

CSCI 124/224: 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 do the problems from the handout.

\exists denotes “there exists”.

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

Examples: $2|1024$, $3|171$, $5 \nmid 1024$ (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 $a|b$ and $b|c$, then $a|c$.

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

$$\begin{aligned} & a|b, b|c \\ \Rightarrow & \exists m_1, m_2, \text{ s.t. } b = m_1a, c = m_2b \\ & \Rightarrow c = m_1m_2a \\ & \Rightarrow a|c \end{aligned}$$

Example: $9|126$ and $126|378$, hence $9|378$.

Division 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 do not study its proof.

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?)

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 $2q + 1$.

If the product of two integers is the integer 1, both integers are either 1 or -1 .