# MTHSC 412 Section 1.2 – Divisibility

Kevin James

## Definition

Let $a, b \in \mathbb{Z}$ with $b \neq 0$. We say that $b$ *divides* $a$ or that $a$ is a *multiple* of $b$ if there is an integer $c$ such that $a = bc$. In this case, we write $b|a$.

## Example

- $3|12$ but $3 \not| 13$.
- If $b \neq 0$, then $b|0$ because $0 = b \cdot 0$.

**Remark**

- $a$ and $-a$ have the same divisors.
- If $a \neq 0$, then every divisor $b$ of $a$ satisfies $|b| \leq |a|$.
- A nonzero integer $a$ has only finitely many divisors.

### Definition

Suppose that $a, b \in \mathbb{Z}$, not both zero. Then we say that $d \in \mathbb{Z}$ is a greatest common divisor (gcd) of $a$ and $b$ if the following conditions are satisfied.

1. $d|a$ and $d|b$.
2. If $c|a$ and $c|b$ then $c \leq d$.

### Notation

If $d$ is the gcd of $a$ and $b$ we may write $(a, b) = d$.

### My Convention

It is sometimes useful to define $(0, 0) = 0$.

## Example

1. $(14,35) = 7$.
2. $(15,29) = 1$.

## Definition

If $(a, b) = 1$ then $a$ and $b$ are said to be *relatively prime* or *coprime*.

### Theorem

*Let $a, b \in \mathbb{Z}$ with at least one nonzero. Then there exists a unique gcd $d$ of $a$ and $b$. Moreover $d$ can be realized as an integral linear combination of $a$ and $b$. That is, there are (not necessarily unique) $m, n \in \mathbb{Z}$ such that*

$$d = am + bn.$$

*Further, $d$ is the smallest positive integer of this form.*

### Proof

Suppose that $a, b \in \mathbb{Z}$ with at least one being nonzero.
**Existence:** Let $S = \{ax + by \mid x, y \in \mathbb{Z}; ax + by > 0\}$.
First note that $a^2 + b^2 = a \cdot a + b \cdot b \in S$. So, $S \neq \emptyset$.
Using the well ordering principle, let $d$ be the least element of $S$.
Since, $d \in S$, there are $x, y \in \mathbb{Z}$ such that $d = ax + by$.
It is also clear that $d$ is the smallest such number which is positive.
By the division algorithm, we can write $a = dq + r$ with $0 \leq r < d$.
Then $r = a - dq = a - (ax + by)q = a(1 - xq) + b(-yq)$.
However, $r < d \Rightarrow r \notin S$, (b/c $d$ is the least element of $S$).
Thus $r = 0$ and $d|a$.
We can prove that $d|b$ in a similar way.

**Proof continued ...**

Finally suppose that $c|a$ and $c|b$.
Then we have $a = ck$ and $b = cm$ for some $k, m \in \mathbb{Z}$.
Thus $d = ax + by = ckx + cmy = c(kx + my)$ and $c|d$.
Thus, $c \leq |d| = d$. So, $d$ is the gcd of $a$ and $b$.
**Uniqueness:** Suppose now that we have two gcd's $d$ and $e$.
Since $d|a$ and $d|b$ and since $e$ is a gcd, $d \leq e$.
Since $e|a$ and $e|b$ and since $d$ is a gcd, $e \leq d$.
So, we have $d \leq e \leq d$ which can only be true if $e = d$. $\square$

### Corollary

*Let $a, b \in \mathbb{Z}$, not both zero, and let $0 < d \in \mathbb{Z}$. Then, $d$ is the gcd of $a$ and $b$ if and only if $d$ satisfies the following two conditions.*

1. $d|a$ *and* $d|b$.
2. *if* $c|a$ *and* $c|b$, *then* $c|d$.

## Proof.

($\Rightarrow$:) Suppose that $d = (a, b)$.
Then $d|a$ and $d|b$ by definition.
Also, there are $x, y \in \mathbb{Z}$ such that $d = ax + by$.
Suppose that $c|a$ and $c|b$.
Then we can write $a = ck$ and $b = cm$ for some $k, m \in \mathbb{Z}$.
So, $d = ax + by = (ck)x + (cm)y = c(kx + my)$.
Thus, $c|d$.
So, $d$ satisfies both conditions of our result.

($\Leftarrow$:) Now suppose $0 < d \in \mathbb{Z}$ satisfying conditions 1 and 2.
Then $d|a$ and $d|b$.
Now, suppose that $c|a$ and $c|b$.
Then we know that $c|d$ by condition 2.
So, by our remark, $c \leq |c| \leq |d| = d$.
Thus $d$ is the gcd of $a$ and $b$. $\square$

**Theorem**

*If $a$ and $b$ are coprime and $a|bc$ then $a|c$.*

**Proof.**

Since $a$ and $b$ are coprime, there are $x, y \in \mathbb{Z}$ such that $ax + by = 1$.
Since $a|bc$ there is $k \in \mathbb{Z}$ such that $bc = ak$. So,

$$\begin{aligned} 1 = ax + by &\Rightarrow c = acx + bcy \\ &\Rightarrow c = acx + aky \quad \text{(because } bc = ak\text{)} \\ &\Rightarrow c = a(cx + ky) \\ &\Rightarrow a|c. \end{aligned}$$

□

### Fact

*If $a = bq + r$ then $(a, b) = (b, r)$.*

### Proof

Suppose that $c$ is a common divisor of $a$ and $b$.
Then $a = ck$ and $b = cm$ for some $k, m \in \mathbb{Z}$.
Thus $r = a - bq = ck - (cm)q = c(k - mq)$.
Thus $c|r$ and is thus a common divisor of $b$ (by assumption) and $r$.

Now suppose that $c$ is a common divisor of $b$ and $r$. A similar argument shows that $c$ is a common divisor of $a$ and $b$.
So, the set of common divisors of $a$ and $b$ is identical to the set of common divisors of $b$ and $r$.
It follows that $(a, b) = (b, r)$ □

## Euclidean Algorithm

Given $a$ and $b$ not both zero, first note that $(a, b) = (|a|, |b|)$. So we may replace $a$ and $b$ by $|a|$ and $|b|$ respectively.
Thus after rearrangement if necessary we can assume that $a \geq 0$ and that $b > 0$.
Use the division algorithm to write

$$a = bq + r; \quad 0 \leq r < b$$

Then recall that $(a, b) = (b, r)$.
Now repeat the process with $a$ replaced by $b$ and $b$ replaced by $r$.
Continuing in this manner you will encounter a remainder of 0 because the remainders must be nonnegative and must decrease.
Now, note that $(r, 0) = r$.

Compute the $(246, 180)$.

$246 = 180(1) + 66 \Rightarrow (246, 180) = (180, 66)$.

$180 = 66(2) + 48 \Rightarrow (180, 66) = (66, 48)$.

$66 = 48(1) + 18 \Rightarrow (66, 48) = (48, 18)$.

$48 = 18(2) + 12 \Rightarrow (48, 18) = (18, 12)$.

$18 = 12(1) + 6 \Rightarrow (18, 12) = (12, 6)$.

$12 = 6(2) + 0 \Rightarrow (12, 6) = (6, 0) = 6!$

The Euclidean algorithm produces:

$$\begin{aligned}
a &= bq_1 + r_1 \\
b &= r_1 q_2 + r_2 \\
r_1 &= r_2 q_3 + r_3 \\
r_2 &= r_3 q_4 + r_4 \\
&\vdots \\
r_{i-2} &= r_{i-1} q_i + r_i \\
&\vdots \\
r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1} \\
r_{n-2} &= r_{n-1} q_n + r_n \\
r_{n-1} &= r_n q_{n+1} + 0
\end{aligned}$$

The Euclidean algorithm produces:

$$
\begin{aligned}
a &= bq_1 + r_1 & \Rightarrow \quad & r_1 = a - bq \\
b &= r_1 q_2 + r_2 & \Rightarrow \quad & r_2 = b - r_1 q_2 \\
r_1 &= r_2 q_3 + r_3 & \Rightarrow \quad & r_3 = r_1 - r_2 q_3 \\
r_2 &= r_3 q_4 + r_4 & \Rightarrow \quad & r_4 = r_2 - r_3 q_4 \\
&\vdots & & \vdots \\
r_{i-2} &= r_{i-1} q_i + r_i & \Rightarrow \quad & r_i = r_{i-2} - r_{i-1} q_i \\
&\vdots & & \vdots \\
r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1} & \Rightarrow \quad & r_{n-1} = r_{n-3} - r_{n-2} q_{n-1} \\
r_{n-2} &= r_{n-1} q_n + r_n & \Rightarrow \quad & r_n = r_{n-2} - r_{n-1} q_n \\
r_{n-1} &= r_n q_{n+1} + 0
\end{aligned}
$$

The Euclidean algorithm produces:

$$
\begin{aligned}
a &= bq_1 + r_1 & \Rightarrow \quad & r_1 = a - bq \\
b &= r_1 q_2 + r_2 & \Rightarrow \quad & r_2 = b - r_1 q_2 \\
r_1 &= r_2 q_3 + r_3 & \Rightarrow \quad & r_3 = r_1 - r_2 q_3 \\
r_2 &= r_3 q_4 + r_4 & \Rightarrow \quad & r_4 = r_2 - r_3 q_4 \\
&\vdots & & \vdots \\
r_{i-2} &= r_{i-1} q_i + r_i & \Rightarrow \quad & r_i = r_{i-2} - r_{i-1} q_i \\
&\vdots & & \vdots \\
r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1} & \Rightarrow \quad & r_{n-1} = r_{n-3} - r_{n-2} q_{n-1} \\
r_{n-2} &= r_{n-1} q_n + r_n & \Rightarrow \quad & r_n = r_{n-2} - r_{n-1} q_n \\
r_{n-1} &= r_n q_{n+1} + 0
\end{aligned}
$$

Note that $(a, b) = r_n$

The Euclidean algorithm produces:

$$
\begin{aligned}
a &= bq_1 + r_1 &\Rightarrow\quad & r_1 = a - bq \\
b &= r_1 q_2 + r_2 &\Rightarrow\quad & r_2 = b - r_1 q_2 \\
r_1 &= r_2 q_3 + r_3 &\Rightarrow\quad & r_3 = r_1 - r_2 q_3 \\
r_2 &= r_3 q_4 + r_4 &\Rightarrow\quad & r_4 = r_2 - r_3 q_4 \\
&\vdots & & \vdots \\
r_{i-2} &= r_{i-1} q_i + r_i &\Rightarrow\quad & r_i = r_{i-2} - r_{i-1} q_i \\
&\vdots & & \vdots \\
r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1} &\Rightarrow\quad & r_{n-1} = r_{n-3} - r_{n-2} q_{n-1} \\
r_{n-2} &= r_{n-1} q_n + r_n &\Rightarrow\quad & r_n = r_{n-2} - r_{n-1} q_n \\
r_{n-1} &= r_n q_{n+1} + 0
\end{aligned}
$$

Note that $(a, b) = r_n$ and we can use successive back substitution to write $r_n$ in terms of $r_k$ and $r_{k-1}$ eventually expressing $r_n$ in terms of $a$ and $b$.

## Example

Let's reconsider our previous example: $(246, 180) = 6$.

$$\begin{aligned}
246 = 180(1) + 66 &\quad\Rightarrow\quad 66 = 246 + (-1)180 \\
180 = 66(2) + 48 &\quad\Rightarrow\quad 48 = 180 + (-2)66 \\
66 = 48(1) + 18 &\quad\Rightarrow\quad 18 = 66 + (-1)48 \\
48 = 18(2) + 12 &\quad\Rightarrow\quad 12 = 48 + (-2)18 \\
18 = 12(1) + 6 &\quad\Rightarrow\quad 6 = 18 + (-1)12 \\
12 = 6(2) + 0 &
\end{aligned}$$

Now write

$$\begin{aligned}
6 &= 18 + (-1)12 = 18 + (-1)[48 + (-2)18] = (3)18 + (-1)48 \\
&= (3)[66 + (-1)48] + (-1)48 = (3)66 + (-4)48 \\
&= (3)66 + (-4)[180 + (-2)66] = (11)66 + (-4)180 \\
&= (11)[246 + (-1)180] + (-4)180 = (11)246 + (-15)180.
\end{aligned}$$

So, take $x = 11$ and $y = -15$.