1.2 Divisibility

Evan Hughes

January 2023

Definition of Divisibility

Let a and b be integers with $b \neq 0$. We say that b divides a(or that b is a divisor of a, or that b is a factor of a) if $a = bc$ for some integer c. "b divides a" is written $b \mid a$. And "b does not divide a" is written $b \nmid a$.

Example:(from the book)
$3 \mid 24$ because $24 = 3 \cdot 8$, but $3 \nmid 17$. Negative divisors are allowed: $-6 \mid 54$ because $54 = (-6) \cdot (-9)$, but $-6 \nmid -13$.

Note: If b divides a, then $a = bc$ for some c. Hence $-a = b(-c)$, so that $b \mid (-a)$. An analogous argument shows that every divisor of $-a$ is also a divisor of a. Therefore a and $-a$ have the same divisors.
Note: Suppose $a \neq 0$ and $b \mid a$. Then $a = bc$, so that $|a| = |b|\,|c|$. Consequently, $0 \leq |b| \leq |a|$. This last inequality is equivalent to $-|a| \leq b \leq |a|$. Therefore

- every divisor of the nonzero integer a is less than or equal to $|a|$;
- a nonzero integer has only finitely many divisors.

Greatest Common Divisor

Definition: Let a and b be integers, not both 0. The greatest common divisor (gcd) of a and b is the largest integer d that divides both a and b. In other words, d is the gcd of a and b provided that
(1) $d \mid a$ and $d \mid b$;
(2) If $c \mid a$ and $c \mid b$, then $c \leq d$.
The greatest common divisor of a and b is usually denoted (a, b).

Theorem 1.2

Let a and b be integers, not both 0, and let d be their greatest common divisor. Then there exist (not necessarily unique) integers u and v such that $d = au + bv$.

Corollary 1.3

Let a and b be integers, not both 0, and let d be a positive integer. Then d is the greatest common divisor of a and b if and only if d satisfies these conditions:
(i) $d \mid a$ and $d \mid b$;
(ii) if $c \mid a$ and $c \mid b$, then $c \mid d$.

Theorem 1.4

lf $a \mid bc$ and $(a, b) = 1$, then $a \mid c$.