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

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

If M is an integer, then $M \equiv (M \bmod n) \pmod{n}$.

Proof: Let M be an integer. By definition of the "mod" function, $(M \bmod n)$ 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 $r = (M \bmod n)$.

Thus, by Theorem 8.4.1, $M \equiv r \pmod{n}$.

Since $r = (M \bmod n)$, $M \equiv (M \bmod n) \pmod{n}$. QED

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

$76 \equiv 4 \pmod{9}$, by Theorem (NIB) 4.

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

If r is an integer and $0 \le r < n$, then $(r \bmod n) = r$.

Proof: Let r be an integer such that $0 \le r < n$.

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

Thus, r is the remainder from dividing r by n when $0 \le r < n$.

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

Therefore, $(r \bmod n) = r$. QED

Example: Thus, by Theorem (NIB) 5, since $0 \le 7 < 12$, $(7 \bmod 12) = 7$.

Also, since $0 \le 5{,}236 < 9{,}377$, $(5{,}236 \bmod 9{,}377) = 5{,}236$.

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

If $K \equiv r \pmod{n}$ and $0 \le r < n$, then $(K \bmod n) = r$.

Proof: Let K, n and r be integers with $n > 1$. Suppose $K \equiv r \pmod{n}$ and $0 \le r < n$.

Since $K \equiv r \pmod{n}$, $(K \bmod n) = (r \bmod n)$, by Theorem 8.4.1.

Since $0 \le r < n$, $(r \bmod n) = r$ by Theorem (NIB) 5.

$\therefore (K \bmod n) = r$, by substitution. QED

Example: It can be shown that $14^8 \equiv 16 \pmod{55}$ and $0 \le 16 < 55$.

Therefore, $(14^8 \bmod 55) = 16$, by Theorem (NIB) 6.

Theorem (N1B) 7: For any integer $n \geq 1$ and any integer $K > 0$, to determine $(-K \bmod n)$, you do the following:

A. Determine $(+K \bmod n)$

B. If $(+K \bmod n) = 0$, then $(-K \bmod n) = 0$.

C. If $(+K \bmod n) \neq 0$, then $(-K \bmod n) = n - (+K \bmod n)$.

Before presenting the proof, we illustrate applications of Theorem (N1B) 7.

Examples: ① Determine $(-36 \bmod 13)$.

Solution: $(+36 \bmod 13) = 10$ because $36 = 2 \times 13 + 10$ and $0 \leq 10 < 13$.

Since $(+36 \bmod 13) \neq 0$, by Theorem (N1B) 7,

$(-36 \bmod 13) = 13 - (+36 \bmod 13)$

$\therefore$ $\underline{(-36 \bmod 13) = 13 - 10 = 3}$.

Note that $-36 = (-3)(13) + 3 = -39 + 3 = -36$ and $0 \leq 3 < 13$.

---

② Determine $(-200 \bmod 5)$.

Solution: $(+200 \bmod 5) = 0$

Since $200 = 40 \times 5 + 0$ and $0 \leq 0 < 5$.

$\therefore$ By Theorem (N1B) 7, Since $(+200 \bmod 5) = 0$

$(-200 \bmod 5) = 0$,

Note that $-200 = (-40) \times 5 + 0$ and $0 \leq 0 < 5$.

(3) FIND $(-479 \bmod 91)$.

Solution: $(+479 \bmod 91) = 24$

since $479 = 5 \times 91 + 24$

and $0 \le 24 < 91$.

Since $(479 \bmod 91) \ne 0$,

$(-479 \bmod 91) = 91 - (479 \bmod 91)$

by Theorem (W13) 7.

$\therefore \underline{(-479 \bmod 91) = 91 - 24 = 67}$

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

and $0 \le 67 < 91$.

Proof of Theorem (W13) 7:

Let n and K be integers such that $n \ge 1$ and $K > 0$.

Let $r = (+K \bmod n)$.

$\therefore$ There exists an integer q such that

$K = q \cdot n + r$ and $0 \le r < n$,

by the Quotient Remainder Theorem and the definition of $(K \bmod n)$.

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

Then, since $K = qn + r$, $K = qn$.

$\therefore -K = (-q)n = (-q)n + 0$ and $0 \le 0 < 91$.

$\therefore$ By definition of $(-K \bmod n)$, $(-K \bmod n) = 0$.

FINALLY, Suppose $(+K \bmod n) \neq 0$.

$\therefore$ $r \neq 0$ since $r = (K \bmod n)$.

Since $0 \leq r < n$ and $r \neq 0$, $r - r < n - r$,

That is, $0 < (n-r)$ $\therefore$

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

$\therefore$, $0 < (n-r) < n$

$\therefore$ $0 \leq (n-r) < n$.

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 $(-K \bmod n)$, $r_1 = (-K \bmod n)$.

Recall that $K = qn + r$ and $0 < n - r < n$.

$\therefore$ $-K = -qn - r = (-q)n - r$

$\therefore$ $-K = (-q)n - n + n - r$

$\therefore$ $-K = (-q-1)n + (n-r)$ and $0 \leq (n-r) < r$.

$\therefore$ By the uniqueness of q_1 and r_1,

$r_1 = n - r$.

$\therefore$ Since $r_1 = (-K \bmod n)$ and $r = (+K \bmod n)$, we have, by substitution, $(-K \bmod n) = n - (+K \bmod n)$.

QED, by direct proof.