Math Definitions and Theorems in Chapter 4. Integers (Full Version)

for the purpose of proof citation[1]

Definition 7.1. (page 2 of lecture slides)
Let $n, d \in \mathbb{Z}$ with $d \neq 0$. We say that d **divides** n, denoted as $d \mid n$, if $n = dk$ for some $k \in \mathbb{Z}$, or equivalently, $n/d \in \mathbb{Z}$.

Theorem 7.2. (page 6 of lecture slides)
$\forall n \in \mathbb{Z}, n \neq 0, n \mid 0$.

Theorem 7.3. (page 8 of lecture slides)
If $d \mid n$, then $\pm d \mid \pm n$.

Theorem 7.4. (page 10 of lecture slides)
If $d \mid n$ and $n \neq 0$, then $|d| \leq |n|$.

Theorem 7.5 (Divisibility Theorem)**.** (page 15 of lecture slides)
Let $a, b, c \in \mathbb{Z}$. Then

(i) if $a \mid b$, $b \mid c$, then $a \mid c$. (**transitivity** property.)

(ii) $\forall m, n \in \mathbb{Z}$, if $a \mid b$, $a \mid c$, then $a \mid mb + nc$.

Theorem 7.6 (Division Algorithm)**.** (page 19 of lecture slides)
Let $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. Then there are unique integers q and r, with $0 \leq r < d$ such that $n = dq + r$.
(Here, $q = \lfloor n/q \rfloor$, $r = n - dq$.)

Definition 7.7. (page 40 of lecture slides)
If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then a is **congruent** to b modulo m if $m \mid (a - b)$. We write $a \equiv b \pmod{m}$.

Theorem 7.8. (page 44 of lecture slides)
Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then $a \equiv b \pmod{m}$ iff a **mod** $m = b$ **mod** m, i.e., a and b leave the same remainder when divided by m.

Theorem 7.9. (page 51 of lecture slides)
Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then $a \equiv b \pmod{m}$ iff $\exists k \in \mathbb{Z}$ such that $a = b + km$.

Theorem 7.10. (page 55 of lecture slides)
Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m}, \qquad ac \equiv bd \pmod{m}.$$

Definition 7.11. (page 64 of lecture slides)
A positive integer is

- **prime** if it has exactly 2 positive divisors, 1 and itself;
- **composite** if it has more than 2 positive divisors.

[1] In the numbering, 7 represents week 7 in Theorem/Defintion 7. $* *$; 8 represents week 8 in Theorem/Defintion 8. $* *$;

Theorem 7.12. (page 66 of lecture slides)
Every positive integer n greater than 1 has a divisor which is prime.

Theorem 7.13 (prime factorization theorem/Fundamental Theorem of Arithmetic)**.** (page 74 of lecture slides)
Every positive integer greater than 1 can be written uniquely as a product of primes where the prime factors are written in order of nondecreasing size.

Corollary 7.14. (page 77 of lecture slides)
Let the prime factorization of a positive integer m be

$$m = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}.$$

Then its divisors are of the form

$$d = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$$

where $0 \leq b_i \leq a_i$ for $i = 1, \dots, n$.

Theorem 7.15. (page 79 of lecture slides)
If n is composite, then it has a divisor d with $1 < d \leq \sqrt{n}$.

Corollary 7.16. (page 84 of lecture slides)
If $n > 1$ does not have a divisor d with $1 < d \leq \sqrt{n}$, then n is prime.

Theorem 7.17. (page 85 of lecture slides remark) If n is composite, then it has a prime divisor d with $1 < d \leq \sqrt{n}$.

Corollary 7.18. (page 85 of lecture slides remark) If $n > 1$ does not have a prime divisor d with $1 < d \leq \sqrt{n}$, then n is prime.

Theorem 7.19. (page 88 of lecture slides)
There are Infinitely Many Primes.

Definition 7.20. (page 95 of lecture slides)
Let a and b be integers, not both zero. The **greatest common divisor** of a and b, denoted by $\gcd(a, b)$, is the largest integer d such that $d \mid a$ and $d \mid b$.

Definition 7.21. (page 98 of lecture slides)
The integers a, b are **relatively prime** if $\gcd(a, b) = 1$

Theorem 7.22. (page 100 of lecture slides)
For any integer n, n and $n + 1$ are relatively prime.

Theorem 7.23 (GCD via Prime factorization)**.** (page 104 of lecture slides)
Let the prime factorizations of a, b be

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}, \quad b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$$

where $a_i, b_i \geq 0$ for $i = 1, \dots, n$. Then

$$\gcd(a, b) = p_1^{\min\{a_1, b_1\}} p_2^{\min\{a_2, b_2\}} \dots p_n^{\min\{a_n, b_n\}}.$$

Here $\min\{x, y\}$ represents the smaller of the two numbers x, y.

Theorem 7.24 (base b-expansion)**.** (page 107 of lecture slides)
Let $b(>1)$ be an integer. If $n \in \mathbb{Z}^+$, then it can be expressed uniquely in the form

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_0 b^0$$

where $k \in \mathbb{Z}_{\geq 0}$ and $0 \leq a_i < b$ for $i = 0, \ldots, k$ and $a_k \neq 0$.

Theorem 8.1. (page 119 of lecture slides)
Let a, b, q, r be integers such that

$$a = bq + r \text{ i.e.,} a \textbf{ mod } b = r.$$

Then

$$\gcd(a, b) = \gcd(b, r).$$

Theorem 8.2 (Bézout's Lemma)**.** (page 134 of lecture slides)
Let $a, b \in \mathbb{Z}^+$ and $d = \gcd(a, b)$. Then $\exists s, t \in \mathbb{Z}$ such that $d = as + bt$.

Theorem 8.3. (page 146 of lecture slides)
If $a, b, c \in \mathbb{Z}^+$ such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Theorem 8.4. (page 150 of lecture slides)
If p is a prime and $p \mid a_1 a_2 \ldots a_n$, then $p \mid a_k$ for some k.

Theorem 8.5 (Cancellation Theorem)**.** (page 151 of lecture slides)
Let $m \in \mathbb{Z}^+$ and $a, b, c \in \mathbb{Z}$. Then

$$ac \equiv bc \pmod{m} \& \ \gcd(c, m) = 1 \Rightarrow a \equiv b \pmod{m}.$$

Definition 8.6. (page 155 of lecture slides)
Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. An integer $\overline{a}$ such that

$$\overline{a}a \equiv 1 \pmod{m}$$

is called a **multiplicative inverse of** a **modulo** m.

Theorem 8.7 (Existence and uniqueness of the multiplicative inverse)**.** (page 159 of lecture slides)
Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. Then the multiplicative inverse of a modulo m exists iff $\gcd(a, m) = 1$. The multiplicative inverse, if exists, is unique modulo m, i.e., if c, d are inverses, then

$$c \equiv d \pmod{m}$$

Theorem 8.8. (page 173 of lecture slides)
Let $m \in \mathbb{Z}^+$. Suppose $a, b, c \in \mathbb{Z}$, where b is a multiplicative inverse of a modulo m. Then

$$ax \equiv c \pmod{m} \Leftrightarrow x \equiv bc \pmod{m}.$$

Theorem 8.9 (Fermat's Little Theorem)**.** (page 189 of lecture slides)
If p is a prime and $a \in \mathbb{Z}$ such that $\gcd(p, a) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.