Theorems and Corollaries of Chapter 2

Theorem 2.1: Let n be a positive integer. Then for any integers a, b, and c,

i. $a \equiv a \ mod \ n$ (reflexive);
ii. If $a \equiv b \ mod \ n$, then $b \equiv a \ mod \ n$ (symmetric); and
iii. If $a \equiv b \ mod \ n$ and $b \equiv c \ mod \ n$, then $a \equiv c \ mod \ n$ (transitive).

Theorem 2.2: Let n be a positive integer. Then for any integers a, b, c, and d such that $a \equiv b \ mod \ n$ and $c \equiv d \ mod \ n$, we have

i. $a + c \equiv b + d \ \ mod \ n$; and
ii. $ac \equiv bd \ \ mod \ n$.

Theorem 2.3: Let n be a positive integer. Then for any integers a and c, we have that $a \equiv c \ mod \ n$ if and only if $[a]_n = [c]_n$.

Corollary 2.4: Two congruence classes modulo n are either disjoint or identical.

Corollary 2.5: Let $n > 1$ be an integer and consider congruence modulo n.

i. If a is any integer and r is the remainder when a is divided by n, then $[a] = [r]$.
ii. There are exactly n distinct congruency classes, namely $[0], [1], \dots, [n-1]$.

Theorem 2.6: If $[a] = [b]$ and $[c] = [d]$ in $\mathbb{Z}_n$, then $[a + c] = [b + d]$ and $[ac] = [bd]$.

Theorem 2.7: For any classes $[a]$, $[b]$, and $[c]$ in $\mathbb{Z}_n$,

1. If $[a]$ and $[b]$ in $\mathbb{Z}_n$, then $[a] \oplus [b] = [a + b]$.
2. $[a] \oplus ([b] \oplus [c]) = ([a] \oplus [b]) \oplus [c]$
3. $[a] \oplus [b] = [b] \oplus [a]$
4. $[a] \oplus [0] = [a] = [0] \oplus [a]$
5. For each $[a]$ in $\mathbb{Z}_n$, the equation $[a] \oplus X = [0]$ has a solution in $\mathbb{Z}_n$.
6. If $[a]$ and $[b]$ in $\mathbb{Z}_n$, then $[a] \odot [b] = [ab]$.
7. $[a] \odot ([b] \odot [c]) = ([a] \odot [b]) \odot [c]$
8. $[a] \odot ([b] \oplus [c]) = ([a] \odot [b]) \oplus ([a] \odot [c])$ and $[a] \oplus ([b] \odot [c]) = ([a] \oplus [b]) \odot ([a] \oplus [c])$
9. $[a] \odot [b] = [b] \odot [a]$
10. $[a] \odot [1] = [a] = [1] \odot [a]$

Theorems and Corollaries of Chapter 2

Theorem 2.8: If $p > 1$ is an integer, then the following statements are equivalent:

i. p is prime.
ii. For any $a \neq 0$ in $\mathbb{Z}_p$, the equation $ax = 1$ has a solution in $\mathbb{Z}_p$.
iii. Whenever $ab = 0$ in $\mathbb{Z}_p$, then $a = 0$ or $b = 0$.

Corollary 2.9: Let p be a positive prime. For any $a \neq 0$ and any b in $\mathbb{Z}_p$, the equation $ax = b$ has a unique solution in $\mathbb{Z}_p$.

Corollary 2.10: Let a, b, and n be integers with $n > 1$ and $\gcd(a, n) = 1$. Then the equation $[a]x = [b]$ has a unique solution in $\mathbb{Z}_n$.

Theorem 2.11: Let a, b, and n be integers with $n > 1$, and let $\gcd(a, n) = d$. Then

i. the equation $[a]x = [b]$ has solutions in $\mathbb{Z}_n$ if and only if d divides b, and
ii. if d divides b, then the equation $[a]x = [b]$ has exactly d distinct solutions in $\mathbb{Z}_n$.