Math 3110 Lecture 6

February 7, 2023

The GCD

Recall that we showed that if a and b are integers which are not both zero, then there is a unique largest integer d such that $d|a$ and $d|b$.

The GCD

Recall that we showed that if a and b are integers which are not both zero, then there is a unique largest integer d such that $d|a$ and $d|b$. We call d the *greatest common divisor* of a and b.

The GCD

Recall that we showed that if a and b are integers which are not both zero, then there is a unique largest integer d such that $d|a$ and $d|b$. We call d the *greatest common divisor* of a and b.

Example

Find $\gcd(54, 80)$.

The GCD

Recall that we showed that if a and b are integers which are not both zero, then there is a unique largest integer d such that $d|a$ and $d|b$. We call d the *greatest common divisor* of a and b.

Example

Find $\gcd(54, 80)$.

Solution

The gcd is 2.

The GCD

Recall that we showed that if a and b are integers which are not both zero, then there is a unique largest integer d such that $d|a$ and $d|b$. We call d the *greatest common divisor* of a and b.

Example

Find $\gcd(54, 80)$.

Solution

The gcd is 2.

The main purpose of this lecture is to prove a fundamental theorem which characterizes the GCD is a 'useful' way.

The GCD

Recall that we showed that if a and b are integers which are not both zero, then there is a unique largest integer d such that $d|a$ and $d|b$. We call d the *greatest common divisor* of a and b.

Example

Find $\gcd(54, 80)$.

Solution

The gcd is 2.

The main purpose of this lecture is to prove a fundamental theorem which characterizes the GCD is a 'useful' way. This will pave the way for proving the Fundamental Theorem of Arithmetic.

The GCD

Recall that we showed that if a and b are integers which are not both zero, then there is a unique largest integer d such that $d|a$ and $d|b$. We call d the *greatest common divisor* of a and b.

Example

Find $\gcd(54, 80)$.

Solution

The gcd is 2.

The main purpose of this lecture is to prove a fundamental theorem which characterizes the GCD is a 'useful' way. This will pave the way for proving the Fundamental Theorem of Arithmetic.

The GCD

Theorem (Characterization of the GCD)

Let a and b be integers which are not both 0 and let d be an integer.

The GCD

Theorem (Characterization of the GCD)

Let a and b be integers which are not both 0 and let d be an integer. Then $d = \gcd(a, b)$ if and only if the following hold:

The GCD

Theorem (Characterization of the GCD)

Let a and b be integers which are not both 0 and let d be an integer. Then $d = \gcd(a, b)$ if and only if the following hold:

(a) $d > 0$,

The GCD

Theorem (Characterization of the GCD)

Let a and b be integers which are not both 0 and let d be an integer. Then $d = \gcd(a, b)$ if and only if the following hold:

(a) $d > 0$,

(b) $d|a$ *and* $d|b$, *and*

The GCD

Theorem (Characterization of the GCD)

Let a and b be integers which are not both 0 and let d be an integer. Then $d = \gcd(a, b)$ if and only if the following hold:

(a) $d > 0$,

(b) $d|a$ *and* $d|b$, *and*

(c) *if c is any integer such that $c|a$ and $c|b$, then $c|d$.*

The GCD

Theorem (Characterization of the GCD)

Let a and b be integers which are not both 0 and let d be an integer. Then $d = \gcd(a, b)$ if and only if the following hold:

(a) $d > 0$,

(b) $d|a$ *and* $d|b$, *and*

(c) *if c is any integer such that $c|a$ and $c|b$, then $c|d$.*

Proof.

Let a and b be integers which are not both zero, and let $S = \{ax + by : x, y \in \mathbb{Z}\}$.

The GCD

Theorem (Characterization of the GCD)

Let a and b be integers which are not both 0 and let d be an integer. Then $d = \gcd(a, b)$ if and only if the following hold:

(a) $d > 0$,

(b) $d|a$ *and* $d|b$, *and*

(c) *if c is any integer such that $c|a$ and $c|b$, then $c|d$.*

Proof.

Let a and b be integers which are not both zero, and let $S = \{ax + by : x, y \in \mathbb{Z}\}$. We begin by proving several properties about S.

1. S is closed under addition:

The GCD

Theorem (Characterization of the GCD)

Let a and b be integers which are not both 0 and let d be an integer. Then $d = \gcd(a, b)$ if and only if the following hold:

(a) $d > 0$,

(b) $d|a$ *and* $d|b$, *and*

(c) *if c is any integer such that $c|a$ and $c|b$, then $c|d$.*

Proof.

Let a and b be integers which are not both zero, and let $S = \{ax + by : x, y \in \mathbb{Z}\}$. We begin by proving several properties about S.

1. S is closed under addition: let $\alpha, \beta \in S$.

The GCD

Theorem (Characterization of the GCD)

Let a and b be integers which are not both 0 and let d be an integer. Then $d = \gcd(a, b)$ if and only if the following hold:

(a) $d > 0$,

(b) $d|a$ *and* $d|b$, *and*

(c) *if c is any integer such that $c|a$ and $c|b$, then $c|d$.*

Proof.

Let a and b be integers which are not both zero, and let $S = \{ax + by : x, y \in \mathbb{Z}\}$. We begin by proving several properties about S.

1. S is closed under addition: let $\alpha, \beta \in S$. We will show that $\alpha + \beta \in S$.

The GCD

Theorem (Characterization of the GCD)

Let a and b be integers which are not both 0 and let d be an integer. Then $d = \gcd(a, b)$ if and only if the following hold:

(a) $d > 0$,

(b) $d|a$ *and* $d|b$, *and*

(c) *if c is any integer such that $c|a$ and $c|b$, then $c|d$.*

Proof.

Let a and b be integers which are not both zero, and let $S = \{ax + by : x, y \in \mathbb{Z}\}$. We begin by proving several properties about S.

1. S is closed under addition: let $\alpha, \beta \in S$. We will show that $\alpha + \beta \in S$. Since $\alpha, \beta \in S$, we see that $\alpha = ax_1 + bx_2$ for some integers x_2 and x_2 and $\beta = ay_1 + by_2$ for some integers y_1 and y_2.

The GCD

Theorem (Characterization of the GCD)

Let a and b be integers which are not both 0 and let d be an integer. Then $d = \gcd(a, b)$ if and only if the following hold:

(a) $d > 0$,

(b) $d|a$ *and* $d|b$, *and*

(c) *if c is any integer such that $c|a$ and $c|b$, then $c|d$.*

Proof.

Let a and b be integers which are not both zero, and let $S = \{ax + by : x, y \in \mathbb{Z}\}$. We begin by proving several properties about S.

1. S is closed under addition: let $\alpha, \beta \in S$. We will show that $\alpha + \beta \in S$. Since $\alpha, \beta \in S$, we see that $\alpha = ax_1 + bx_2$ for some integers x_2 and x_2 and $\beta = ay_1 + by_2$ for some integers y_1 and y_2. So $\alpha + \beta = ax_1 + bx_2 + ay_1 + by_2 = a(x_1 + y_1) + b(x_2 + y_2) \in S$.

The GCD

Theorem (Characterization of the GCD)

Let a and b be integers which are not both 0 and let d be an integer. Then $d = \gcd(a, b)$ if and only if the following hold:

(a) $d > 0$,

(b) $d|a$ *and* $d|b$, *and*

(c) *if c is any integer such that $c|a$ and $c|b$, then $c|d$.*

Proof.

Let a and b be integers which are not both zero, and let $S = \{ax + by : x, y \in \mathbb{Z}\}$. We begin by proving several properties about S.

1. S is closed under addition: let $\alpha, \beta \in S$. We will show that $\alpha + \beta \in S$. Since $\alpha, \beta \in S$, we see that $\alpha = ax_1 + bx_2$ for some integers x_2 and x_2 and $\beta = ay_1 + by_2$ for some integers y_1 and y_2. So $\alpha + \beta = ax_1 + bx_2 + ay_1 + by_2 = a(x_1 + y_1) + b(x_2 + y_2) \in S$. □

The GCD

Proof.

2. $S = \{ax + by : x, y \in \mathbb{Z}\}$ is closed under negatives:

The GCD

Proof.

2. $S = \{ax + by : x, y \in \mathbb{Z}\}$ is closed under negatives: let $\alpha \in S$.

The GCD

Proof.

2. $S = \{ax + by : x, y \in \mathbb{Z}\}$ is closed under negatives: let $\alpha \in S$. Then $\alpha = ax_1 + bx_2$ for some integers x and y.

The GCD

Proof.

2. $S = \{ax + by : x, y \in \mathbb{Z}\}$ is closed under negatives: let $\alpha \in S$. Then $\alpha = ax_1 + bx_2$ for some integers x and y. So $-\alpha = -(ax_1 + bx_2) = -ax_1 - bx_2 = a(-x_1) + b(-x_2) \in S$.

The GCD

Proof.

2. $S = \{ax + by : x, y \in \mathbb{Z}\}$ is closed under negatives: let $\alpha \in S$. Then $\alpha = ax_1 + bx_2$ for some integers x and y. So $-\alpha = -(ax_1 + bx_2) = -ax_1 - bx_2 = a(-x_1) + b(-x_2) \in S$.

3. If $z \in S$ and m is any integer, then $mz \in S$.

The GCD

Proof.

2. $S = \{ax + by : x, y \in \mathbb{Z}\}$ is closed under negatives: let $\alpha \in S$. Then $\alpha = ax_1 + bx_2$ for some integers x and y. So $-\alpha = -(ax_1 + bx_2) = -ax_1 - bx_2 = a(-x_1) + b(-x_2) \in S$.

3. If $z \in S$ and m is any integer, then $mz \in S$. Let $z = ax_1 + bx_2$ for some $x_1, x_2 \in \mathbb{Z}$.

The GCD

Proof.

2. $S = \{ax + by : x, y \in \mathbb{Z}\}$ is closed under negatives: let $\alpha \in S$. Then $\alpha = ax_1 + bx_2$ for some integers x and y. So $-\alpha = -(ax_1 + bx_2) = -ax_1 - bx_2 = a(-x_1) + b(-x_2) \in S$.

3. If $z \in S$ and m is any integer, then $mz \in S$. Let $z = ax_1 + bx_2$ for some $x_1, x_2 \in \mathbb{Z}$. Then $mz = max_1 + max_2 = a(mx_1) + b(mx_2) \in S$.

The GCD

Proof.

4. S contains a positive integer.

The GCD

Proof.

4. S contains a positive integer. To see this, note that by definition, $S = \{ax + by : x, y \in \mathbb{Z}\}$.

The GCD

Proof.

4. S contains a positive integer. To see this, note that by definition, $S = \{ax + by : x, y \in \mathbb{Z}\}$. Thus $a^2 + b^2 \in S$. Since a and b are not both zero, it follows that $a^2 + b^2 > 0$.

The GCD

Proof.

4. S contains a positive integer. To see this, note that by definition, $S = \{ax + by : x, y \in \mathbb{Z}\}$. Thus $a^2 + b^2 \in S$. Since a and b are not both zero, it follows that $a^2 + b^2 > 0$.Now let d^* be the smallest positive member of S.

5. Every member of S is a multiple of d^*.

The GCD

Proof.

4. S contains a positive integer. To see this, note that by definition, $S = \{ax + by : x, y \in \mathbb{Z}\}$. Thus $a^2 + b^2 \in S$. Since a and b are not both zero, it follows that $a^2 + b^2 > 0$.Now let d^* be the smallest positive member of S.

5. Every member of S is a multiple of d^*. Let $ax + by \in S$ be arbitrary (where $x, y \in \mathbb{Z}$).

The GCD

Proof.

4. S contains a positive integer. To see this, note that by definition, $S = \{ax + by : x, y \in \mathbb{Z}\}$. Thus $a^2 + b^2 \in S$. Since a and b are not both zero, it follows that $a^2 + b^2 > 0$.Now let d^* be the smallest positive member of S.

5. Every member of S is a multiple of d^*. Let $ax + by \in S$ be arbitrary (where $x, y \in \mathbb{Z}$). Now divide $ax + by$ by d^* using the Division Algorithm to get $ax + by = d^*q + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < d^*$.

The GCD

Proof.

4. S contains a positive integer. To see this, note that by definition, $S = \{ax + by : x, y \in \mathbb{Z}\}$. Thus $a^2 + b^2 \in S$. Since a and b are not both zero, it follows that $a^2 + b^2 > 0$.Now let d^* be the smallest positive member of S.

5. Every member of S is a multiple of d^*. Let $ax + by \in S$ be arbitrary (where $x, y \in \mathbb{Z}$). Now divide $ax + by$ by d^* using the Division Algorithm to get $ax + by = d^*q + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < d^*$. It now suffices to show that $r = 0$.

The GCD

Proof.

4. S contains a positive integer. To see this, note that by definition, $S = \{ax + by : x, y \in \mathbb{Z}\}$. Thus $a^2 + b^2 \in S$. Since a and b are not both zero, it follows that $a^2 + b^2 > 0$.Now let d^* be the smallest positive member of S.

5. Every member of S is a multiple of d^*. Let $ax + by \in S$ be arbitrary (where $x, y \in \mathbb{Z}$). Now divide $ax + by$ by d^* using the Division Algorithm to get $ax + by = d^*q + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < d^*$. It now suffices to show that $r = 0$. If not, then observe that $0 < r < d^*$.

The GCD

Proof.

4. S contains a positive integer. To see this, note that by definition, $S = \{ax + by : x, y \in \mathbb{Z}\}$. Thus $a^2 + b^2 \in S$. Since a and b are not both zero, it follows that $a^2 + b^2 > 0$.Now let d^* be the smallest positive member of S.

5. Every member of S is a multiple of d^*. Let $ax + by \in S$ be arbitrary (where $x, y \in \mathbb{Z}$). Now divide $ax + by$ by d^* using the Division Algorithm to get $ax + by = d^*q + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < d^*$. It now suffices to show that $r = 0$. If not, then observe that $0 < r < d^*$. Also, $r = ax + by - d^*q \in S$ by 1. - 3. above.

The GCD

Proof.

4. S contains a positive integer. To see this, note that by definition, $S = \{ax + by : x, y \in \mathbb{Z}\}$. Thus $a^2 + b^2 \in S$. Since a and b are not both zero, it follows that $a^2 + b^2 > 0$.Now let d^* be the smallest positive member of S.

5. Every member of S is a multiple of d^*. Let $ax + by \in S$ be arbitrary (where $x, y \in \mathbb{Z}$). Now divide $ax + by$ by d^* using the Division Algorithm to get $ax + by = d^*q + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < d^*$. It now suffices to show that $r = 0$. If not, then observe that $0 < r < d^*$. Also, $r = ax + by - d^*q \in S$ by 1. - 3. above. But now r is a SMALLER positive member of S than d^* is, a contradiction. □

The GCD

Proof.

We now prove that d^* satisfies (a) - (c) of the theorem.

The GCD

Proof.

We now prove that d^* satisfies (a) - (c) of the theorem.

(a) $d^* > 0$: this is immediate, since d^* was chosen to be the smallest positive member of S.

The GCD

Proof.

We now prove that d^* satisfies (a) - (c) of the theorem.

(a) $d^* > 0$: this is immediate, since d^* was chosen to be the smallest positive member of S.

(b) $d^*|a$ and $d^*|b$.

The GCD

Proof.

We now prove that d^* satisfies (a) - (c) of the theorem.

(a) $d^* > 0$: this is immediate, since d^* was chosen to be the smallest positive member of S.

(b) $d^*|a$ and $d^*|b$. To see this, note that $a = a \cdot 1 + b \cdot 0 \in S$.

The GCD

Proof.

We now prove that d^* satisfies (a) - (c) of the theorem.

(a) $d^* > 0$: this is immediate, since d^* was chosen to be the smallest positive member of S.

(b) $d^*|a$ and $d^*|b$. To see this, note that $a = a \cdot 1 + b \cdot 0 \in S$. By 5., a is a multiple of d^*.

The GCD

Proof.

We now prove that d^* satisfies (a) - (c) of the theorem.

(a) $d^* > 0$: this is immediate, since d^* was chosen to be the smallest positive member of S.

(b) $d^*|a$ and $d^*|b$. To see this, note that $a = a \cdot 1 + b \cdot 0 \in S$. By 5., a is a multiple of d^*. Similarly, $b = a \cdot 0 + b \cdot 1 = b$, so b is a multiple of d^*.

The GCD

Proof.

We now prove that d^* satisfies (a) - (c) of the theorem.

(a) $d^* > 0$: this is immediate, since d^* was chosen to be the smallest positive member of S.

(b) $d^*|a$ and $d^*|b$. To see this, note that $a = a \cdot 1 + b \cdot 0 \in S$. By 5., a is a multiple of d^*. Similarly, $b = a \cdot 0 + b \cdot 1 = b$, so b is a multiple of d^*.

(c) For every integer m: if $m|a$ and $m|b$, then $m|d^*$.

The GCD

Proof.

We now prove that d^* satisfies (a) - (c) of the theorem.

(a) $d^* > 0$: this is immediate, since d^* was chosen to be the smallest positive member of S.

(b) $d^*|a$ and $d^*|b$. To see this, note that $a = a \cdot 1 + b \cdot 0 \in S$. By 5., a is a multiple of d^*. Similarly, $b = a \cdot 0 + b \cdot 1 = b$, so b is a multiple of d^*.

(c) For every integer m: if $m|a$ and $m|b$, then $m|d^*$. To see this, recall that $d^* \in S$.

The GCD

Proof.

We now prove that d^* satisfies (a) - (c) of the theorem.

(a) $d^* > 0$: this is immediate, since d^* was chosen to be the smallest positive member of S.

(b) $d^*|a$ and $d^*|b$. To see this, note that $a = a \cdot 1 + b \cdot 0 \in S$. By 5., a is a multiple of d^*. Similarly, $b = a \cdot 0 + b \cdot 1 = b$, so b is a multiple of d^*.

(c) For every integer m: if $m|a$ and $m|b$, then $m|d^*$. To see this, recall that $d^* \in S$. Thus $d^* = ax + by$ for some integers x and y.

The GCD

Proof.

We now prove that d^* satisfies (a) - (c) of the theorem.

(a) $d^* > 0$: this is immediate, since d^* was chosen to be the smallest positive member of S.

(b) $d^*|a$ and $d^*|b$. To see this, note that $a = a \cdot 1 + b \cdot 0 \in S$. By 5., a is a multiple of d^*. Similarly, $b = a \cdot 0 + b \cdot 1 = b$, so b is a multiple of d^*.

(c) For every integer m: if $m|a$ and $m|b$, then $m|d^*$. To see this, recall that $d^* \in S$. Thus $d^* = ax + by$ for some integers x and y. Since $m|a$ and $m|b$, $mv = a$ and $mw = b$ for some integers v and w. So $d^* = ax + by = mvx + mwy = m(vx + wy)$, showing that $m|d^*$.

The GCD

Proof.

We now prove that d^* satisfies (a) - (c) of the theorem.

(a) $d^* > 0$: this is immediate, since d^* was chosen to be the smallest positive member of S.

(b) $d^*|a$ and $d^*|b$. To see this, note that $a = a \cdot 1 + b \cdot 0 \in S$. By 5., a is a multiple of d^*. Similarly, $b = a \cdot 0 + b \cdot 1 = b$, so b is a multiple of d^*.

(c) For every integer m: if $m|a$ and $m|b$, then $m|d^*$. To see this, recall that $d^* \in S$. Thus $d^* = ax + by$ for some integers x and y. Since $m|a$ and $m|b$, $mv = a$ and $mw = b$ for some integers v and w. So $d^* = ax + by = mvx + mwy = m(vx + wy)$, showing that $m|d^*$. □

The GCD

Proof.

We now show that $d^* = \gcd(a, b)$.

The GCD

Proof.

We now show that $d^* = \gcd(a, b)$. We have shown that d^* is positive and that $d^* | a$ and $d^* | b$.

The GCD

Proof.

We now show that $d^* = \gcd(a, b)$. We have shown that d^* is positive and that $d^*|a$ and $d^*|b$. Suppose that d is any integer dividing both a and b.

The GCD

Proof.

We now show that $d^* = \gcd(a, b)$. We have shown that d^* is positive and that $d^*|a$ and $d^*|b$. Suppose that d is any integer dividing both a and b. Then by (c) above, $d|d^*$.

The GCD

Proof.

We now show that $d^* = \gcd(a, b)$. We have shown that d^* is positive and that $d^*|a$ and $d^*|b$. Suppose that d is any integer dividing both a and b. Then by (c) above, $d|d^*$. Thus $d \leq |d| \leq |d^*| = d^*$, proving that d^* is the largest divisor of both a and b.

The GCD

Proof.

We now show that $d^* = \gcd(a, b)$. We have shown that d^* is positive and that $d^*|a$ and $d^*|b$. Suppose that d is any integer dividing both a and b. Then by (c) above, $d|d^*$. Thus $d \leq |d| \leq |d^*| = d^*$, proving that d^* is the largest divisor of both a and b.

Now suppose that d is any integer satisfying (a) - (c). We will show that $d = d^*$, where d^* is defined as above.

The GCD

Proof.

We now show that $d^* = \gcd(a, b)$. We have shown that d^* is positive and that $d^*|a$ and $d^*|b$. Suppose that d is any integer dividing both a and b. Then by (c) above, $d|d^*$. Thus $d \leq |d| \leq |d^*| = d^*$, proving that d^* is the largest divisor of both a and b.

Now suppose that d is any integer satisfying (a) - (c). We will show that $d = d^*$, where d^* is defined as above. Now, since $d|a$ and $d|b$, then $d|d^*$.

The GCD

Proof.

We now show that $d^* = \gcd(a, b)$. We have shown that d^* is positive and that $d^*|a$ and $d^*|b$. Suppose that d is any integer dividing both a and b. Then by (c) above, $d|d^*$. Thus $d \leq |d| \leq |d^*| = d^*$, proving that d^* is the largest divisor of both a and b.

Now suppose that d is any integer satisfying (a) - (c). We will show that $d = d^*$, where d^* is defined as above. Now, since $d|a$ and $d|b$, then $d|d^*$. Also, $d^*|a$ and $d^*|b$, and so by the third condition on d, we have $d^*|d$.

The GCD

Proof.

We now show that $d^* = \gcd(a, b)$. We have shown that d^* is positive and that $d^*|a$ and $d^*|b$. Suppose that d is any integer dividing both a and b. Then by (c) above, $d|d^*$. Thus $d \leq |d| \leq |d^*| = d^*$, proving that d^* is the largest divisor of both a and b.

Now suppose that d is any integer satisfying (a) - (c). We will show that $d = d^*$, where d^* is defined as above. Now, since $d|a$ and $d|b$, then $d|d^*$. Also, $d^*|a$ and $d^*|b$, and so by the third condition on d, we have $d^*|d$.Because d and d^* are both positive, $d = d^*$, and so d is the gcd of a and b.

The GCD

Proof.

We now show that $d^* = \gcd(a, b)$. We have shown that d^* is positive and that $d^*|a$ and $d^*|b$. Suppose that d is any integer dividing both a and b. Then by (c) above, $d|d^*$. Thus $d \leq |d| \leq |d^*| = d^*$, proving that d^* is the largest divisor of both a and b.

Now suppose that d is any integer satisfying (a) - (c). We will show that $d = d^*$, where d^* is defined as above. Now, since $d|a$ and $d|b$, then $d|d^*$. Also, $d^*|a$ and $d^*|b$, and so by the third condition on d, we have $d^*|d$.Because d and d^* are both positive, $d = d^*$, and so d is the gcd of a and b. □

The GCD

Now that we have given a more useful description of the gcd, we focus on proving some consequences.

The GCD

Now that we have given a more useful description of the gcd, we focus on proving some consequences.

Example

1. What is $\gcd(4, 5)$?

The GCD

Now that we have given a more useful description of the gcd, we focus on proving some consequences.

Example

1. What is $\gcd(4, 5)$? What is $\gcd(4, 4 + 5)$?

The GCD

Now that we have given a more useful description of the gcd, we focus on proving some consequences.

Example

1. What is $\gcd(4, 5)$? What is $\gcd(4, 4 + 5)$?
2. What is $\gcd(24, 28)$?

The GCD

Now that we have given a more useful description of the gcd, we focus on proving some consequences.

Example

1. What is $\gcd(4, 5)$? What is $\gcd(4, 4 + 5)$?
2. What is $\gcd(24, 28)$? What is $\gcd(24, 24 + 28)$?

The GCD

Now that we have given a more useful description of the gcd, we focus on proving some consequences.

Example

1. What is $\gcd(4, 5)$? What is $\gcd(4, 4 + 5)$?
2. What is $\gcd(24, 28)$? What is $\gcd(24, 24 + 28)$?

Example

Let a and b be integers which are not both zero.

The GCD

Now that we have given a more useful description of the gcd, we focus on proving some consequences.

Example

1. What is $\gcd(4, 5)$? What is $\gcd(4, 4 + 5)$?
2. What is $\gcd(24, 28)$? What is $\gcd(24, 24 + 28)$?

Example

Let a and b be integers which are not both zero. Is it true that $\gcd(a, b) = \gcd(a, a + b)$?

The GCD

Now that we have given a more useful description of the gcd, we focus on proving some consequences.

Example

1. What is $\gcd(4, 5)$? What is $\gcd(4, 4 + 5)$?
2. What is $\gcd(24, 28)$? What is $\gcd(24, 24 + 28)$?

Example

Let a and b be integers which are not both zero. Is it true that $\gcd(a, b) = \gcd(a, a + b)$?

Sketch of Proof.

Let $d = \gcd(a, b)$

The GCD

Now that we have given a more useful description of the gcd, we focus on proving some consequences.

Example

1. What is $\gcd(4, 5)$? What is $\gcd(4, 4 + 5)$?
2. What is $\gcd(24, 28)$? What is $\gcd(24, 24 + 28)$?

Example

Let a and b be integers which are not both zero. Is it true that $\gcd(a, b) = \gcd(a, a + b)$?

Sketch of Proof.

Let $d = \gcd(a, b)$ Then $d > 0$, $d|a$, and $d|b$.

The GCD

Now that we have given a more useful description of the gcd, we focus on proving some consequences.

Example

1. What is $\gcd(4, 5)$? What is $\gcd(4, 4 + 5)$?
2. What is $\gcd(24, 28)$? What is $\gcd(24, 24 + 28)$?

Example

Let a and b be integers which are not both zero. Is it true that $\gcd(a, b) = \gcd(a, a + b)$?

Sketch of Proof.

Let $d = \gcd(a, b)$ Then $d > 0$, $d|a$, and $d|b$. But now also $d|a + b$.

The GCD

Now that we have given a more useful description of the gcd, we focus on proving some consequences.

Example

1. What is $\gcd(4, 5)$? What is $\gcd(4, 4 + 5)$?
2. What is $\gcd(24, 28)$? What is $\gcd(24, 24 + 28)$?

Example

Let a and b be integers which are not both zero. Is it true that $\gcd(a, b) = \gcd(a, a + b)$?

Sketch of Proof.

Let $d = \gcd(a, b)$ Then $d > 0$, $d|a$, and $d|b$. But now also $d|a + b$. Let $x|a$ and $x|a + b$.

The GCD

Now that we have given a more useful description of the gcd, we focus on proving some consequences.

Example

1. What is $\gcd(4, 5)$? What is $\gcd(4, 4 + 5)$?
2. What is $\gcd(24, 28)$? What is $\gcd(24, 24 + 28)$?

Example

Let a and b be integers which are not both zero. Is it true that $\gcd(a, b) = \gcd(a, a + b)$?

Sketch of Proof.

Let $d = \gcd(a, b)$ Then $d > 0$, $d|a$, and $d|b$. But now also $d|a + b$. Let $x|a$ and $x|a + b$. Then $x|(-1)a + 1(a + b) = b$.

The GCD

Now that we have given a more useful description of the gcd, we focus on proving some consequences.

Example

1. What is $\gcd(4, 5)$? What is $\gcd(4, 4 + 5)$?
2. What is $\gcd(24, 28)$? What is $\gcd(24, 24 + 28)$?

Example

Let a and b be integers which are not both zero. Is it true that $\gcd(a, b) = \gcd(a, a + b)$?

Sketch of Proof.

Let $d = \gcd(a, b)$ Then $d > 0$, $d|a$, and $d|b$. But now also $d|a + b$. Let $x|a$ and $x|a + b$. Then $x|(-1)a + 1(a + b) = b$. So $x|a$ and $x|b$, and thus $x|d$.

The GCD

Now that we have given a more useful description of the gcd, we focus on proving some consequences.

Example

1. What is $\gcd(4, 5)$? What is $\gcd(4, 4 + 5)$?
2. What is $\gcd(24, 28)$? What is $\gcd(24, 24 + 28)$?

Example

Let a and b be integers which are not both zero. Is it true that $\gcd(a, b) = \gcd(a, a + b)$?

Sketch of Proof.

Let $d = \gcd(a, b)$ Then $d > 0$, $d|a$, and $d|b$. But now also $d|a + b$. Let $x|a$ and $x|a + b$. Then $x|(-1)a + 1(a + b) = b$. So $x|a$ and $x|b$, and thus $x|d$. This proves that $d = \gcd(a, a + b)$. □

The GCD

Example

Prove that for any integer m, we have $\gcd(m, m+1) = 1$.

Proof.

Let m be an integer, and let $d = \gcd(m, m+1)$.

The GCD

Example

Prove that for any integer m, we have $\gcd(m, m+1) = 1$.

Proof.

Let m be an integer, and let $d = \gcd(m, m+1)$. Then $d|m$ and $d|m+1$.

The GCD

Example

Prove that for any integer m, we have $\gcd(m, m+1) = 1$.

Proof.

Let m be an integer, and let $d = \gcd(m, m+1)$. Then $d|m$ and $d|m+1$. But then also $d|1(m+1) + -1(m) = 1$.

The GCD

Example

Prove that for any integer m, we have $\gcd(m, m+1) = 1$.

Proof.

Let m be an integer, and let $d = \gcd(m, m+1)$. Then $d|m$ and $d|m+1$. But then also $d|1(m+1) + -1(m) = 1$. Since $d > 0$, $d = 1$. $\square$

The GCD

Example

Prove that for any integer m, we have $\gcd(m, m+1) = 1$.

Proof.

Let m be an integer, and let $d = \gcd(m, m+1)$. Then $d|m$ and $d|m+1$. But then also $d|1(m+1) + -1(m) = 1$. Since $d > 0$, $d = 1$. □

Definition

Let a and b be integers.

The GCD

Example

Prove that for any integer m, we have $\gcd(m, m+1) = 1$.

Proof.

Let m be an integer, and let $d = \gcd(m, m+1)$. Then $d|m$ and $d|m+1$. But then also $d|1(m+1) + -1(m) = 1$. Since $d > 0$, $d = 1$. □

Definition

Let a and b be integers. Then we say that a and b are **relatively prime** provided $\gcd(a, b) = 1$.

The GCD

Example

Prove that for any integer m, we have $\gcd(m, m+1) = 1$.

Proof.

Let m be an integer, and let $d = \gcd(m, m+1)$. Then $d|m$ and $d|m+1$. But then also $d|1(m+1) + -1(m) = 1$. Since $d > 0$, $d = 1$. □

Definition

Let a and b be integers. Then we say that a and b are **relatively prime** provided $\gcd(a, b) = 1$.

Corollary

Let a and b be any integers.

The GCD

Example

Prove that for any integer m, we have $\gcd(m, m+1) = 1$.

Proof.

Let m be an integer, and let $d = \gcd(m, m+1)$. Then $d|m$ and $d|m+1$. But then also $d|1(m+1) + -1(m) = 1$. Since $d > 0$, $d = 1$. □

Definition

Let a and b be integers. Then we say that a and b are **relatively prime** provided $\gcd(a, b) = 1$.

Corollary

Let a and b be any integers. Then a and b are relatively prime if and only if there are integers x and y such that $ax + by = 1$.

The GCD

Example

Prove that for any integer m, we have $\gcd(m, m+1) = 1$.

Proof.

Let m be an integer, and let $d = \gcd(m, m+1)$. Then $d|m$ and $d|m+1$. But then also $d|1(m+1) + -1(m) = 1$. Since $d > 0$, $d = 1$. □

Definition

Let a and b be integers. Then we say that a and b are **relatively prime** provided $\gcd(a, b) = 1$.

Corollary

Let a and b be any integers. Then a and b are relatively prime if and only if there are integers x and y such that $ax + by = 1$.

The GCD

Proof.

REMEMBER: for ANY integers a and b which are not both zero, $\gcd(a, b) = d \in S = \{ax + by : x, y \in \mathbb{Z}\}$ and so THE GCD OF ANY TWO NONZERO INTEGERS IS ALWAYS AN INTEGER LINEAR COMBINATION OF THEM.

The GCD

Proof.

REMEMBER: for ANY integers a and b which are not both zero, $\gcd(a, b) = d \in S = \{ax + by : x, y \in \mathbb{Z}\}$ and so THE GCD OF ANY TWO NONZERO INTEGERS IS ALWAYS AN INTEGER LINEAR COMBINATION OF THEM.

Suppose first that a and b are relatively prime.

The GCD

Proof.

REMEMBER: for ANY integers a and b which are not both zero, $\gcd(a, b) = d \in S = \{ax + by : x, y \in \mathbb{Z}\}$ and so THE GCD OF ANY TWO NONZERO INTEGERS IS ALWAYS AN INTEGER LINEAR COMBINATION OF THEM.

Suppose first that a and b are relatively prime. Then $\gcd(a, b) = 1$.

The GCD

Proof.

REMEMBER: for ANY integers a and b which are not both zero, $\gcd(a, b) = d \in S = \{ax + by : x, y \in \mathbb{Z}\}$ and so THE GCD OF ANY TWO NONZERO INTEGERS IS ALWAYS AN INTEGER LINEAR COMBINATION OF THEM.

Suppose first that a and b are relatively prime. Then $\gcd(a, b) = 1$. By the above remark, $ax + by = 1$ for some integers x and y.

The GCD

Proof.

REMEMBER: for ANY integers a and b which are not both zero, $\gcd(a, b) = d \in S = \{ax + by : x, y \in \mathbb{Z}\}$ and so THE GCD OF ANY TWO NONZERO INTEGERS IS ALWAYS AN INTEGER LINEAR COMBINATION OF THEM.

Suppose first that a and b are relatively prime. Then $\gcd(a, b) = 1$. By the above remark, $ax + by = 1$ for some integers x and y. Conversely, suppose that $ax + by = 1$ for some integers x and y.

The GCD

Proof.

REMEMBER: for ANY integers a and b which are not both zero, $\gcd(a, b) = d \in S = \{ax + by : x, y \in \mathbb{Z}\}$ and so THE GCD OF ANY TWO NONZERO INTEGERS IS ALWAYS AN INTEGER LINEAR COMBINATION OF THEM.

Suppose first that a and b are relatively prime. Then $\gcd(a, b) = 1$. By the above remark, $ax + by = 1$ for some integers x and y. Conversely, suppose that $ax + by = 1$ for some integers x and y. Then a and b can't both be zero; let $d = \gcd(a, b)$.

The GCD

Proof.

REMEMBER: for ANY integers a and b which are not both zero, $\gcd(a, b) = d \in S = \{ax + by : x, y \in \mathbb{Z}\}$ and so THE GCD OF ANY TWO NONZERO INTEGERS IS ALWAYS AN INTEGER LINEAR COMBINATION OF THEM.

Suppose first that a and b are relatively prime. Then $\gcd(a, b) = 1$. By the above remark, $ax + by = 1$ for some integers x and y. Conversely, suppose that $ax + by = 1$ for some integers x and y. Then a and b can't both be zero; let $d = \gcd(a, b)$. Then $dv = a$ and $dw = b$ for some integers v and w.

The GCD

Proof.

REMEMBER: for ANY integers a and b which are not both zero, $\gcd(a, b) = d \in S = \{ax + by : x, y \in \mathbb{Z}\}$ and so THE GCD OF ANY TWO NONZERO INTEGERS IS ALWAYS AN INTEGER LINEAR COMBINATION OF THEM.

Suppose first that a and b are relatively prime. Then $\gcd(a, b) = 1$. By the above remark, $ax + by = 1$ for some integers x and y. Conversely, suppose that $ax + by = 1$ for some integers x and y. Then a and b can't both be zero; let $d = \gcd(a, b)$. Then $dv = a$ and $dw = b$ for some integers v and w. So $1 = ax + by = dvx + dwy = d(vx + wy)$.

The GCD

Proof.

REMEMBER: for ANY integers a and b which are not both zero, $\gcd(a, b) = d \in S = \{ax + by : x, y \in \mathbb{Z}\}$ and so THE GCD OF ANY TWO NONZERO INTEGERS IS ALWAYS AN INTEGER LINEAR COMBINATION OF THEM.

Suppose first that a and b are relatively prime. Then $\gcd(a, b) = 1$. By the above remark, $ax + by = 1$ for some integers x and y. Conversely, suppose that $ax + by = 1$ for some integers x and y. Then a and b can't both be zero; let $d = \gcd(a, b)$. Then $dv = a$ and $dw = b$ for some integers v and w. So $1 = ax + by = dvx + dwy = d(vx + wy)$. Thus $d|1$, and since $d > 0$, $d = 1$. □