THEOREMS 8.4.1 AND 8.4.3 SUMMARY

Thm 8.4.1

The following are EQUIVALENT

(1) $n \mid (a-b)$

(2) $a \equiv b \pmod{n}$

(3) $a = b + nk$ for some integer k

(4) a and b have the same QR Theorem remainder when divided by n

(5) $(a \bmod n) = (b \bmod n)$

Thm 8.4.3:

Given that $a \equiv A \pmod{n}$ and $b \equiv B \pmod{n}$ and k is a positive integer,

Then
1. $(a+b) \equiv (A+B) \pmod{n}$
2. $(a-b) \equiv (A-B) \pmod{n}$
3. $ab \equiv AB \pmod{n}$
4. $a^k \equiv A^k \pmod{n}$

THm 8.4.1 Let $a, b, n \in \mathbb{Z}, n > 1$ be given.

The following statements are EQUIVALENT: $(1) \Leftrightarrow (2) \Leftrightarrow \dots \Leftrightarrow (5)$.

(1) $n \mid (a-b)$

(2) $a \equiv b \pmod{n}$

(3) $a = b + nk$ for some $k \in \mathbb{Z}$

(4) a and b have the same Q-R Thm remainder when $\div n$.

(5) $(a \bmod n) = (b \bmod n)$

Proof: $(1) \Leftrightarrow (2)$. By def'n of "$\equiv \pmod{n}$"

$(1) \Leftrightarrow (3)$:

$[(1) \Rightarrow (3)]$: Suppose $n \mid (b-a)$. Then $b-a = nk$ for some $k \in \mathbb{Z}$.

$\therefore b = a + nk$. $\therefore (3)$.

$[(3) \Rightarrow (1)]$ $a = b + kn \Rightarrow a - b = kn \Rightarrow (1)$

$(4) \Leftrightarrow (5)$ by def'n of "$(x \bmod n)$" function.

$(1) \Leftrightarrow (5)$

$[(5) \Rightarrow (1)]$: Suppose $(a \bmod n) = (b \bmod n) = r$.

$\therefore$ By def'n and the QR Thm $a = nq_1 + r$ and $b = nq_2 + r$

$\therefore a - b = nq_1 - nq_2 = n(q_1 - q_2)$ $\therefore (1)$.

$[(1) \Rightarrow (5)]$: Assume $n \mid (a-b)$.

$\therefore a - b = nk$ for some $k \in \mathbb{Z}$. $(*)$

By The QR Thm, $b = nq + (b \bmod n)$ and $0 \le (b \bmod n) < n$, uniquely so.

$\therefore$ By $(*)$ $a = b + nk = \underbrace{nq + (b \bmod n)}_{= b} + nk$

$\therefore a = n(q+k) + (b \bmod n)$ and $0 \le (b \bmod n) < r$.

$\therefore a \bmod n = b \bmod n$, by def'n of "$x \bmod n$".

QED.

Theorem 8.4.3 (The Modular Arithmetic Theorem)

Let $a, b, A, B, n \in \mathbb{Z}$, $n > 1$ be given such that $a \equiv A \pmod{n}$ and $b \equiv B \pmod{n}$.

Then: (1) $(a+b) \equiv (A+B) \pmod{n}$

(2) $(a-b) \equiv (A-B) \pmod{n}$

(3) $ab \equiv AB \pmod{n}$

(4) For all positive integers k,

$$a^k \equiv A^k \pmod{n}$$

$$(\text{also, } b^k \equiv B^k \pmod{n}).$$

Proof: The proofs of (1), (2), (4) are left as an exercise.

(3): Since $a \equiv A \pmod{n}$ and $b \equiv B \pmod{n}$, by Theorem 8.4.1, there exist integers k and l such that $a = A + nk$ and $b = B + nl$.

$$\begin{aligned}
\therefore ab &= (A+nk)(B+nl) \\
&= AB + nkB + Anl + (nk)(nl) \\
&= AB + n(kB + Al + knl) \\
&= AB + nt, \text{ where } t = (kB + Al + knl),
\end{aligned}$$

which is an integer.

$\therefore ab \equiv AB \pmod{n}$ by Theorem 8.4.1.

QED.