MTHSC 412 Section 2.3 – Divisibility

Kevin James

Theorem (Well-Ordering Principle)

Every nonempty set S of positive integers has a least element. That is, there is $m \in S$ such that $x \in S \Rightarrow m \leq x$.

Theorem (Well-Ordering Principle)

Every nonempty set S of positive integers has a least element. That is, there is $m \in S$ such that $x \in S \Rightarrow m \leq x$.

Note

The well ordering principle is equivalent to the principle of mathematical induction.

Definition

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

Definition

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

Theorem

The divisors of 1 *are* ± 1.

Theorem (The Division Algorithm)

Suppose that $a, b \in \mathbb{Z}$ *with* $b > 0$. *Then there exist* $q, r \in \mathbb{Z}$ *such that*

1. $a = bq + r$, *and*
2. $0 \leq r < b$.

Theorem (The Division Algorithm)

Suppose that $a, b \in \mathbb{Z}$ *with* $b > 0$. *Then there exist* $q, r \in \mathbb{Z}$ *such that*

1. $a = bq + r$, *and*
2. $0 \leq r < b$.

Example

1. Given $a = 14$ and $b = 3$, we can write

Theorem (The Division Algorithm)

Suppose that $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist $q, r \in \mathbb{Z}$ such that

1. $a = bq + r$, *and*
2. $0 \leq r < b$.

Example

1. Given $a = 14$ and $b = 3$, we can write $14 = 3 * 4 + 2$. So, $q = 4$ and $r = 2$.

Theorem (The Division Algorithm)

Suppose that $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist $q, r \in \mathbb{Z}$ such that

1. $a = bq + r$, *and*
2. $0 \leq r < b$.

Example

1. Given $a = 14$ and $b = 3$, we can write $14 = 3 * 4 + 2$. So, $q = 4$ and $r = 2$.
2. Given $a = -14$ and $b = 3$, we can write

Theorem (The Division Algorithm)

Suppose that $a, b \in \mathbb{Z}$ *with* $b > 0$. *Then there exist* $q, r \in \mathbb{Z}$ *such that*

1. $a = bq + r$, *and*
2. $0 \leq r < b$.

Example

1. Given $a = 14$ and $b = 3$, we can write $14 = 3 * 4 + 2$. So, $q = 4$ and $r = 2$.
2. Given $a = -14$ and $b = 3$, we can write $-14 = 3 * (-5) + 1$. So, $q = -5$ and $r = 1$.

Proof.

Let $a, b \in \mathbb{Z}$ with $b > 0$.

Proof.

Let $a, b \in \mathbb{Z}$ with $b > 0$.
Let $S = \{a - bq \quad | \quad q \in \mathbb{Z}; a - bq \geq 0\}$.

PROOF.

Let $a, b \in \mathbb{Z}$ with $b > 0$.
Let $S = \{a - bq \quad | \quad q \in \mathbb{Z}; a - bq \geq 0\}$.
Note that if $0 \in S$ then There exists $q \in \mathbb{Z}$ such that

Proof.

Let $a, b \in \mathbb{Z}$ with $b > 0$.
Let $S = \{a - bq \quad | \quad q \in \mathbb{Z}; a - bq \geq 0\}$.
Note that if $0 \in S$ then There exists $q \in \mathbb{Z}$ such that
$a - bq = 0 \Rightarrow a = bq$

Proof.

Let $a, b \in \mathbb{Z}$ with $b > 0$.
Let $S = \{a - bq \quad | \quad q \in \mathbb{Z}; a - bq \geq 0\}$.
Note that if $0 \in S$ then There exists $q \in \mathbb{Z}$ such that
$a - bq = 0 \Rightarrow a = bq$
If $0 \notin S$ then S is a subset of the positive integers and thus has a smallest element.

Proof.

Let $a, b \in \mathbb{Z}$ with $b > 0$.
Let $S = \{a - bq \quad | \quad q \in \mathbb{Z}; a - bq \geq 0\}$.
Note that if $0 \in S$ then There exists $q \in \mathbb{Z}$ such that
$a - bq = 0 \Rightarrow a = bq$
If $0 \notin S$ then S is a subset of the positive integers and thus has a smallest element.
Let r be the smallest element of S.

Proof.

Let $a, b \in \mathbb{Z}$ with $b > 0$.
Let $S = \{a - bq \quad | \quad q \in \mathbb{Z}; a - bq \geq 0\}$.
Note that if $0 \in S$ then There exists $q \in \mathbb{Z}$ such that
$a - bq = 0 \Rightarrow a = bq$
If $0 \notin S$ then S is a subset of the positive integers and thus has a smallest element.
Let r be the smallest element of S.
Then $r \geq 0$ and we have for some $q \in \mathbb{Z}$, $a - bq = r \Rightarrow a = bq + r$.

Proof.

Let $a, b \in \mathbb{Z}$ with $b > 0$.
Let $S = \{a - bq \quad | \quad q \in \mathbb{Z}; a - bq \geq 0\}$.
Note that if $0 \in S$ then There exists $q \in \mathbb{Z}$ such that
$a - bq = 0 \Rightarrow a = bq$
If $0 \notin S$ then S is a subset of the positive integers and thus has a smallest element.
Let r be the smallest element of S.
Then $r \geq 0$ and we have for some $q \in \mathbb{Z}$, $a - bq = r \Rightarrow a = bq + r$.
Also, note that

Proof.

Let $a, b \in \mathbb{Z}$ with $b > 0$.
Let $S = \{a - bq \quad | \quad q \in \mathbb{Z}; a - bq \geq 0\}$.
Note that if $0 \in S$ then There exists $q \in \mathbb{Z}$ such that
$a - bq = 0 \Rightarrow a = bq$
If $0 \notin S$ then S is a subset of the positive integers and thus has a smallest element.
Let r be the smallest element of S.
Then $r \geq 0$ and we have for some $q \in \mathbb{Z}$, $a - bq = r \Rightarrow a = bq + r$.
Also, note that
$r - b = (a - bq) - b =$

Proof.

Let $a, b \in \mathbb{Z}$ with $b > 0$.
Let $S = \{a - bq \quad | \quad q \in \mathbb{Z}; a - bq \geq 0\}$.
Note that if $0 \in S$ then There exists $q \in \mathbb{Z}$ such that
$a - bq = 0 \Rightarrow a = bq$
If $0 \notin S$ then S is a subset of the positive integers and thus has a smallest element.
Let r be the smallest element of S.
Then $r \geq 0$ and we have for some $q \in \mathbb{Z}$, $a - bq = r \Rightarrow a = bq + r$.
Also, note that
$r - b = (a - bq) - b = \; = a - b(q + 1)$.

Proof.

Let $a, b \in \mathbb{Z}$ with $b > 0$.
Let $S = \{a - bq \quad | \quad q \in \mathbb{Z}; a - bq \geq 0\}$.
Note that if $0 \in S$ then There exists $q \in \mathbb{Z}$ such that
$a - bq = 0 \Rightarrow a = bq$
If $0 \notin S$ then S is a subset of the positive integers and thus has a smallest element.
Let r be the smallest element of S.
Then $r \geq 0$ and we have for some $q \in \mathbb{Z}$, $a - bq = r \Rightarrow a = bq + r$.
Also, note that
$r - b = (a - bq) - b = \ = a - b(q + 1)$.
Since $r - b < r$ and r is the least element of S, it follows that

Proof.

Let $a, b \in \mathbb{Z}$ with $b > 0$.
Let $S = \{a - bq \quad | \quad q \in \mathbb{Z}; a - bq \geq 0\}$.
Note that if $0 \in S$ then There exists $q \in \mathbb{Z}$ such that
$a - bq = 0 \Rightarrow a = bq$
If $0 \notin S$ then S is a subset of the positive integers and thus has a smallest element.
Let r be the smallest element of S.
Then $r \geq 0$ and we have for some $q \in \mathbb{Z}$, $a - bq = r \Rightarrow a = bq + r$.
Also, note that
$r - b = (a - bq) - b = \; = a - b(q + 1)$.
Since $r - b < r$ and r is the least element of S, it follows that
$r - b < 0 \Rightarrow r < b$. $\square$