CSci 2312: Discrete Structures II: Divisibility

In this section, we study the divisibility of one integer by another. You should already be familiar with the basic ideas, but need to be able to prove them, using simple logical steps. Again, there is no way to become familiar with proofs without practice. Make sure you read the chapters on proofs from the recommended text.

$\exists$ denotes "there exists".

Definition For integers a and b, $a \neq 0$, a is said to *divide* b if $\exists m \in \mathbb{Z}$ such that $b = ma$. This is denoted as $a \mid b$. b is said to be *divisible* by a. Also, a is a *factor* or *divisor* of b, which is a *multiple* of a.

Examples: $2 \mid 1024$, $3 \mid 171$, $7 \mid -56$, $5 \nmid 1024$ (5 does not divide 1024).

Theorem Divisibility is *transitive*. That is, for integers a, b, c such that $a \neq 0$ and $b \neq 0$, if $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof: Suppose $a \neq 0$ and $b \neq 0$. Suppose further that $a \mid b$ and $b \mid c$.

$$a \mid b,\ b \mid c \Rightarrow\ \exists\, m_1, m_2 \in \mathbb{Z},\ s.t. b = m_1 a,\ c = m_2 b \Rightarrow c = m_1 m_2 a \Rightarrow \exists m = m_1 m_2 \in \mathbb{Z}\, such\ that\, c = ma \Rightarrow a \mid c$$

Example: $9 \mid 126$ and $126 \mid 378$, hence $9 \mid 378$.

Further, divisibility is *reflexive*:

$$a = 1 \times a \Rightarrow \exists m = 1 \in \mathbb{Z}\ such\ that\ a = ma \Rightarrow a \mid a$$

Example $3 \mid 3$

Divisibility is <u>not</u> *symmetric*. That is

$$a \mid b \nRightarrow b \mid a$$

To see this:

$$a \mid b \Rightarrow \exists m \in \mathbb{Z}\ such\ that\ b = ma \Rightarrow a = \frac{1}{m} b$$

Unless $m = \pm 1$, $\frac{1}{m} \notin \mathbb{Z}$, and, in general, $b \nmid a$.

Division Theorem or **Remainder Theorem:** If a and b are integers such that $b > 0$, $\exists$ unique integers q (the *quotient*) and r (the *remainder*) such that $a = bq + r$, with $0 \leq r < b$.

We study the proof in the text.

Example: $a = 7$, $b = 3$, $r = 1$, $q = 2$. Another example: $a = -9$, $b = 5$, $q = -2$, $r = 1$, and not $q = -1$ and $r = -4$. Why not? Because the remainder is not negative even if the number itself is. How do you obtain the non-negative remainder? Because the remainder is unique, and one obtains a negative value of r and a

corresponding quotient q such that $a = bq + r$, one can add multiples of b till the value of r is non-negative. So, for example, if you got $r = -4$, you could add $b = 5$ to it to obtain 1. Thus:

$$a = -9 = -1 \cdot 5 + -4 = -1 \cdot 5 + (5 - 5) + -4 = -2 \cdot 5 + 1$$

An *even integer* is an integer that is divisible by 2. That is, there is an integer m such that the even integer may be written as $2m$.

An *odd integer* is one that is not divisible by 2. Its remainder is 1 when divided by 2, hence $\exists$ unique integer q such that the odd integer may be written as $2q + 1$.