 \equiv 0 \mod (2) \]

and its solution is \( x = 2 \). Next, we solve the equation modulo 3:

\[ x^2 + 2x + 3 \equiv x^2 + 2x = x(x + 2) \equiv 0 \mod (3) \]

and its solutions are \( x = 0 \) and \( x = -2 = 1 \). We have \( f'(x) = 2x + 2 = 2(x + 1) \), so \( f'(0) = 2 \not\equiv 0 \) (3) and \( f'(1) = 4 \not\equiv 0 \) (3). Hence, both solutions are non singular, and they both lift to a unique solution modulo 9. They are:

\[ 0 \rightarrow 0 - [f'(0)]^{-1}f(0) = 3 \mod (9) \]
\[ 1 \rightarrow 1 - [f'(1)]^{-1}f(1) = 1 - 6 = 4 \mod (9) \]

The solutions of the original equations are the (unique modulo 18) solutions of the following Chinese systems:

\[ \begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 3 \pmod{9} \end{cases} \quad \text{and} \quad \begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 4 \pmod{9} \end{cases} \]

The first system has solution \( x = 3 \) (18), while the second has solution

\[ x = \frac{18}{2} \cdot [\frac{18}{2}]^{-1} \cdot 1 + \frac{18}{9} \cdot [\frac{18}{9}]^{-1} \cdot 4 = 9 + 2 \cdot 5 \cdot 4 = 49 \equiv 13 \mod (18) \]

**Answer:**

\[ x = 3, 13 \]
Problem 5. Find a polynomial $P(x) \in (\mathbb{Z}/5\mathbb{Z})[x]$ of degree less than or equal to 4 which corresponds to the same function $\mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ as $x^6 + 2x^5 + 3x^4 + x^2 + 3$.

Solution:
It suffices to find the remainder in the division of $x^6 + 2x^5 + 3x^4 + x^2 + 3$ by $x^5 - x$. We have
\[ x^6 + 2x^5 + 3x^4 + x^2 + 3 = (x^5 - x)(x + 2) + 3x^4 + 2x^2 + 2x + 3 \]
Hence, $P(x) = 3x^4 + 2x^2 + 2x + 3$.

Answer:

\[ P(X) = 3x^4 + 2x^2 + 2x + 3 \]