Hw #7 Solutions

1. #8 in 2.1

Show that \( a^{p-1} \equiv 1 \pmod{p} \)

(a) \( a = 2, \ p = 5 \)
\[ 2^4 = 16 = 1 + 5 \cdot 3 \equiv 1 \pmod{5} \]

(b) \( a = 4, \ p = 7 \)
\[ 4^6 = 2^{12} = 4096 = 1 + 7 \cdot 585 \equiv 1 \pmod{7} \]

(c) \( a = 3, \ p = 11 \)
\[ 3^{10} = 9^5 \equiv (-2)^5 \pmod{11} \]
\[ (-2)^5 = -32 = 1 + 11 \cdot (-3) \equiv 1 \pmod{11} \]

2. #16 in 2.1

(a) If \( a \in \mathbb{N} \), prove that \( a \) is congruent to its last digit \( \pmod{10} \).

Proof: The base 10 expansion is
\[ a = d_0 + d_1 \cdot 10 + \cdots + d_n \cdot 10^n \]
So, \( a \equiv d_0 + 0 + \cdots + 0 \equiv d_0 \pmod{10} \)

(b) Show that no perfect square has 2, 3, 7, or 8 as its last digit.

Proof: By part (a), this is the same as showing a perfect square cannot be congruent to 2, 3, 7, or 8 \( \pmod{10} \).

Test all congruence classes \( \pmod{10} \):
\[ \begin{align*}
[0]^2 &= [0] \\
[9]^2 &= [1] \end{align*} \]
Thus, every perfect square is in the set \([0, 1, 5, 6, 9] \).

\( \square \)
3. #26 in 201

a) Give an example to show that the following is false: If \( ab \equiv ac \pmod{n} \) and \( a \neq 0 \pmod{n} \), then \( b \equiv c \pmod{n} \).

Example: \( n = 12 \), \( a = 4 \), \( b = 3 \), \( c = 6 \)

b) Prove the statement in (a) when \( (a, n) = 1 \).

Proof: We are given that \( ab \equiv ac \pmod{n} \).

Therefore, \( n | (b - c) \). Since \( (a, n) = 1 \), \( n | (b - c) \). Thus \( b \equiv c \pmod{n} \). \( \square \)

4. #2 in 2.2

a) Solve \( x^2 = 1 \) in \( \mathbb{Z}_8 \)

<table>
<thead>
<tr>
<th>Not Solutions</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>( [0]^2 \neq [1] )</td>
<td>( [1]^2 = [17] ); ( x = [17] ) ( \checkmark )</td>
</tr>
</tbody>
</table>

b) \( x^4 = 1 \) in \( \mathbb{Z}_8 \); \( x = [1], [2], [5], [7] \) are solutions.

e.g. \( [37]^4 = [5-2]^4 = [16]^2 = [17] \).

c) \( x^2 + 3x + 2 = 0 \) in \( \mathbb{Z}_6 \)

\((x+2)(x+1) = 0 \) \( x = [1], [2], [4], [5] \) are solutions.

d) \( x^2 + 1 = 0 \) in \( \mathbb{Z}_{12} \)

No Solutions:
\( 0^2 = 0 \), \( 1^2 = 1 \), \( 2^2 = 4 \), \( 3^2 = 9 \), \( 4^2 = 4 \), \( 5^2 = 1 \), \( 6^2 = 0 \), \( (-6)^2 = 0 \), \( (-5)^2 = 1 \), \( (-4)^2 = 4 \), \( (-3)^2 = 9 \), \( (-2)^2 = 4 \), \( (-1)^2 = 1 \).

Adding [13] does not yield \([07]\).

e) False: \( 6 \cdot 2 = 0 \) in \( \mathbb{Z}_{12} \); \( 2 \cdot 6 \neq 0 \) in \( \mathbb{Z}_{12} \).