# **Section 2.3.** The Integers and Division

**Note.** In this section we take you intuitive understanding of the integers $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ as an informal definition and develop some properties of the integers.

**Definition 2.3.1.** If $a$ and $b$ are integers with $a \neq 0$, we say that $a$ *divides* $b$ if $b = ac$ for some integer $c$. We denote this as $a \mid b$. If $a \mid b$ then $a$ is a *factor* of $b$ and $b$ is a *multiple* of $a$.

**Theorem 2.3.1.** Let $a, b, c \in \mathbb{Z}$. Then

**1.** if $a \mid b$ and $a \mid c$ then $a \mid (b + c)$,

**2.** if $a \mid b$ then $a \mid bc$ for all $c \in \mathbb{Z}$, and

**3.** if $a \mid b$ and $b \mid c$ then $a \mid c$.

**Definition 2.3.2.** A positive integer $p$ greater than 1 is *prime* if the only positive factors of $p$ are 1 and $p$. A positive integer that is greater than 1 and is not prime is *composite*.

**Theorem 2.3.2. The Fundamental Theorem of Arithmetic.**
Every positive integer can be written uniquely as the product of primes. (This unique way of factoring the number is called its *prime factorization*.)

**Theorem 2.3.3.** If $n$ is a positive composite integer, then $n$ has a prime divisor less than or equal to $\sqrt{n}$.

**Proof.** If $n$ is composite, then $n = ab$ for some positive integers $a$ and $b$. Now if both $a > \sqrt{n}$ and $b > \sqrt{n}$ then $ab > \sqrt{n}\sqrt{n} = n$, a contradiction. So either $a$ or $b$ is less than or equal to $\sqrt{n}$ (say it is $a$). By Theorem 2.3.2, $a$ has a prime factor and this factor is less than or equal to $a$, and so is $\leq \sqrt{n}$. ∎

**Example.** Is 113 prime? (We need only check up through $\sqrt{113} < 11$ for prime factors.)

**Theorem 2.3.4. The Division Algorithm.**
Let $a$ be an integer and $d$ a positive integer. Then there are unique integers $q$ and $r$, with $0 \leq r < d$, such that $a = dq + r$.

**Definition 2.3.3.** In Theorem 2.3.4, $d$ is the *divisor*, $a$ is the *dividend*, $q$ is the *quotient*, and $r$ is the *remainder*.

**Definition 2.3.4.** Let $a, b \in \mathbb{Z}$, not both zero. The largest integer $d$ such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of $a$ and $b$, denoted $\gcd(a, b)$.

**Definition 2.3.5.** Integers $a$ and $b$ are *relatively prime* if $\gcd(a, b) = 1$.

**Definition 2.3.6.** The integers $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ for $1 \leq i < j \leq n$.

**Note.** We can find greatest common divisors using prime factorizations. For example, $\gcd(40, 100) = \gcd(2^3 5, 2^2 5^2) = 2^2 5 = 20$.

**Definition.** The *least common multiple* of positive integers $a$ and $b$ is the smallest positive integer that is divisible by both $a$ and $b$, denoted $\operatorname{lcm}(a, b)$.

**Note.** We can find least common multiples using prime factorizations. For example, $\operatorname{lcm}(40, 100) = \operatorname{lcm}(2^3 5, 2^2 5^2) = 2^3 5^2 = 200$.

**Theorem 2.3.5.** Let $a$ and $b$ be positive integers. Then $ab = \gcd(a, b) \operatorname{lcm}(a, b)$.

**Definition 2.3.8.** Let $a \in \mathbb{Z}$ and let $m$ be a positive integer ($m \in \mathbb{Z}^+$). Denote the remainder when $a$ is divided by $m$ as "$a \pmod{m}$."

**Definition 2.3.9.** If $a$ and $b$ are integers and $m$ is a positive integer, then *$a$ is congruent to $b$ modulo $m$* if $m \mid (a - b)$, denoted $a \equiv b \pmod{m}$.

**Theorem 2.3.6.** Let $m \in \mathbb{Z}^+$. The integrs $a$ and $b$ are congruent modulo $m$ if and only if there is an integer $k$ such that $a = b + km$.

**Proof.** If $a \equiv b \pmod{m}$, then $m \mid (a-b)$. Therefore $a-b = km$ for some $k \in \mathbb{Z}$. So $a = b + km$.

If $a = b + km$ for some $k \in \mathbb{Z}$, then $a - b = km$ and $m \mid (a-b)$. Therefore $a \equiv b \pmod{m}$. ∎

**Theorem 2.3.7.** Let $m$ be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

**Proof.** Since $a \equiv b \pmod{m}$ and $c \equiv d$ (mod m), then there are integers $s$ and $t$ such that $b = a + sm$ and $d = c + tm$. hence $b + d = (a + sm) + )c + tm) = (a + c) + m(s + t)$ and $bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$. Therefore $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$. ∎

*Revised: 4/3/2019*