Math 3110 Lecture 11

Greg Oman

University of Colorado
Colorado Springs

Finishing the LCM

We now prove a characterization of the LCM which is the analog to the characterization of the GCD.

Finishing the LCM

We now prove a characterization of the LCM which is the analog to the characterization of the GCD.

Theorem (Characterization of the LCM)

Let a and b be nonzero integers, and let m be an integer.

Finishing the LCM

We now prove a characterization of the LCM which is the analog to the characterization of the GCD.

Theorem (Characterization of the LCM)

Let a and b be nonzero integers, and let m be an integer. Then $m = \operatorname{lcm}(a, b)$ if and only if the following hold:

Finishing the LCM

We now prove a characterization of the LCM which is the analog to the characterization of the GCD.

Theorem (Characterization of the LCM)

Let a and b be nonzero integers, and let m be an integer. Then $m = \operatorname{lcm}(a, b)$ if and only if the following hold:

1. $m > 0$,

Finishing the LCM

We now prove a characterization of the LCM which is the analog to the characterization of the GCD.

Theorem (Characterization of the LCM)

Let a and b be nonzero integers, and let m be an integer. Then $m = \operatorname{lcm}(a, b)$ if and only if the following hold:

1. $m > 0$,
2. $a|m$ *and* $b|m$, *and*

Finishing the LCM

We now prove a characterization of the LCM which is the analog to the characterization of the GCD.

Theorem (Characterization of the LCM)

Let a and b be nonzero integers, and let m be an integer. Then $m = \operatorname{lcm}(a, b)$ if and only if the following hold:

1. $m > 0$,
2. $a|m$ *and* $b|m$, *and*
3. *for every integer* x: *if* $a|x$ *and* $b|x$, *then* $m|x$.

Finishing the LCM

We now prove a characterization of the LCM which is the analog to the characterization of the GCD.

Theorem (Characterization of the LCM)

Let a and b be nonzero integers, and let m be an integer. Then $m = \operatorname{lcm}(a, b)$ if and only if the following hold:

1. $m > 0$,
2. $a|m$ *and* $b|m$, *and*
3. *for every integer* x: *if* $a|x$ *and* $b|x$, *then* $m|x$.

Finishing the LCM

We now prove a characterization of the LCM which is the analog to the characterization of the GCD.

Theorem (Characterization of the LCM)

Let a and b be nonzero integers, and let m be an integer. Then $m = \operatorname{lcm}(a, b)$ if and only if the following hold:

1. $m > 0$,
2. $a|m$ *and* $b|m$, *and*
3. *for every integer x: if $a|x$ and $b|x$, then $m|x$.*

Proof.

The proof is very similar the the characterization of the GCD.

Finishing the LCM

We now prove a characterization of the LCM which is the analog to the characterization of the GCD.

Theorem (Characterization of the LCM)

Let a and b be nonzero integers, and let m be an integer. Then $m = \operatorname{lcm}(a, b)$ if and only if the following hold:

1. $m > 0$,
2. $a|m$ *and* $b|m$, *and*
3. *for every integer x: if $a|x$ and $b|x$, then $m|x$.*

Proof.

The proof is very similar the the characterization of the GCD. We let a and b be nonzero integers.

Finishing the LCM

We now prove a characterization of the LCM which is the analog to the characterization of the GCD.

Theorem (Characterization of the LCM)

Let a and b be nonzero integers, and let m be an integer. Then $m = \operatorname{lcm}(a, b)$ if and only if the following hold:

1. $m > 0$,
2. $a|m$ *and* $b|m$, *and*
3. *for every integer x: if $a|x$ and $b|x$, then $m|x$.*

Proof.

The proof is very similar the the characterization of the GCD. We let a and b be nonzero integers. First, we show that $\operatorname{lcm}(a, b)$ satisfies 1.-3. above.

Finishing the LCM

We now prove a characterization of the LCM which is the analog to the characterization of the GCD.

Theorem (Characterization of the LCM)

Let a and b be nonzero integers, and let m be an integer. Then $m = \operatorname{lcm}(a, b)$ if and only if the following hold:

1. $m > 0$,
2. $a|m$ *and* $b|m$, *and*
3. *for every integer x: if $a|x$ and $b|x$, then $m|x$.*

Proof.

The proof is very similar the the characterization of the GCD. We let a and b be nonzero integers. First, we show that $\operatorname{lcm}(a, b)$ satisfies 1.-3. above. Toward this end, Let $S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$.

Finishing the LCM

We now prove a characterization of the LCM which is the analog to the characterization of the GCD.

Theorem (Characterization of the LCM)

Let a and b be nonzero integers, and let m be an integer. Then $m = \operatorname{lcm}(a, b)$ if and only if the following hold:

1. $m > 0$,
2. $a|m$ *and* $b|m$, *and*
3. *for every integer x: if $a|x$ and $b|x$, then $m|x$.*

Proof.

The proof is very similar the the characterization of the GCD. We let a and b be nonzero integers. First, we show that $\operatorname{lcm}(a, b)$ satisfies 1.-3. above. Toward this end, Let $S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$. We make several claims.

Finishing the LCM

We now prove a characterization of the LCM which is the analog to the characterization of the GCD.

Theorem (Characterization of the LCM)

Let a and b be nonzero integers, and let m be an integer. Then $m = \operatorname{lcm}(a, b)$ if and only if the following hold:

1. $m > 0$,
2. $a|m$ *and* $b|m$, *and*
3. *for every integer* x: *if* $a|x$ *and* $b|x$, *then* $m|x$.

Proof.

The proof is very similar the the characterization of the GCD. We let a and b be nonzero integers. First, we show that $\operatorname{lcm}(a, b)$ satisfies 1.-3. above. Toward this end, Let $S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$. We make several claims. □

Finishing the LCM

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$.

Finishing the LCM

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$.

Proof.

(0) S is contains a positive integer:

Finishing the LCM

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$.

Proof.

(0) S is contains a positive integer: recall that we proved that $a||ab|$ and $b||ab|$ and $|ab|$ is a positive integer.

Finishing the LCM

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$.

Proof.

(0) S is contains a positive integer: recall that we proved that $a||ab|$ and $b||ab|$ and $|ab|$ is a positive integer. Thus $|ab|$ is a positive integer which is a member of S.

Finishing the LCM

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$.

Proof.

(0) S is contains a positive integer: recall that we proved that $a||ab|$ and $b||ab|$ and $|ab|$ is a positive integer. Thus $|ab|$ is a positive integer which is a member of S.

(1) S is closed under addition:

Finishing the LCM

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$.

Proof.

(0) S is contains a positive integer: recall that we proved that $a||ab|$ and $b||ab|$ and $|ab|$ is a positive integer. Thus $|ab|$ is a positive integer which is a member of S.

(1) S is closed under addition: suppose that $x, y \in S$.

Finishing the LCM

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$.

Proof.

(0) S is contains a positive integer: recall that we proved that $a||ab|$ and $b||ab|$ and $|ab|$ is a positive integer. Thus $|ab|$ is a positive integer which is a member of S.

(1) S is closed under addition: suppose that $x, y \in S$. We will show that $x + y \in S$.

Finishing the LCM

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$.

Proof.

(0) S is contains a positive integer: recall that we proved that $a||ab|$ and $b||ab|$ and $|ab|$ is a positive integer. Thus $|ab|$ is a positive integer which is a member of S.

(1) S is closed under addition: suppose that $x, y \in S$. We will show that $x + y \in S$. Since $x \in S$, $a|x$ and $b|x$.

Finishing the LCM

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$.

Proof.

(0) S is contains a positive integer: recall that we proved that $a||ab|$ and $b||ab|$ and $|ab|$ is a positive integer. Thus $|ab|$ is a positive integer which is a member of S.

(1) S is closed under addition: suppose that $x, y \in S$. We will show that $x + y \in S$. Since $x \in S$, $a|x$ and $b|x$. So $au = x$ and $bv = x$ for some integers u and v.

Finishing the LCM

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$.

Proof.

(0) S is contains a positive integer: recall that we proved that $a||ab|$ and $b||ab|$ and $|ab|$ is a positive integer. Thus $|ab|$ is a positive integer which is a member of S.

(1) S is closed under addition: suppose that $x, y \in S$. We will show that $x + y \in S$. Since $x \in S$, $a|x$ and $b|x$. So $au = x$ and $bv = x$ for some integers u and v. Since $y \in S$, $a|y$ and $b|y$.

Finishing the LCM

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$.

Proof.

(0) S is contains a positive integer: recall that we proved that $a||ab|$ and $b||ab|$ and $|ab|$ is a positive integer. Thus $|ab|$ is a positive integer which is a member of S.

(1) S is closed under addition: suppose that $x, y \in S$. We will show that $x + y \in S$. Since $x \in S$, $a|x$ and $b|x$. So $au = x$ and $bv = x$ for some integers u and v. Since $y \in S$, $a|y$ and $b|y$. So $af = y$ and $bg = y$ for some integers f and g. Hence $x + y = au + af = a(u + f)$, and this shows that $a|x + y$.

Finishing the LCM

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$.

Proof.

(0) S is contains a positive integer: recall that we proved that $a||ab|$ and $b||ab|$ and $|ab|$ is a positive integer. Thus $|ab|$ is a positive integer which is a member of S.

(1) S is closed under addition: suppose that $x, y \in S$. We will show that $x + y \in S$. Since $x \in S$, $a|x$ and $b|x$. So $au = x$ and $bv = x$ for some integers u and v. Since $y \in S$, $a|y$ and $b|y$. So $af = y$ and $bg = y$ for some integers f and g. Hence $x + y = au + af = a(u + f)$, and this shows that $a|x + y$. Similarly, $x + y = bv + bg = b(v + g)$, and so $b|x + y$. This proves that $x + y \in S$.

Finishing the LCM

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$.

Proof.

(0) S is contains a positive integer: recall that we proved that $a||ab|$ and $b||ab|$ and $|ab|$ is a positive integer. Thus $|ab|$ is a positive integer which is a member of S.

(1) S is closed under addition: suppose that $x, y \in S$. We will show that $x + y \in S$. Since $x \in S$, $a|x$ and $b|x$. So $au = x$ and $bv = x$ for some integers u and v. Since $y \in S$, $a|y$ and $b|y$. So $af = y$ and $bg = y$ for some integers f and g. Hence $x + y = au + af = a(u + f)$, and this shows that $a|x + y$. Similarly, $x + y = bv + bg = b(v + g)$, and so $b|x + y$. This proves that $x + y \in S$.

Finishing the LCM

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$.

Proof.

(2) S 'absorbs products': let $x \in S$ and let $n \in \mathbb{Z}$.

Finishing the LCM

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$.

Proof.

(2) S 'absorbs products': let $x \in S$ and let $n \in \mathbb{Z}$. We will show that $nx \in S$. Since $x \in S$, $a|x$ and $b|x$.

Finishing the LCM

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$.

Proof.

(2) S 'absorbs products': let $x \in S$ and let $n \in \mathbb{Z}$. We will show that $nx \in S$. Since $x \in S$, $a|x$ and $b|x$. Thus $au = x$ and $bv = x$ for some integers u and v. Thus $aun = nx$ and $bvn = nx$, and it follows that both a and b divide nx, showing that $nx \in S$.

Finishing the LCM

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$.

Proof.

(2) S 'absorbs products': let $x \in S$ and let $n \in \mathbb{Z}$. We will show that $nx \in S$. Since $x \in S$, $a|x$ and $b|x$. Thus $au = x$ and $bv = x$ for some integers u and v. Thus $aun = nx$ and $bvn = nx$, and it follows that both a and b divide nx, showing that $nx \in S$.

(3) By (0), S has at least one positive integer; let m denote the least positive integer in S.

Finishing the LCM

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$.

Proof.

(2) S 'absorbs products': let $x \in S$ and let $n \in \mathbb{Z}$. We will show that $nx \in S$. Since $x \in S$, $a|x$ and $b|x$. Thus $au = x$ and $bv = x$ for some integers u and v. Thus $aun = nx$ and $bvn = nx$, and it follows that both a and b divide nx, showing that $nx \in S$.

(3) By (0), S has at least one positive integer; let m denote the least positive integer in S. We will show that every member of S is a multiple of m.

Finishing the LCM

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$.

Proof.

(2) S 'absorbs products': let $x \in S$ and let $n \in \mathbb{Z}$. We will show that $nx \in S$. Since $x \in S$, $a|x$ and $b|x$. Thus $au = x$ and $bv = x$ for some integers u and v. Thus $aun = nx$ and $bvn = nx$, and it follows that both a and b divide nx, showing that $nx \in S$.

(3) By (0), S has at least one positive integer; let m denote the least positive integer in S. We will show that every member of S is a multiple of m. So let $x \in S$ be arbitrary; by the D.A., $x = mq + r$ for some integers q and r such that $0 \leq r < m$.

Finishing the LCM

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$.

Proof.

(2) S 'absorbs products': let $x \in S$ and let $n \in \mathbb{Z}$. We will show that $nx \in S$. Since $x \in S$, $a|x$ and $b|x$. Thus $au = x$ and $bv = x$ for some integers u and v. Thus $aun = nx$ and $bvn = nx$, and it follows that both a and b divide nx, showing that $nx \in S$.

(3) By (0), S has at least one positive integer; let m denote the least positive integer in S. We will show that every member of S is a multiple of m. So let $x \in S$ be arbitrary; by the D.A., $x = mq + r$ for some integers q and r such that $0 \leq r < m$. Now $r = x - mq = x + (-q)m \in S$ by (1) and (2).

Finishing the LCM

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$.

Proof.

(2) S 'absorbs products': let $x \in S$ and let $n \in \mathbb{Z}$. We will show that $nx \in S$. Since $x \in S$, $a|x$ and $b|x$. Thus $au = x$ and $bv = x$ for some integers u and v. Thus $aun = nx$ and $bvn = nx$, and it follows that both a and b divide nx, showing that $nx \in S$.

(3) By (0), S has at least one positive integer; let m denote the least positive integer in S. We will show that every member of S is a multiple of m. So let $x \in S$ be arbitrary; by the D.A., $x = mq + r$ for some integers q and r such that $0 \leq r < m$. Now $r = x - mq = x + (-q)m \in S$ by (1) and (2). If $r \neq 0$, then r would be a SMALLER positive element of S than the LEAST positive member m of S, a contradiction.

Finishing the LCM

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$.

Proof.

(2) S 'absorbs products': let $x \in S$ and let $n \in \mathbb{Z}$. We will show that $nx \in S$. Since $x \in S$, $a|x$ and $b|x$. Thus $au = x$ and $bv = x$ for some integers u and v. Thus $aun = nx$ and $bvn = nx$, and it follows that both a and b divide nx, showing that $nx \in S$.

(3) By (0), S has at least one positive integer; let m denote the least positive integer in S. We will show that every member of S is a multiple of m. So let $x \in S$ be arbitrary; by the D.A., $x = mq + r$ for some integers q and r such that $0 \leq r < m$. Now $r = x - mq = x + (-q)m \in S$ by (1) and (2). If $r \neq 0$, then r would be a SMALLER positive element of S than the LEAST positive member m of S, a contradiction.

Finishing the LCM

Proof.

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$. We have shown that the least positive element m of S has the property that

$$m|x \text{ for every integer } x \in S.$$

Finishing the LCM

Proof.

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$. We have shown that the least positive element m of S has the property that

$$m|x \text{ for every integer } x \in S.$$

So $m > 0$, and since $m \in S$, we see that $a|m$ and $b|m$.

Finishing the LCM

Proof.

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$. We have shown that the least positive element m of S has the property that

$$m|x \text{ for every integer } x \in S.$$

So $m > 0$, and since $m \in S$, we see that $a|m$ and $b|m$. Now let x be any integer and suppose that $a|x$ and $b|x$.

Finishing the LCM

Proof.

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$. We have shown that the least positive element m of S has the property that

$$m|x \text{ for every integer } x \in S.$$

So $m > 0$, and since $m \in S$, we see that $a|m$ and $b|m$. Now let x be any integer and suppose that $a|x$ and $b|x$. Then $x \in S$, and so from above, $m|x$.

Finishing the LCM

Proof.

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$. We have shown that the least positive element m of S has the property that

$$m|x \text{ for every integer } x \in S.$$

So $m > 0$, and since $m \in S$, we see that $a|m$ and $b|m$. Now let x be any integer and suppose that $a|x$ and $b|x$. Then $x \in S$, and so from above, $m|x$. This proves that m satisfies 1. - 3. of the theorem.

Finishing the LCM

Proof.

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$. We have shown that the least positive element m of S has the property that

$$m|x \text{ for every integer } x \in S.$$

So $m > 0$, and since $m \in S$, we see that $a|m$ and $b|m$. Now let x be any integer and suppose that $a|x$ and $b|x$. Then $x \in S$, and so from above, $m|x$. This proves that m satisfies 1. - 3. of the theorem. It is immediate that $m = \text{lcm}(a, b)$, since we know that $m > 0$, $a|m$ and $b|m$, and we can see that m is the LEAST positive multiple of a and b as follows:

Finishing the LCM

Proof.

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$. We have shown that the least positive element m of S has the property that

$$m|x \text{ for every integer } x \in S.$$

So $m > 0$, and since $m \in S$, we see that $a|m$ and $b|m$. Now let x be any integer and suppose that $a|x$ and $b|x$. Then $x \in S$, and so from above, $m|x$. This proves that m satisfies 1. - 3. of the theorem. It is immediate that $m = \text{lcm}(a, b)$, since we know that $m > 0$, $a|m$ and $b|m$, and we can see that m is the LEAST positive multiple of a and b as follows: suppose that x is a positive integer and $a|x$ and $b|x$.

Finishing the LCM

Proof.

$S = \{x \in \mathbb{Z} : a|x \text{ and } b|x\}$. We have shown that the least positive element m of S has the property that

$$m|x \text{ for every integer } x \in S.$$

So $m > 0$, and since $m \in S$, we see that $a|m$ and $b|m$. Now let x be any integer and suppose that $a|x$ and $b|x$. Then $x \in S$, and so from above, $m|x$. This proves that m satisfies 1. - 3. of the theorem. It is immediate that $m = \text{lcm}(a, b)$, since we know that $m > 0$, $a|m$ and $b|m$, and we can see that m is the LEAST positive multiple of a and b as follows: suppose that x is a positive integer and $a|x$ and $b|x$. Then by 3., $m|x$, and so $m \leq x$, showing the leastness of m.

Finishing the LCM

Proof.

$S = \{x \in \mathbb{Z}: a|x \text{ and } b|x\}$. We have shown that the least positive element m of S has the property that

$$m|x \text{ for every integer } x \in S.$$

So $m > 0$, and since $m \in S$, we see that $a|m$ and $b|m$. Now let x be any integer and suppose that $a|x$ and $b|x$. Then $x \in S$, and so from above, $m|x$. This proves that m satisfies 1. - 3. of the theorem. It is immediate that $m = \text{lcm}(a, b)$, since we know that $m > 0$, $a|m$ and $b|m$, and we can see that m is the LEAST positive multiple of a and b as follows: suppose that x is a positive integer and $a|x$ and $b|x$. Then by 3., $m|x$, and so $m \leq x$, showing the leastness of m. This also shows that if m is any integer satisfying 1. - 3. of the theorem, then $m = \text{lcm}(a, b)$, and the proof is complete. □

Finishing the LCM

Example

Let a, b, and c be integers.

Finishing the LCM

Example

Let a, b, and c be integers. Suppose that $\gcd(a, b) = \gcd(a, c) = 1$.

Finishing the LCM

Example

Let a, b, and c be integers. Suppose that $\gcd(a, b) = \gcd(a, c) = 1$. Prove that $\gcd(a, bc) = 1$.

Finishing the LCM

Example

Let a, b, and c be integers. Suppose that $\gcd(a, b) = \gcd(a, c) = 1$. Prove that $\gcd(a, bc) = 1$.

Proof.

Let a, b, and c be integers, and suppose that $\gcd(a, b) = \gcd(a, c) = 1$.

Finishing the LCM

Example

Let a, b, and c be integers. Suppose that $\gcd(a, b) = \gcd(a, c) = 1$. Prove that $\gcd(a, bc) = 1$.

Proof.

Let a, b, and c be integers, and suppose that $\gcd(a, b) = \gcd(a, c) = 1$. We will prove that $\gcd(a, bc) = 1$.

Finishing the LCM

Example

Let a, b, and c be integers. Suppose that $\gcd(a, b) = \gcd(a, c) = 1$. Prove that $\gcd(a, bc) = 1$.

Proof.

Let a, b, and c be integers, and suppose that $\gcd(a, b) = \gcd(a, c) = 1$. We will prove that $\gcd(a, bc) = 1$. Toward this end, $ax + by = 1$ and $au + cv = 1$ for some $x, y, u, v \in \mathbb{Z}$.

Finishing the LCM

Example

Let a, b, and c be integers. Suppose that $\gcd(a, b) = \gcd(a, c) = 1$. Prove that $\gcd(a, bc) = 1$.

Proof.

Let a, b, and c be integers, and suppose that $\gcd(a, b) = \gcd(a, c) = 1$. We will prove that $\gcd(a, bc) = 1$. Toward this end, $ax + by = 1$ and $au + cv = 1$ for some $x, y, u, v \in \mathbb{Z}$. Now multiply these equations together to get $axau + axcv + byau + bycv = 1$, that is, $a(axu + xcv + byu) + bc(yv) = 1$.

Finishing the LCM

Example

Let a, b, and c be integers. Suppose that $\gcd(a, b) = \gcd(a, c) = 1$. Prove that $\gcd(a, bc) = 1$.

Proof.

Let a, b, and c be integers, and suppose that $\gcd(a, b) = \gcd(a, c) = 1$. We will prove that $\gcd(a, bc) = 1$. Toward this end, $ax + by = 1$ and $au + cv = 1$ for some $x, y, u, v \in \mathbb{Z}$. Now multiply these equations together to get $axau + axcv + byau + bycv = 1$, that is, $a(axu + xcv + byu) + bc(yv) = 1$. This proves that $\gcd(a, bc) = 1$, as desired. □

Finishing the LCM

Example

Prove that the following are equivalent for positive integers a and b:

Finishing the LCM

Example

Prove that the following are equivalent for positive integers a and b:

1. $a|b$,

Finishing the LCM

Example

Prove that the following are equivalent for positive integers a and b:

1. $a|b$,
2. $\gcd(a, b) = a$, and

Finishing the LCM

Example

Prove that the following are equivalent for positive integers a and b:

1. $a|b$,
2. $\gcd(a, b) = a$, and
3. $\operatorname{lcm}(a, b) = b$.

Finishing the LCM

Example

Prove that the following are equivalent for positive integers a and b:

1. $a|b$,
2. $\gcd(a, b) = a$, and
3. $\operatorname{lcm}(a, b) = b$.

Finishing the LCM

Example

Prove that the following are equivalent for positive integers a and b:

1. $a|b$,
2. $\gcd(a, b) = a$, and
3. $\operatorname{lcm}(a, b) = b$.

Proof.

Let a and b be positive integers.

1. implies 2.:

Finishing the LCM

Example

Prove that the following are equivalent for positive integers a and b:

1. $a|b$,
2. $\gcd(a, b) = a$, and
3. $\operatorname{lcm}(a, b) = b$.

Proof.

Let a and b be positive integers.

1. implies 2.: assume that $a|b$.

Finishing the LCM

Example

Prove that the following are equivalent for positive integers a and b:

1. $a|b$,
2. $\gcd(a, b) = a$, and
3. $\operatorname{lcm}(a, b) = b$.

Proof.

Let a and b be positive integers.

1. implies 2.: assume that $a|b$. We must show that $\gcd(a, b) = a$, that is a is the largest common divisor of a and b.

Finishing the LCM

Example

Prove that the following are equivalent for positive integers a and b:

1. $a|b$,
2. $\gcd(a, b) = a$, and
3. $\operatorname{lcm}(a, b) = b$.

Proof.

Let a and b be positive integers.

1. implies 2.: assume that $a|b$. We must show that $\gcd(a, b) = a$, that is a is the largest common divisor of a and b. Since $a \cdot 1 = a$, $a|a$.

Finishing the LCM

Example

Prove that the following are equivalent for positive integers a and b:

1. $a|b$,
2. $\gcd(a, b) = a$, and
3. $\operatorname{lcm}(a, b) = b$.

Proof.

Let a and b be positive integers.

1. implies 2.: assume that $a|b$. We must show that $\gcd(a, b) = a$, that is a is the largest common divisor of a and b. Since $a \cdot 1 = a$, $a|a$. It is given that $a|b$, and so a divides both a and b.

Finishing the LCM

Example

Prove that the following are equivalent for positive integers a and b:

1. $a|b$,
2. $\gcd(a, b) = a$, and
3. $\operatorname{lcm}(a, b) = b$.

Proof.

Let a and b be positive integers.

1. implies 2.: assume that $a|b$. We must show that $\gcd(a, b) = a$, that is a is the largest common divisor of a and b. Since $a \cdot 1 = a$, $a|a$. It is given that $a|b$, and so a divides both a and b. It remains to show that a is the largest common divisor of a and b.

Finishing the LCM

Example

Prove that the following are equivalent for positive integers a and b:

1. $a|b$,
2. $\gcd(a, b) = a$, and
3. $\operatorname{lcm}(a, b) = b$.

Proof.

Let a and b be positive integers.

1. implies 2.: assume that $a|b$. We must show that $\gcd(a, b) = a$, that is a is the largest common divisor of a and b. Since $a \cdot 1 = a$, $a|a$. It is given that $a|b$, and so a divides both a and b. It remains to show that a is the largest common divisor of a and b. Suppose by way of contradiction that $x \in \mathbb{Z}$, $x > a$, and $x|a, x|b$.

Finishing the LCM

Example

Prove that the following are equivalent for positive integers a and b:

1. $a|b$,
2. $\gcd(a, b) = a$, and
3. $\text{lcm}(a, b) = b$.

Proof.

Let a and b be positive integers.

1. implies 2.: assume that $a|b$. We must show that $\gcd(a, b) = a$, that is a is the largest common divisor of a and b. Since $a \cdot 1 = a$, $a|a$. It is given that $a|b$, and so a divides both a and b. It remains to show that a is the largest common divisor of a and b. Suppose by way of contradiction that $x \in \mathbb{Z}$, $x > a$, and $x|a, x|b$. Since $x > a$ and a is positive, x is positive, as is a. Since $x|a$, $x \leq a$, and this is a contradiction. $\square$

Finishing the LCM

Proof.

2. implies 3.:

Finishing the LCM

Proof.

2. implies 3.: assume that $\gcd(a, b) = a$.

Finishing the LCM

Proof.

2. implies 3.: assume that $\gcd(a, b) = a$. We must show that $\mathrm{lcm}(a, b) = b$.

Finishing the LCM

Proof.

2. implies 3.: assume that $\gcd(a, b) = a$. We must show that $\mathrm{lcm}(a, b) = b$. Recall from last lecture that $\gcd(a, b) \cdot \mathrm{lcm}(a, b) = ab$.

Finishing the LCM

Proof.

2. implies 3.: assume that $\gcd(a, b) = a$. We must show that $\operatorname{lcm}(a, b) = b$. Recall from last lecture that $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$. Since $\gcd(a, b) = a$, the previous equation becomes $a \cdot \operatorname{lcm}(a, b) = ab$.

Finishing the LCM

Proof.

2. implies 3.: assume that $\gcd(a, b) = a$. We must show that $\mathrm{lcm}(a, b) = b$. Recall from last lecture that $\gcd(a, b) \cdot \mathrm{lcm}(a, b) = ab$. Since $\gcd(a, b) = a$, the previous equation becomes $a \cdot \mathrm{lcm}(a, b) = ab$. Cancelling the a (how do we know that we can do this?), we get $\mathrm{lcm}(a, b) = b$.

Finishing the LCM

Proof.

2. implies 3.: assume that $\gcd(a, b) = a$. We must show that $\mathrm{lcm}(a, b) = b$. Recall from last lecture that $\gcd(a, b) \cdot \mathrm{lcm}(a, b) = ab$. Since $\gcd(a, b) = a$, the previous equation becomes $a \cdot \mathrm{lcm}(a, b) = ab$. Cancelling the a (how do we know that we can do this?), we get $\mathrm{lcm}(a, b) = b$.

3. implies 1.:

Finishing the LCM

Proof.

2. implies 3.: assume that $\gcd(a, b) = a$. We must show that $\mathrm{lcm}(a, b) = b$. Recall from last lecture that $\gcd(a, b) \cdot \mathrm{lcm}(a, b) = ab$. Since $\gcd(a, b) = a$, the previous equation becomes $a \cdot \mathrm{lcm}(a, b) = ab$. Cancelling the a (how do we know that we can do this?), we get $\mathrm{lcm}(a, b) = b$.

3. implies 1.: assume that $\mathrm{lcm}(a, b) = b$.

Finishing the LCM

Proof.

2. implies 3.: assume that $\gcd(a, b) = a$. We must show that $\mathrm{lcm}(a, b) = b$. Recall from last lecture that $\gcd(a, b) \cdot \mathrm{lcm}(a, b) = ab$. Since $\gcd(a, b) = a$, the previous equation becomes $a \cdot \mathrm{lcm}(a, b) = ab$. Cancelling the a (how do we know that we can do this?), we get $\mathrm{lcm}(a, b) = b$.

3. implies 1.: assume that $\mathrm{lcm}(a, b) = b$. We will show that $a|b$.

Finishing the LCM

Proof.

2. implies 3.: assume that $\gcd(a, b) = a$. We must show that $\mathrm{lcm}(a, b) = b$. Recall from last lecture that $\gcd(a, b) \cdot \mathrm{lcm}(a, b) = ab$. Since $\gcd(a, b) = a$, the previous equation becomes $a \cdot \mathrm{lcm}(a, b) = ab$. Cancelling the a (how do we know that we can do this?), we get $\mathrm{lcm}(a, b) = b$.

3. implies 1.: assume that $\mathrm{lcm}(a, b) = b$. We will show that $a|b$. This is immediate by the def., since we have $a|b$ and $b|b$, hence $a|b$. □

Intro to the Fundamental Theorem of Arithmetic

We are now ready to prove one of the most fundamental results in number theory, the so-called **Fundamental Theorem of Arithmetic** (statement forthcoming).

Intro to the Fundamental Theorem of Arithmetic

We are now ready to prove one of the most fundamental results in number theory, the so-called **Fundamental Theorem of Arithmetic** (statement forthcoming). First, we make the following important definition.

Intro to the Fundamental Theorem of Arithmetic

We are now ready to prove one of the most fundamental results in number theory, the so-called **Fundamental Theorem of Arithmetic** (statement forthcoming). First, we make the following important definition.

Definition

Let p be an integer.

Intro to the Fundamental Theorem of Arithmetic

We are now ready to prove one of the most fundamental results in number theory, the so-called **Fundamental Theorem of Arithmetic** (statement forthcoming). First, we make the following important definition.

Definition

Let p be an integer. Then we say that p is **prime** or a **prime number** if $p > 1$ and the only POSITIVE factors of p are 1 and p.

Intro to the Fundamental Theorem of Arithmetic

We are now ready to prove one of the most fundamental results in number theory, the so-called **Fundamental Theorem of Arithmetic** (statement forthcoming). First, we make the following important definition.

Definition

Let p be an integer. Then we say that p is **prime** or a **prime number** if $p > 1$ and the only POSITIVE factors of p are 1 and p. An integer $n > 1$ which is not prime is called **composite**.

Intro to the Fundamental Theorem of Arithmetic

We are now ready to prove one of the most fundamental results in number theory, the so-called **Fundamental Theorem of Arithmetic** (statement forthcoming). First, we make the following important definition.

Definition

Let p be an integer. Then we say that p is **prime** or a **prime number** if $p > 1$ and the only POSITIVE factors of p are 1 and p. An integer $n > 1$ which is not prime is called **composite**.

Example

The following hold:

1. 1 is NOT PRIME!

Intro to the Fundamental Theorem of Arithmetic

We are now ready to prove one of the most fundamental results in number theory, the so-called **Fundamental Theorem of Arithmetic** (statement forthcoming). First, we make the following important definition.

Definition

Let p be an integer. Then we say that p is **prime** or a **prime number** if $p > 1$ and the only POSITIVE factors of p are 1 and p. An integer $n > 1$ which is not prime is called **composite**.

Example

The following hold:

1. 1 is NOT PRIME!
2. 2 is prime

Intro to the Fundamental Theorem of Arithmetic

We are now ready to prove one of the most fundamental results in number theory, the so-called **Fundamental Theorem of Arithmetic** (statement forthcoming). First, we make the following important definition.

Definition

Let p be an integer. Then we say that p is **prime** or a **prime number** if $p > 1$ and the only POSITIVE factors of p are 1 and p. An integer $n > 1$ which is not prime is called **composite**.

Example

The following hold:

1. 1 is NOT PRIME!
2. 2 is prime
3. 3 is prime

Intro to the Fundamental Theorem of Arithmetic

We are now ready to prove one of the most fundamental results in number theory, the so-called **Fundamental Theorem of Arithmetic** (statement forthcoming). First, we make the following important definition.

Definition

Let p be an integer. Then we say that p is **prime** or a **prime number** if $p > 1$ and the only POSITIVE factors of p are 1 and p. An integer $n > 1$ which is not prime is called **composite**.

Example

The following hold:

1. 1 is NOT PRIME!
2. 2 is prime
3. 3 is prime
4. 5 is prime...

Intro to the Fundamental Theorem of Arithmetic

We are now ready to prove one of the most fundamental results in number theory, the so-called **Fundamental Theorem of Arithmetic** (statement forthcoming). First, we make the following important definition.

Definition

Let p be an integer. Then we say that p is **prime** or a **prime number** if $p > 1$ and the only POSITIVE factors of p are 1 and p. An integer $n > 1$ which is not prime is called **composite**.

Example

The following hold:

1. 1 is NOT PRIME!
2. 2 is prime
3. 3 is prime
4. 5 is prime...

Intro to the Fundamental Theorem of Arithmetic

Lemma

Let m be an integer.

Intro to the Fundamental Theorem of Arithmetic

Lemma

Let m be an integer. Then m is composite if and only if $m = rs$ for some integers r, s with $1 < r, s < m$.

Intro to the Fundamental Theorem of Arithmetic

Lemma

Let m be an integer. Then m is composite if and only if $m = rs$ for some integers r, s with $1 < r, s < m$.

Proof.

Let m be an integer.

Intro to the Fundamental Theorem of Arithmetic

Lemma

Let m be an integer. Then m is composite if and only if $m = rs$ for some integers r, s with $1 < r, s < m$.

Proof.

Let m be an integer. Assume first that m is composite. Then $m > 1$ and m is not prime.

Intro to the Fundamental Theorem of Arithmetic

Lemma

Let m be an integer. Then m is composite if and only if $m = rs$ for some integers r, s with $1 < r, s < m$.

Proof.

Let m be an integer. Assume first that m is composite. Then $m > 1$ and m is not prime. So it is NOT the case that the only positive factors of m are 1 and m.

Intro to the Fundamental Theorem of Arithmetic

Lemma

Let m be an integer. Then m is composite if and only if $m = rs$ for some integers r, s with $1 < r, s < m$.

Proof.

Let m be an integer. Assume first that m is composite. Then $m > 1$ and m is not prime. So it is NOT the case that the only positive factors of m are 1 and m. So there is a positive factor r of m which is different from 1 and m.

Intro to the Fundamental Theorem of Arithmetic

Lemma

Let m be an integer. Then m is composite if and only if $m = rs$ for some integers r, s with $1 < r, s < m$.

Proof.

Let m be an integer. Assume first that m is composite. Then $m > 1$ and m is not prime. So it is NOT the case that the only positive factors of m are 1 and m. So there is a positive factor r of m which is different from 1 and m. Since $r|m$ and r and m are POSITIVE, $r \leq m$.

Intro to the Fundamental Theorem of Arithmetic

Lemma

Let m be an integer. Then m is composite if and only if $m = rs$ for some integers r, s with $1 < r, s < m$.

Proof.

Let m be an integer. Assume first that m is composite. Then $m > 1$ and m is not prime. So it is NOT the case that the only positive factors of m are 1 and m. So there is a positive factor r of m which is different from 1 and m. Since $r|m$ and r and m are POSITIVE, $r \leq m$. Hence $1 < r < m$.

Intro to the Fundamental Theorem of Arithmetic

Lemma

Let m be an integer. Then m is composite if and only if $m = rs$ for some integers r, s with $1 < r, s < m$.

Proof.

Let m be an integer. Assume first that m is composite. Then $m > 1$ and m is not prime. So it is NOT the case that the only positive factors of m are 1 and m. So there is a positive factor r of m which is different from 1 and m. Since $r|m$ and r and m are POSITIVE, $r \leq m$. Hence $1 < r < m$. Also, there is an integer s such that $rs = m$, since $r|m$.

Intro to the Fundamental Theorem of Arithmetic

Lemma

Let m be an integer. Then m is composite if and only if $m = rs$ for some integers r, s with $1 < r, s < m$.

Proof.

Let m be an integer. Assume first that m is composite. Then $m > 1$ and m is not prime. So it is NOT the case that the only positive factors of m are 1 and m. So there is a positive factor r of m which is different from 1 and m. Since $r|m$ and r and m are POSITIVE, $r \leq m$. Hence $1 < r < m$. Also, there is an integer s such that $rs = m$, since $r|m$. Note that since $s = \frac{m}{r}$, s is positive.

Intro to the Fundamental Theorem of Arithmetic

Lemma

Let m be an integer. Then m is composite if and only if $m = rs$ for some integers r, s with $1 < r, s < m$.

Proof.

Let m be an integer. Assume first that m is composite. Then $m > 1$ and m is not prime. So it is NOT the case that the only positive factors of m are 1 and m. So there is a positive factor r of m which is different from 1 and m. Since $r|m$ and r and m are POSITIVE, $r \leq m$. Hence $1 < r < m$. Also, there is an integer s such that $rs = m$, since $r|m$. Note that since $s = \frac{m}{r}$, s is positive. Because $s|m$, also $s \leq m$.

Intro to the Fundamental Theorem of Arithmetic

Lemma

Let m be an integer. Then m is composite if and only if $m = rs$ for some integers r, s with $1 < r, s < m$.

Proof.

Let m be an integer. Assume first that m is composite. Then $m > 1$ and m is not prime. So it is NOT the case that the only positive factors of m are 1 and m. So there is a positive factor r of m which is different from 1 and m. Since $r|m$ and r and m are POSITIVE, $r \leq m$. Hence $1 < r < m$. Also, there is an integer s such that $rs = m$, since $r|m$. Note that since $s = \frac{m}{r}$, s is positive. Because $s|m$, also $s \leq m$. If $s = 1$, then $r = m$, a contradiction;

Intro to the Fundamental Theorem of Arithmetic

Lemma

Let m be an integer. Then m is composite if and only if $m = rs$ for some integers r, s with $1 < r, s < m$.

Proof.

Let m be an integer. Assume first that m is composite. Then $m > 1$ and m is not prime. So it is NOT the case that the only positive factors of m are 1 and m. So there is a positive factor r of m which is different from 1 and m. Since $r|m$ and r and m are POSITIVE, $r \leq m$. Hence $1 < r < m$. Also, there is an integer s such that $rs = m$, since $r|m$. Note that since $s = \frac{m}{r}$, s is positive. Because $s|m$, also $s \leq m$. If $s = 1$, then $r = m$, a contradiction; if $s = m$, then $r = 1$, which is also a contradiction.

Intro to the Fundamental Theorem of Arithmetic

Lemma

Let m be an integer. Then m is composite if and only if $m = rs$ for some integers r, s with $1 < r, s < m$.

Proof.

Let m be an integer. Assume first that m is composite. Then $m > 1$ and m is not prime. So it is NOT the case that the only positive factors of m are 1 and m. So there is a positive factor r of m which is different from 1 and m. Since $r|m$ and r and m are POSITIVE, $r \leq m$. Hence $1 < r < m$. Also, there is an integer s such that $rs = m$, since $r|m$. Note that since $s = \frac{m}{r}$, s is positive. Because $s|m$, also $s \leq m$. If $s = 1$, then $r = m$, a contradiction; if $s = m$, then $r = 1$, which is also a contradiction. Hence $1 < s < m$. □

Intro to the Fundamental Theorem of Arithmetic

Proof.

Now suppose that $m = rs$ for some integers r, s with $1 < r, s < m$.

Intro to the Fundamental Theorem of Arithmetic

Proof.

Now suppose that $m = rs$ for some integers r, s with $1 < r, s < m$. Then $m > 1$ and r is a positive factor of m different from 1 and m, so m is composite. $\square$

Intro to the Fundamental Theorem of Arithmetic

Example

Prove that every integer $n \geq 2$ is either prime or a product of two or more primes using the Principle of Strong Induction.

Intro to the Fundamental Theorem of Arithmetic

Example

Prove that every integer $n \geq 2$ is either prime or a product of two or more primes using the Principle of Strong Induction.

Proof.

Recall that we have a base case and an inductive step:

Intro to the Fundamental Theorem of Arithmetic

Example

Prove that every integer $n \geq 2$ is either prime or a product of two or more primes using the Principle of Strong Induction.

Proof.

Recall that we have a base case and an inductive step:

(i) (base case) We must show that 2 is either prime or a product of two or more primes.

Intro to the Fundamental Theorem of Arithmetic

Example

Prove that every integer $n \geq 2$ is either prime or a product of two or more primes using the Principle of Strong Induction.

Proof.

Recall that we have a base case and an inductive step:

(i) (base case) We must show that 2 is either prime or a product of two or more primes. This is clear since 2 is prime.

Intro to the Fundamental Theorem of Arithmetic

Example

Prove that every integer $n \geq 2$ is either prime or a product of two or more primes using the Principle of Strong Induction.

Proof.

Recall that we have a base case and an inductive step:

(i) (base case) We must show that 2 is either prime or a product of two or more primes. This is clear since 2 is prime.

(ii) (inductive step) Let $n \geq 2$ be an integer, and assume the claim holds for every integer m such that $2 \leq m \leq n$.

Intro to the Fundamental Theorem of Arithmetic

Example

Prove that every integer $n \geq 2$ is either prime or a product of two or more primes using the Principle of Strong Induction.

Proof.

Recall that we have a base case and an inductive step:

(i) (base case) We must show that 2 is either prime or a product of two or more primes. This is clear since 2 is prime.

(ii) (inductive step) Let $n \geq 2$ be an integer, and assume the claim holds for every integer m such that $2 \leq m \leq n$. We must show that $n + 1$ is prime or a product of two or more primes.

Intro to the Fundamental Theorem of Arithmetic

Example

Prove that every integer $n \geq 2$ is either prime or a product of two or more primes using the Principle of Strong Induction.

Proof.

Recall that we have a base case and an inductive step:

(i) (base case) We must show that 2 is either prime or a product of two or more primes. This is clear since 2 is prime.

(ii) (inductive step) Let $n \geq 2$ be an integer, and assume the claim holds for every integer m such that $2 \leq m \leq n$. We must show that $n+1$ is prime or a product of two or more primes. If $n+1$ is prime, we are done.

Intro to the Fundamental Theorem of Arithmetic

Example

Prove that every integer $n \geq 2$ is either prime or a product of two or more primes using the Principle of Strong Induction.

Proof.

Recall that we have a base case and an inductive step:

(i) (base case) We must show that 2 is either prime or a product of two or more primes. This is clear since 2 is prime.

(ii) (inductive step) Let $n \geq 2$ be an integer, and assume the claim holds for every integer m such that $2 \leq m \leq n$. We must show that $n+1$ is prime or a product of two or more primes. If $n+1$ is prime, we are done. So assume that $n+1$ is not prime.

Intro to the Fundamental Theorem of Arithmetic

Example

Prove that every integer $n \geq 2$ is either prime or a product of two or more primes using the Principle of Strong Induction.

Proof.

Recall that we have a base case and an inductive step:

(i) (base case) We must show that 2 is either prime or a product of two or more primes. This is clear since 2 is prime.

(ii) (inductive step) Let $n \geq 2$ be an integer, and assume the claim holds for every integer m such that $2 \leq m \leq n$. We must show that $n+1$ is prime or a product of two or more primes. If $n+1$ is prime, we are done. So assume that $n+1$ is not prime. Note that $n+1 > 1$ (why?).

Intro to the Fundamental Theorem of Arithmetic

Example

Prove that every integer $n \geq 2$ is either prime or a product of two or more primes using the Principle of Strong Induction.

Proof.

Recall that we have a base case and an inductive step:

(i) (base case) We must show that 2 is either prime or a product of two or more primes. This is clear since 2 is prime.

(ii) (inductive step) Let $n \geq 2$ be an integer, and assume the claim holds for every integer m such that $2 \leq m \leq n$. We must show that $n+1$ is prime or a product of two or more primes. If $n+1$ is prime, we are done. So assume that $n+1$ is not prime. Note that $n+1 > 1$ (why?). So by the lemma, $n+1 = rs$ for some integers r and s such that $1 < r, s < n+1$.

Intro to the Fundamental Theorem of Arithmetic

Example

Prove that every integer $n \geq 2$ is either prime or a product of two or more primes using the Principle of Strong Induction.

Proof.

Recall that we have a base case and an inductive step:

(i) (base case) We must show that 2 is either prime or a product of two or more primes. This is clear since 2 is prime.

(ii) (inductive step) Let $n \geq 2$ be an integer, and assume the claim holds for every integer m such that $2 \leq m \leq n$. We must show that $n+1$ is prime or a product of two or more primes. If $n+1$ is prime, we are done. So assume that $n+1$ is not prime. Note that $n+1 > 1$ (why?). So by the lemma, $n+1 = rs$ for some integers r and s such that $1 < r, s < n+1$. This means that $2 \leq r, s \leq n$.

Intro to the Fundamental Theorem of Arithmetic

Example

Prove that every integer $n \geq 2$ is either prime or a product of two or more primes using the Principle of Strong Induction.

Proof.

Recall that we have a base case and an inductive step:

(i) (base case) We must show that 2 is either prime or a product of two or more primes. This is clear since 2 is prime.

(ii) (inductive step) Let $n \geq 2$ be an integer, and assume the claim holds for every integer m such that $2 \leq m \leq n$. We must show that $n+1$ is prime or a product of two or more primes. If $n+1$ is prime, we are done. So assume that $n+1$ is not prime. Note that $n+1 > 1$ (why?). So by the lemma, $n+1 = rs$ for some integers r and s such that $1 < r, s < n+1$. This means that $2 \leq r, s \leq n$. So by the inductive hypothesis, r, s are either prime or the product of two or more primes, and hence $n+1 = rs$ is a product of two or more primes, and we are done. □