CSCI 2312: Discrete Structures II: Divisibility: Definition and Properties

We study the divisibility of one integer by another. You should already be familiar with the basic ideas. The following results can be easily proven from the definition; you will prove some in class, some in discussion and some for HW.

We begin with the definition:

Definition For integers a and b, $a \neq 0$, a is said to *divide* b if $\exists q \in \mathbb{Z}$ such that $b = qa$. 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. q is the integer quotient when b is divided by a; there is no remainder.

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

1. The following hold $\forall\ a, b, c, d \in \mathbb{Z},\ a \neq 0$ (that is, for all integers a, b, c, d such that a is non-zero) and $m \in \mathbb{Z}^+$ (that is, for all positive m):
   (a) $1 \mid a$, $a \mid 0$ and $a \mid a$
   (b) $a \mid b \Rightarrow a \mid kb\ \forall\ k\ \in \mathbb{Z}$
   (c) $a \mid b\ and\ a \mid c \Rightarrow a \mid (b + c)$
   (d) Using (b) and (c) above, one can show that:
      i. $a \mid b\ and\ a \mid c \Rightarrow a \mid (b - c)$
      ii. $a \mid b\ and\ a \mid\ c\ \Rightarrow\ a \mid (sb + tc)\ \forall\ s, t\ \in\ \mathbb{Z}$
   (e) $a \mid b \Leftrightarrow a \mid (-b) \Leftrightarrow (-a) \mid b$
   (f) $\forall a, b \in \mathbb{Z},\ a, b \neq 0\ \ a \mid b\ and\ b \mid a \Leftrightarrow a = \pm b$. You may use the fact that the product of two integers is 1 if and only if (often written as *iff*) the two integers are both either $+1$ or both -1.
   (g) Given $d \neq 0$, show that $a \mid b \Leftrightarrow da \mid db$
2. Divisibility is reflexive, that is $a \mid a$.
3. Divisibility is not symmetric. That is, the following statement is not true (you can think of many counterexamples):
$$a \mid b \Rightarrow b \mid a$$
4. 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 $a \mid c$.