Theorems (NIB) 4, 5, 6, and 7

**Theorem (NIB) 4**: Suppose \( n \) is a positive integer.

If \( M \) is an integer, then \( M \equiv (M \mod n) \mod n \).

**Proof**: Let \( M \) be an integer. By definition of the "mod" function, \((M \mod n)\) equals the remainder \( r \) which results when the Quotient-Remainder Theorem is applied to the division of \( M \) by \( n \). Thus, \( M = nq + r \) for some integers \( q \) and \( r \), with \( r = (M \mod n) \).

Thus, by Theorem 8.4.1, \( M \equiv r \mod n \).

Since \( r = (M \mod n) \), \( M \equiv (M \mod n) \mod n \). QED

**Example**: Thus, since \((76 \mod 9) = 4\), because \(9 \cdot 8 = 72\),

\[ 76 \equiv 4 \mod 9, \] by Theorem (NIB) 4.

**Theorem (NIB) 5**: Suppose \( n \) is a positive integer.

If \( r \) is an integer and \( 0 \leq r < n \), then \( (r \mod n) = r \).

**Proof**: Let \( r \) be an integer such that \( 0 \leq r < n \).

Thus, \( r = (n)(0) + r \) and \( 0 \leq r < n \).

Thus, \( r \) is the remainder from dividing \( r \) by \( n \) when \( 0 \leq r < n \).

By the uniqueness of the remainder coming from the Quotient-Remainder Theorem and by the definition of the "mod" function, \( r = (r \mod n) \).

Therefore, \( (r \mod n) = r \). QED

**Example**: Thus, by Theorem (NIB) 5, since \( 0 \leq 7 < 12 \), \((7 \mod 12) = 7\).

Also, since \( 0 \leq 5,236 < 9,377 \), \((5,236 \mod 9,377) = 5,236\).

**Theorem (NIB) 6**: Suppose \( K, n \) and \( r \) are integers with \( n > 1 \).

If \( K \equiv r \mod n \) and \( 0 \leq r < n \), then \( (K \mod n) = r \).

**Proof**: Let \( K, n \) and \( r \) be integers with \( n > 1 \). Suppose \( K \equiv r \mod n \) and \( 0 \leq r < n \).

Since \( K \equiv r \mod n \), \((K \mod n) = (r \mod n)\), by Theorem 8.4.1.

Since \( 0 \leq r < n \), \((r \mod n) = r \) by Theorem (NIB) 5.

\[ \therefore (K \mod n) = r, \] by substitution. QED

**Example**: It can be shown that \( 14^8 \equiv 16 \mod 55 \) and \( 0 \leq 16 < 55 \).

Therefore, \((14^8 \mod 55) = 16\), by Theorem (NIB) 6.
Theorem (N18) 7: For any integer \( n \geq 1 \) and any integer \( K > 0 \), to determine \((-K \mod n)\), you do the following:

A. Determine \((+K \mod n)\)
B. If \((+K \mod n) = 0\), then \((-K \mod n) = 0\).
C. If \((+K \mod n) \neq 0\),
   then \((-K \mod n) = n - (+K \mod n)\).

Before presenting the proof, we illustrate applications of Theorem (N18) 7.

Examples:

1. Determine \((-36 \mod 13)\).
   
   Solution: \((+36 \mod 13) = 10\)
   
   because \(36 = 2 \times 13 + 10\) and \(0 \leq 10 < 13\).

   Since \((+36 \mod 13) \neq 0\), by Theorem (N18) 7,
   
   \((-36 \mod 13) = 13 - (+36 \mod 13)\)
   
   \[\therefore \ (-36 \mod 13) = 13 - 10 = 3.\]
   
   Note that \(-36 = (-3)(13) + 3 = -39 + 3 = -36\)
   and \(0 \leq 3 < 13\).

2. Determine \((-200 \mod 5)\).
   
   Solution: \((+200 \mod 5) = 0\)
   
   Since \(200 = 40 \times 5 + 0\)
   
   and \(0 \leq 0 < 5\),

   \[\therefore \ By \ Theorem \ (N18) \ 7, \ since \ (+200 \mod 5) = 0\]
   
   \((-200 \mod 5) = 0,\]

   \[\text{Note that } -200 = (-40) \times 5 + 0\]
   
   and \(0 \leq 0 < 5\).
3) Find \((-479 \mod 91)\).

Solution: \((+479 \mod 91) = 24\)

Since \(479 = 5 \times 91 + 24\)

and \(0 \leq 24 < 91\).

Since \((479 \mod 91) \neq 0\)

\((-479 \mod 91) = 91 - (479 \mod 91)\)

by Theorem (W18) 7.

\[ \therefore (-479 \mod 91) = 91 - 24 = 67 \]

Note that \(-479 = (-6) \times 91 + 67 = -546 + 67\)

and \(0 \leq 67 < 91\).

Proof of Theorem (W18) 7:

Let \(n\) and \(K\) be integers such that \(n \geq 1\) and \(K > 0\).

Let \(r = (+K \mod n)\).

\[ \therefore \text{There exists an integer } q \text{ such that } K = q \times n + r \text{ and } 0 \leq r < n, \]

by the Quotient-Remainder Theorem and the definition of \((K \mod n)\).

Suppose that \((+K \mod n) = 0\), and so \(r = 0\).

Then, since \(K = q \times n + r\), \(K = q \times n\).

\[ \therefore -K = (-q) \times n = (-q) \times n + 0 \text{ and } 0 \leq 0 < 91. \]

\[ \therefore \text{By definition of } (-K \mod n), (-K \mod n) = 0. \]
Finally, suppose \((+ K \mod n) \neq 0\).

\[ r \neq 0 \text{ since } r = (K \mod n). \]

Since \(0 \leq r < n\) and \(r \neq 0\), \(r - r < n - r\)

That is, \(0 < (n - r)\).

Since \(r \neq 0\), \((n - r) < n\)

\[ 0 < (n - r) < n \]

\[ 0 \leq (n - r) < n. \]

By the Q-R Theorem, there exist unique integers \(q_1\) and \(r_1\) such that \(-K = q_1 n + r_1\) and \(0 \leq r_1 < n\).

Also, by the definition of \((-K \mod n)\), \(r_1 = (-K \mod n)\).

Recall that \(K = q n + r\) and \(0 < n - r < n\).

\[ -K = -q n - r = (-q) n - r \]

\[ -K = (-q) n - n + n - r \]

\[ -K = (-q - 1) n + (n - r) \text{ and } 0 \leq (n - r) < n. \]

By the uniqueness of \(q_1\) and \(r_1\),

\[ r_1 = n - r, \]

\[ \text{Since } r_1 = (-K \mod n) \text{ and } r = (+K \mod n), \]

we have, by substitution, \((-K \mod n) = n - (+K \mod n)\).

\(\Box\) End by direct proof.