Math 3110 Lecture 15

Greg Oman

University of Colorado
Colorado Springs

Intro to Congruences

Definition

Recall that for integers a and b and a POSITIVE integer n, a **is congruent to** b **modulo** n, denoted $a \equiv b \pmod{n}$, provided $n|a-b$.

Intro to Congruences

Definition

Recall that for integers a and b and a POSITIVE integer n, a **is congruent to** b **modulo** n, denoted $a \equiv b \pmod{n}$, provided $n|a-b$.

Example

Verify the following:

Intro to Congruences

Definition

Recall that for integers a and b and a POSITIVE integer n, a **is congruent to** b **modulo** n, denoted $a \equiv b \pmod{n}$, provided $n|a-b$.

Example

Verify the following:

1. $15 \equiv 5 \pmod{5}$

Intro to Congruences

Definition

Recall that for integers a and b and a POSITIVE integer n, a **is congruent to** b **modulo** n, denoted $a \equiv b \pmod{n}$, provided $n|a-b$.

Example

Verify the following:

1. $15 \equiv 5 \pmod{5}$
2. $-32 \equiv 8 \pmod{10}$

Intro to Congruences

Definition

Recall that for integers a and b and a POSITIVE integer n, a **is congruent to** b **modulo** n, denoted $a \equiv b \pmod{n}$, provided $n|a-b$.

Example

Verify the following:

1. $15 \equiv 5 \pmod{5}$
2. $-32 \equiv 8 \pmod{10}$
3. $32 \equiv 5 \pmod{9}$

Intro to Congruences

Definition

Recall that for integers a and b and a POSITIVE integer n, a **is congruent to** b **modulo** n, denoted $a \equiv b \pmod{n}$, provided $n|a-b$.

Example

Verify the following:

1. $15 \equiv 5 \pmod{5}$
2. $-32 \equiv 8 \pmod{10}$
3. $32 \equiv 5 \pmod{9}$

Intro to Congruences

Definition

Recall that for integers a and b and a POSITIVE integer n, a **is congruent to** b **modulo** n, denoted $a \equiv b \pmod{n}$, provided $n|a-b$.

Example

Verify the following:

1. $15 \equiv 5 \pmod{5}$
2. $-32 \equiv 8 \pmod{10}$
3. $32 \equiv 5 \pmod{9}$

Intro to Congruences

Theorem (Characterization of Congruences Theorem)

Let n be a positive integer and let a and b be integers.

Intro to Congruences

Theorem (Characterization of Congruences Theorem)

Let n be a positive integer and let a and b be integers. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder upon division by n.

Intro to Congruences

Theorem (Characterization of Congruences Theorem)

Let n be a positive integer and let a and b be integers. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder upon division by n.

Proof.

Let n be a positive integer and let a and b be integers.

Intro to Congruences

Theorem (Characterization of Congruences Theorem)

Let n be a positive integer and let a and b be integers. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder upon division by n.

Proof.

Let n be a positive integer and let a and b be integers. Assume first that $a \equiv b \pmod{n}$.

Intro to Congruences

Theorem (Characterization of Congruences Theorem)

Let n be a positive integer and let a and b be integers. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder upon division by n.

Proof.

Let n be a positive integer and let a and b be integers. Assume first that $a \equiv b \pmod{n}$. Then by definition, $n|a - b$.

Intro to Congruences

Theorem (Characterization of Congruences Theorem)

Let n be a positive integer and let a and b be integers. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder upon division by n.

Proof.

Let n be a positive integer and let a and b be integers. Assume first that $a \equiv b \pmod{n}$. Then by definition, $n|a-b$. Write $a = nq_1 + r_1$ and $b = nq_2 + r_2$, where q_1, q_2, r_1, r_2 are integers and $0 \leq r_1, r_2 < n$.

Intro to Congruences

Theorem (Characterization of Congruences Theorem)

Let n be a positive integer and let a and b be integers. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder upon division by n.

Proof.

Let n be a positive integer and let a and b be integers. Assume first that $a \equiv b \pmod{n}$. Then by definition, $n|a-b$. Write $a = nq_1 + r_1$ and $b = nq_2 + r_2$, where q_1, q_2, r_1, r_2 are integers and $0 \leq r_1, r_2 < n$. We must show that $r_1 = r_2$.

Intro to Congruences

Theorem (Characterization of Congruences Theorem)

Let n be a positive integer and let a and b be integers. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder upon division by n.

Proof.

Let n be a positive integer and let a and b be integers. Assume first that $a \equiv b \pmod{n}$. Then by definition, $n|a-b$. Write $a = nq_1 + r_1$ and $b = nq_2 + r_2$, where q_1, q_2, r_1, r_2 are integers and $0 \leq r_1, r_2 < n$. We must show that $r_1 = r_2$. Suppose not.

Intro to Congruences

Theorem (Characterization of Congruences Theorem)

Let n be a positive integer and let a and b be integers. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder upon division by n.

Proof.

Let n be a positive integer and let a and b be integers. Assume first that $a \equiv b \pmod{n}$. Then by definition, $n|a-b$. Write $a = nq_1 + r_1$ and $b = nq_2 + r_2$, where q_1, q_2, r_1, r_2 are integers and $0 \leq r_1, r_2 < n$. We must show that $r_1 = r_2$. Suppose not. Then we may suppose without loss of generality that $r_1 > r_2$.

Intro to Congruences

Theorem (Characterization of Congruences Theorem)

Let n be a positive integer and let a and b be integers. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder upon division by n.

Proof.

Let n be a positive integer and let a and b be integers. Assume first that $a \equiv b \pmod{n}$. Then by definition, $n|a-b$. Write $a = nq_1 + r_1$ and $b = nq_2 + r_2$, where q_1, q_2, r_1, r_2 are integers and $0 \leq r_1, r_2 < n$. We must show that $r_1 = r_2$. Suppose not. Then we may suppose without loss of generality that $r_1 > r_2$. Now, $n|a-b$ and thus $n|(nq_1 + r_1) - (nq_2 + r_2)$.

Intro to Congruences

Theorem (Characterization of Congruences Theorem)

Let n be a positive integer and let a and b be integers. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder upon division by n.

Proof.

Let n be a positive integer and let a and b be integers. Assume first that $a \equiv b \pmod{n}$. Then by definition, $n|a-b$. Write $a = nq_1 + r_1$ and $b = nq_2 + r_2$, where q_1, q_2, r_1, r_2 are integers and $0 \leq r_1, r_2 < n$. We must show that $r_1 = r_2$. Suppose not. Then we may suppose without loss of generality that $r_1 > r_2$. Now, $n|a-b$ and thus $n|(nq_1 + r_1) - (nq_2 + r_2)$. Hence there is an integer x such that
$nx = (nq_1 + r_1) - (nq_2 + r_2) = nq_1 - nq_2 + r_1 - r_2$.

Intro to Congruences

Theorem (Characterization of Congruences Theorem)

Let n be a positive integer and let a and b be integers. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder upon division by n.

Proof.

Let n be a positive integer and let a and b be integers. Assume first that $a \equiv b \pmod{n}$. Then by definition, $n|a-b$. Write $a = nq_1 + r_1$ and $b = nq_2 + r_2$, where q_1, q_2, r_1, r_2 are integers and $0 \leq r_1, r_2 < n$. We must show that $r_1 = r_2$. Suppose not. Then we may suppose without loss of generality that $r_1 > r_2$. Now, $n|a-b$ and thus $n|(nq_1 + r_1) - (nq_2 + r_2)$. Hence there is an integer x such that
$nx = (nq_1 + r_1) - (nq_2 + r_2) = nq_1 - nq_2 + r_1 - r_2$. But then
$nx - nq_1 + nq_2 = r_1 - r_2$.

Intro to Congruences

Theorem (Characterization of Congruences Theorem)

Let n be a positive integer and let a and b be integers. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder upon division by n.

Proof.

Let n be a positive integer and let a and b be integers. Assume first that $a \equiv b \pmod{n}$. Then by definition, $n|a-b$. Write $a = nq_1 + r_1$ and $b = nq_2 + r_2$, where q_1, q_2, r_1, r_2 are integers and $0 \leq r_1, r_2 < n$. We must show that $r_1 = r_2$. Suppose not. Then we may suppose without loss of generality that $r_1 > r_2$. Now, $n|a-b$ and thus $n|(nq_1 + r_1) - (nq_2 + r_2)$. Hence there is an integer x such that $nx = (nq_1 + r_1) - (nq_2 + r_2) = nq_1 - nq_2 + r_1 - r_2$. But then $nx - nq_1 + nq_2 = r_1 - r_2$. Factoring out the n on the left, $n|r_1 - r_2$.

Intro to Congruences

Theorem (Characterization of Congruences Theorem)

Let n be a positive integer and let a and b be integers. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder upon division by n.

Proof.

Let n be a positive integer and let a and b be integers. Assume first that $a \equiv b \pmod{n}$. Then by definition, $n|a-b$. Write $a = nq_1 + r_1$ and $b = nq_2 + r_2$, where q_1, q_2, r_1, r_2 are integers and $0 \leq r_1, r_2 < n$. We must show that $r_1 = r_2$. Suppose not. Then we may suppose without loss of generality that $r_1 > r_2$. Now, $n|a-b$ and thus $n|(nq_1 + r_1) - (nq_2 + r_2)$. Hence there is an integer x such that $nx = (nq_1 + r_1) - (nq_2 + r_2) = nq_1 - nq_2 + r_1 - r_2$. But then $nx - nq_1 + nq_2 = r_1 - r_2$. Factoring out the n on the left, $n|r_1 - r_2$. By the Divisibility Theorem, it follows that $n \leq r_1 - r_2$.

Intro to Congruences

Theorem (Characterization of Congruences Theorem)

Let n be a positive integer and let a and b be integers. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder upon division by n.

Proof.

Let n be a positive integer and let a and b be integers. Assume first that $a \equiv b \pmod{n}$. Then by definition, $n|a-b$. Write $a = nq_1 + r_1$ and $b = nq_2 + r_2$, where q_1, q_2, r_1, r_2 are integers and $0 \leq r_1, r_2 < n$. We must show that $r_1 = r_2$. Suppose not. Then we may suppose without loss of generality that $r_1 > r_2$. Now, $n|a-b$ and thus $n|(nq_1 + r_1) - (nq_2 + r_2)$. Hence there is an integer x such that $nx = (nq_1 + r_1) - (nq_2 + r_2) = nq_1 - nq_2 + r_1 - r_2$. But then $nx - nq_1 + nq_2 = r_1 - r_2$. Factoring out the n on the left, $n|r_1 - r_2$. By the Divisibility Theorem, it follows that $n \leq r_1 - r_2$. But recall above that $0 \leq r_1, r_2 < n$.

Intro to Congruences

Theorem (Characterization of Congruences Theorem)

Let n be a positive integer and let a and b be integers. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder upon division by n.

Proof.

Let n be a positive integer and let a and b be integers. Assume first that $a \equiv b \pmod{n}$. Then by definition, $n|a-b$. Write $a = nq_1 + r_1$ and $b = nq_2 + r_2$, where q_1, q_2, r_1, r_2 are integers and $0 \leq r_1, r_2 < n$. We must show that $r_1 = r_2$. Suppose not. Then we may suppose without loss of generality that $r_1 > r_2$. Now, $n|a-b$ and thus $n|(nq_1 + r_1) - (nq_2 + r_2)$. Hence there is an integer x such that $nx = (nq_1 + r_1) - (nq_2 + r_2) = nq_1 - nq_2 + r_1 - r_2$. But then $nx - nq_1 + nq_2 = r_1 - r_2$. Factoring out the n on the left, $n|r_1 - r_2$. By the Divisibility Theorem, it follows that $n \leq r_1 - r_2$. But recall above that $0 \leq r_1, r_2 < n$. Thus (since $r_1 > r_2$ in addition (see above)), we have $0 < r_1 - r_2 < n$, hence $n > r_1 - r_2$, and this contradicts $n \leq r_1 - r_2$.

Intro to Congruences

Theorem (Characterization of Congruences Theorem)

Let n be a positive integer and let a and b be integers. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder upon division by n.

Proof.

Let n be a positive integer and let a and b be integers. Assume first that $a \equiv b \pmod{n}$. Then by definition, $n|a-b$. Write $a = nq_1 + r_1$ and $b = nq_2 + r_2$, where q_1, q_2, r_1, r_2 are integers and $0 \leq r_1, r_2 < n$. We must show that $r_1 = r_2$. Suppose not. Then we may suppose without loss of generality that $r_1 > r_2$. Now, $n|a-b$ and thus $n|(nq_1 + r_1) - (nq_2 + r_2)$. Hence there is an integer x such that $nx = (nq_1 + r_1) - (nq_2 + r_2) = nq_1 - nq_2 + r_1 - r_2$. But then $nx - nq_1 + nq_2 = r_1 - r_2$. Factoring out the n on the left, $n|r_1 - r_2$. By the Divisibility Theorem, it follows that $n \leq r_1 - r_2$. But recall above that $0 \leq r_1, r_2 < n$. Thus (since $r_1 > r_2$ in addition (see above)), we have $0 < r_1 - r_2 < n$, hence $n > r_1 - r_2$, and this contradicts $n \leq r_1 - r_2$. This proves the first implication.

Intro to Congruences

Theorem (Characterization of Congruences Theorem)

Let n be a positive integer and let a and b be integers. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder upon division by n.

Proof.

Let n be a positive integer and let a and b be integers. Assume first that $a \equiv b \pmod{n}$. Then by definition, $n|a-b$. Write $a = nq_1 + r_1$ and $b = nq_2 + r_2$, where q_1, q_2, r_1, r_2 are integers and $0 \leq r_1, r_2 < n$. We must show that $r_1 = r_2$. Suppose not. Then we may suppose without loss of generality that $r_1 > r_2$. Now, $n|a-b$ and thus $n|(nq_1 + r_1) - (nq_2 + r_2)$. Hence there is an integer x such that $nx = (nq_1 + r_1) - (nq_2 + r_2) = nq_1 - nq_2 + r_1 - r_2$. But then $nx - nq_1 + nq_2 = r_1 - r_2$. Factoring out the n on the left, $n|r_1 - r_2$. By the Divisibility Theorem, it follows that $n \leq r_1 - r_2$. But recall above that $0 \leq r_1, r_2 < n$. Thus (since $r_1 > r_2$ in addition (see above)), we have $0 < r_1 - r_2 < n$, hence $n > r_1 - r_2$, and this contradicts $n \leq r_1 - r_2$. This proves the first implication. □

Proof.

As for the second, assume now that a and b have the same remainder upon division by n.

Proof.

As for the second, assume now that a and b have the same remainder upon division by n. Then we see that $a = ny_1 + r$ and $b = ny_2 + r$ for some integers y_1, y_2, r such that $0 \leq r < n$.

Intro to Congruences

Proof.

As for the second, assume now that a and b have the same remainder upon division by n. Then we see that $a = ny_1 + r$ and $b = ny_2 + r$ for some integers y_1, y_2, r such that $0 \leq r < n$. Then
$a - b = (ny_1 + r) - (ny_2 + r) = ny_1 - ny_2 = n(y_1 - y_2)$, which is clearly divisible by n.

Intro to Congruences

Proof.

As for the second, assume now that a and b have the same remainder upon division by n. Then we see that $a = ny_1 + r$ and $b = ny_2 + r$ for some integers y_1, y_2, r such that $0 \leq r < n$. Then
$a - b = (ny_1 + r) - (ny_2 + r) = ny_1 - ny_2 = n(y_1 - y_2)$, which is clearly divisible by n. □

With this result in hand, we now state and prove some fundamental properties of congruences.

Intro to Congruences

Proof.

As for the second, assume now that a and b have the same remainder upon division by n. Then we see that $a = ny_1 + r$ and $b = ny_2 + r$ for some integers y_1, y_2, r such that $0 \leq r < n$. Then
$a - b = (ny_1 + r) - (ny_2 + r) = ny_1 - ny_2 = n(y_1 - y_2)$, which is clearly divisible by n. □

With this result in hand, we now state and prove some fundamental properties of congruences. The next theorem is sort of a congruence analog of the Divisbility Theorem, which collected basic properties of divisibility.

Intro to Congruences

Proof.

As for the second, assume now that a and b have the same remainder upon division by n. Then we see that $a = ny_1 + r$ and $b = ny_2 + r$ for some integers y_1, y_2, r such that $0 \leq r < n$. Then
$a - b = (ny_1 + r) - (ny_2 + r) = ny_1 - ny_2 = n(y_1 - y_2)$, which is clearly divisible by n. □

With this result in hand, we now state and prove some fundamental properties of congruences. The next theorem is sort of a congruence analog of the Divisbility Theorem, which collected basic properties of divisibility.

Intro to Congruences

Theorem (Congruences Theorem)

Let n be a positive integer and let a, b, c, d be arbitrary integers.

Intro to Congruences

Theorem (Congruences Theorem)

Let n be a positive integer and let a, b, c, d be arbitrary integers. Then the following hold:

1. $a \equiv a \pmod{n}$,

Intro to Congruences

Theorem (Congruences Theorem)

Let n be a positive integer and let a, b, c, d be arbitrary integers. Then the following hold:

1. $a \equiv a \pmod{n}$,
2. *if* $a \equiv b \pmod{n}$, *then* $b \equiv a \pmod{n}$,

Intro to Congruences

Theorem (Congruences Theorem)

Let n be a positive integer and let a, b, c, d be arbitrary integers. Then the following hold:

1. $a \equiv a \pmod{n}$,
2. *if* $a \equiv b \pmod{n}$, *then* $b \equiv a \pmod{n}$,
3. *if* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$, *then* $a \equiv c \pmod{n}$,

Intro to Congruences

Theorem (Congruences Theorem)

Let n be a positive integer and let a, b, c, d be arbitrary integers. Then the following hold:

1. $a \equiv a \pmod{n}$,
2. *if* $a \equiv b \pmod{n}$, *then* $b \equiv a \pmod{n}$,
3. *if* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$, *then* $a \equiv c \pmod{n}$,
4. *if* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$, *then* $a + c \equiv b + d \pmod{n}$ *and* $ac \equiv bd \pmod{n}$,

Intro to Congruences

Theorem (Congruences Theorem)

Let n be a positive integer and let a, b, c, d be arbitrary integers. Then the following hold:

1. $a \equiv a \pmod{n}$,
2. *if* $a \equiv b \pmod{n}$, *then* $b \equiv a \pmod{n}$,
3. *if* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$, *then* $a \equiv c \pmod{n}$,
4. *if* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$, *then* $a + c \equiv b + d \pmod{n}$ *and* $ac \equiv bd \pmod{n}$,
5. *if* $a \equiv b \pmod{n}$, *then* $a + c \equiv b + c \pmod{n}$ *and* $ac \equiv bc \pmod{n}$,

Intro to Congruences

Theorem (Congruences Theorem)

Let n be a positive integer and let a, b, c, d be arbitrary integers. Then the following hold:

1. $a \equiv a \pmod{n}$,
2. *if* $a \equiv b \pmod{n}$, *then* $b \equiv a \pmod{n}$,
3. *if* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$, *then* $a \equiv c \pmod{n}$,
4. *if* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$, *then* $a + c \equiv b + d \pmod{n}$ *and* $ac \equiv bd \pmod{n}$,
5. *if* $a \equiv b \pmod{n}$, *then* $a + c \equiv b + c \pmod{n}$ *and* $ac \equiv bc \pmod{n}$, *and*
6. *if* $a \equiv b \pmod{n}$, *then* $a^k \equiv b^k \pmod{n}$ *for any positive integer* k.

Intro to Congruences

Theorem (Congruences Theorem)

Let n be a positive integer and let a, b, c, d be arbitrary integers. Then the following hold:

1. $a \equiv a \pmod{n}$,
2. *if* $a \equiv b \pmod{n}$, *then* $b \equiv a \pmod{n}$,
3. *if* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$, *then* $a \equiv c \pmod{n}$,
4. *if* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$, *then* $a + c \equiv b + d \pmod{n}$ *and* $ac \equiv bd \pmod{n}$,
5. *if* $a \equiv b \pmod{n}$, *then* $a + c \equiv b + c \pmod{n}$ *and* $ac \equiv bc \pmod{n}$, *and*
6. *if* $a \equiv b \pmod{n}$, *then* $a^k \equiv b^k \pmod{n}$ *for any positive integer* k.

Intro to Congruences

Proof.

Let n be a positive integer and let a, b, c, and d be integers.

Intro to Congruences

Proof.

Let n be a positive integer and let a, b, c, and d be integers.

(1) Clearly a and a have the same remainder upon division by n, and so $a \equiv a \pmod{n}$.

Intro to Congruences

Proof.

Let n be a positive integer and let a, b, c, and d be integers.

(1) Clearly a and a have the same remainder upon division by n, and so $a \equiv a \pmod{n}$.

(2) Assume that $a \equiv b \pmod{n}$.

Intro to Congruences

Proof.

Let n be a positive integer and let a, b, c, and d be integers.

(1) Clearly a and a have the same remainder upon division by n, and so $a \equiv a \pmod{n}$.

(2) Assume that $a \equiv b \pmod{n}$. Then a and b have the same remainder upon division by n, and so clearly b and a also have the same remainder upon division by n.

Intro to Congruences

Proof.

Let n be a positive integer and let a, b, c, and d be integers.

(1) Clearly a and a have the same remainder upon division by n, and so $a \equiv a \pmod{n}$.

(2) Assume that $a \equiv b \pmod{n}$. Then a and b have the same remainder upon division by n, and so clearly b and a also have the same remainder upon division by n. This shows that $b \equiv a \pmod{n}$.

Intro to Congruences

Proof.

Let n be a positive integer and let a, b, c, and d be integers.

(1) Clearly a and a have the same remainder upon division by n, and so $a \equiv a \pmod{n}$.

(2) Assume that $a \equiv b \pmod{n}$. Then a and b have the same remainder upon division by n, and so clearly b and a also have the same remainder upon division by n. This shows that $b \equiv a \pmod{n}$.

(3) Assume that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$.

Intro to Congruences

Proof.

Let n be a positive integer and let a, b, c, and d be integers.

(1) Clearly a and a have the same remainder upon division by n, and so $a \equiv a \pmod{n}$.

(2) Assume that $a \equiv b \pmod{n}$. Then a and b have the same remainder upon division by n, and so clearly b and a also have the same remainder upon division by n. This shows that $b \equiv a \pmod{n}$.

(3) Assume that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then a and b have the same remainder upon division by n and b and c have the same remainder upon division by n.

Intro to Congruences

Proof.

Let n be a positive integer and let a, b, c, and d be integers.

(1) Clearly a and a have the same remainder upon division by n, and so $a \equiv a \pmod{n}$.

(2) Assume that $a \equiv b \pmod{n}$. Then a and b have the same remainder upon division by n, and so clearly b and a also have the same remainder upon division by n. This shows that $b \equiv a \pmod{n}$.

(3) Assume that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then a and b have the same remainder upon division by n and b and c have the same remainder upon division by n. Thus a and c have the same remainder upon division by n, and $a \equiv c \pmod{n}$.

Proof.

Let n be a positive integer and let a, b, c, and d be integers.

(1) Clearly a and a have the same remainder upon division by n, and so $a \equiv a \pmod{n}$.

(2) Assume that $a \equiv b \pmod{n}$. Then a and b have the same remainder upon division by n, and so clearly b and a also have the same remainder upon division by n. This shows that $b \equiv a \pmod{n}$.

(3) Assume that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then a and b have the same remainder upon division by n and b and c have the same remainder upon division by n. Thus a and c have the same remainder upon division by n, and $a \equiv c \pmod{n}$.

Intro to Congruences

Proof.

(4) Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$.

Intro to Congruences

Proof.

(4) Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $n|a-b$ and $n|c-d$.

Intro to Congruences

Proof.

(4) Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $n|a-b$ and $n|c-d$. By the Divisibility Theorem, $n|a-b+c-d = (a+c)-(b+d)$.

Intro to Congruences

Proof.

(4) Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $n|a-b$ and $n|c-d$. By the Divisibility Theorem, $n|a-b+c-d = (a+c)-(b+d)$. This proves that $a+c \equiv b+d \pmod{n}$.

Intro to Congruences

Proof.

(4) Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $n|a-b$ and $n|c-d$. By the Divisibility Theorem, $n|a-b+c-d = (a+c)-(b+d)$. This proves that $a+c \equiv b+d \pmod{n}$. Also by the Div. Thm., $n|c(a-b) = ac-bc$ and $n|b(c-d) = bc-bd$.

Intro to Congruences

Proof.

(4) Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $n|a-b$ and $n|c-d$. By the Divisibility Theorem, $n|a-b+c-d = (a+c)-(b+d)$. This proves that $a+c \equiv b+d \pmod{n}$. Also by the Div. Thm., $n|c(a-b) = ac-bc$ and $n|b(c-d) = bc-bd$. By the Div. Thm. yet again, $n|ac-bc+bc-bd = ac-bd$.

Intro to Congruences

Proof.

(4) Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $n|a-b$ and $n|c-d$. By the Divisibility Theorem, $n|a-b+c-d = (a+c)-(b+d)$. This proves that $a+c \equiv b+d \pmod{n}$. Also by the Div. Thm., $n|c(a-b) = ac-bc$ and $n|b(c-d) = bc-bd$. By the Div. Thm. yet again, $n|ac-bc+bc-bd = ac-bd$. This proves that $ac \equiv bd \pmod{n}$.

Intro to Congruences

Proof.

(4) Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $n|a-b$ and $n|c-d$. By the Divisibility Theorem, $n|a-b+c-d = (a+c)-(b+d)$. This proves that $a+c \equiv b+d \pmod{n}$. Also by the Div. Thm., $n|c(a-b) = ac-bc$ and $n|b(c-d) = bc-bd$. By the Div. Thm. yet again, $n|ac-bc+bc-bd = ac-bd$. This proves that $ac \equiv bd \pmod{n}$.

(5) Assume that $a \equiv b \pmod{n}$.

Intro to Congruences

Proof.

(4) Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $n|a-b$ and $n|c-d$. By the Divisibility Theorem, $n|a-b+c-d = (a+c)-(b+d)$. This proves that $a+c \equiv b+d \pmod{n}$. Also by the Div. Thm., $n|c(a-b) = ac-bc$ and $n|b(c-d) = bc-bd$. By the Div. Thm. yet again, $n|ac-bc+bc-bd = ac-bd$. This proves that $ac \equiv bd \pmod{n}$.

(5) Assume that $a \equiv b \pmod{n}$. Then $n|a-b = (a+c)-(b+c)$.

Intro to Congruences

Proof.

(4) Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $n|a-b$ and $n|c-d$. By the Divisibility Theorem, $n|a-b+c-d = (a+c)-(b+d)$. This proves that $a+c \equiv b+d \pmod{n}$. Also by the Div. Thm., $n|c(a-b) = ac-bc$ and $n|b(c-d) = bc-bd$. By the Div. Thm. yet again, $n|ac-bc+bc-bd = ac-bd$. This proves that $ac \equiv bd \pmod{n}$.

(5) Assume that $a \equiv b \pmod{n}$. Then $n|a-b = (a+c)-(b+c)$. This proves the first assertion.

Intro to Congruences

Proof.

(4) Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $n|a-b$ and $n|c-d$. By the Divisibility Theorem, $n|a-b+c-d = (a+c)-(b+d)$. This proves that $a+c \equiv b+d \pmod{n}$. Also by the Div. Thm., $n|c(a-b) = ac-bc$ and $n|b(c-d) = bc-bd$. By the Div. Thm. yet again, $n|ac-bc+bc-bd = ac-bd$. This proves that $ac \equiv bd \pmod{n}$.

(5) Assume that $a \equiv b \pmod{n}$. Then $n|a-b = (a+c)-(b+c)$. This proves the first assertion. Second, since $n|a-b$, then by the Div. Thm., $n|c(a-b) = ac-bc$.

Intro to Congruences

Proof.

(4) Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $n|a-b$ and $n|c-d$. By the Divisibility Theorem, $n|a-b+c-d = (a+c)-(b+d)$. This proves that $a+c \equiv b+d \pmod{n}$. Also by the Div. Thm., $n|c(a-b) = ac-bc$ and $n|b(c-d) = bc-bd$. By the Div. Thm. yet again, $n|ac-bc+bc-bd = ac-bd$. This proves that $ac \equiv bd \pmod{n}$.

(5) Assume that $a \equiv b \pmod{n}$. Then $n|a-b = (a+c)-(b+c)$. This proves the first assertion. Second, since $n|a-b$, then by the Div. Thm., $n|c(a-b) = ac-bc$. This proves that $ac \equiv bc \pmod{n}$.

Intro to Congruences

Proof.

(4) Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $n|a-b$ and $n|c-d$. By the Divisibility Theorem, $n|a-b+c-d = (a+c)-(b+d)$. This proves that $a+c \equiv b+d \pmod{n}$. Also by the Div. Thm., $n|c(a-b) = ac-bc$ and $n|b(c-d) = bc-bd$. By the Div. Thm. yet again, $n|ac-bc+bc-bd = ac-bd$. This proves that $ac \equiv bd \pmod{n}$.

(5) Assume that $a \equiv b \pmod{n}$. Then $n|a-b = (a+c)-(b+c)$. This proves the first assertion. Second, since $n|a-b$, then by the Div. Thm., $n|c(a-b) = ac-bc$. This proves that $ac \equiv bc \pmod{n}$.

(6) Assume that $a \equiv b \pmod{n}$.

Intro to Congruences

Proof.

(4) Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $n|a-b$ and $n|c-d$. By the Divisibility Theorem, $n|a-b+c-d = (a+c)-(b+d)$. This proves that $a+c \equiv b+d \pmod{n}$. Also by the Div. Thm., $n|c(a-b) = ac-bc$ and $n|b(c-d) = bc-bd$. By the Div. Thm. yet again, $n|ac-bc+bc-bd = ac-bd$. This proves that $ac \equiv bd \pmod{n}$.

(5) Assume that $a \equiv b \pmod{n}$. Then $n|a-b = (a+c)-(b+c)$. This proves the first assertion. Second, since $n|a-b$, then by the Div. Thm., $n|c(a-b) = ac-bc$. This proves that $ac \equiv bc \pmod{n}$.

(6) Assume that $a \equiv b \pmod{n}$. We will prove that $a^k \equiv b^k \pmod{n}$ via induction for every positive integer k.

Intro to Congruences

Proof.

(4) Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $n|a-b$ and $n|c-d$. By the Divisibility Theorem, $n|a-b+c-d = (a+c)-(b+d)$. This proves that $a+c \equiv b+d \pmod{n}$. Also by the Div. Thm., $n|c(a-b) = ac-bc$ and $n|b(c-d) = bc-bd$. By the Div. Thm. yet again, $n|ac-bc+bc-bd = ac-bd$. This proves that $ac \equiv bd \pmod{n}$.

(5) Assume that $a \equiv b \pmod{n}$. Then $n|a-b = (a+c)-(b+c)$. This proves the first assertion. Second, since $n|a-b$, then by the Div. Thm., $n|c(a-b) = ac-bc$. This proves that $ac \equiv bc \pmod{n}$.

(6) Assume that $a \equiv b \pmod{n}$. We will prove that $a^k \equiv b^k \pmod{n}$ via induction for every positive integer k. The base case $k = 1$ is immediate from our assumption that $a \equiv b \pmod{n}$.

Intro to Congruences

Proof.

(4) Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $n|a-b$ and $n|c-d$. By the Divisibility Theorem, $n|a-b+c-d = (a+c)-(b+d)$. This proves that $a+c \equiv b+d \pmod{n}$. Also by the Div. Thm., $n|c(a-b) = ac-bc$ and $n|b(c-d) = bc-bd$. By the Div. Thm. yet again, $n|ac-bc+bc-bd = ac-bd$. This proves that $ac \equiv bd \pmod{n}$.

(5) Assume that $a \equiv b \pmod{n}$. Then $n|a-b = (a+c)-(b+c)$. This proves the first assertion. Second, since $n|a-b$, then by the Div. Thm., $n|c(a-b) = ac-bc$. This proves that $ac \equiv bc \pmod{n}$.

(6) Assume that $a \equiv b \pmod{n}$. We will prove that $a^k \equiv b^k \pmod{n}$ via induction for every positive integer k. The base case $k = 1$ is immediate from our assumption that $a \equiv b \pmod{n}$. Now let k be a positive integer and assume that $a^k \equiv b^k \pmod{n}$.

Intro to Congruences

Proof.

(4) Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $n|a-b$ and $n|c-d$. By the Divisibility Theorem, $n|a-b+c-d = (a+c)-(b+d)$. This proves that $a+c \equiv b+d \pmod{n}$. Also by the Div. Thm., $n|c(a-b) = ac-bc$ and $n|b(c-d) = bc-bd$. By the Div. Thm. yet again, $n|ac-bc+bc-bd = ac-bd$. This proves that $ac \equiv bd \pmod{n}$.

(5) Assume that $a \equiv b \pmod{n}$. Then $n|a-b = (a+c)-(b+c)$. This proves the first assertion. Second, since $n|a-b$, then by the Div. Thm., $n|c(a-b) = ac-bc$. This proves that $ac \equiv bc \pmod{n}$.

(6) Assume that $a \equiv b \pmod{n}$. We will prove that $a^k \equiv b^k \pmod{n}$ via induction for every positive integer k. The base case $k = 1$ is immediate from our assumption that $a \equiv b \pmod{n}$. Now let k be a positive integer and assume that $a^k \equiv b^k \pmod{n}$. Recall our assumption that $a \equiv b \pmod{n}$.

Intro to Congruences

Proof.

(4) Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $n|a-b$ and $n|c-d$. By the Divisibility Theorem, $n|a-b+c-d = (a+c)-(b+d)$. This proves that $a+c \equiv b+d \pmod{n}$. Also by the Div. Thm., $n|c(a-b) = ac-bc$ and $n|b(c-d) = bc-bd$. By the Div. Thm. yet again, $n|ac-bc+bc-bd = ac-bd$. This proves that $ac \equiv bd \pmod{n}$.

(5) Assume that $a \equiv b \pmod{n}$. Then $n|a-b = (a+c)-(b+c)$. This proves the first assertion. Second, since $n|a-b$, then by the Div. Thm., $n|c(a-b) = ac-bc$. This proves that $ac \equiv bc \pmod{n}$.

(6) Assume that $a \equiv b \pmod{n}$. We will prove that $a^k \equiv b^k \pmod{n}$ via induction for every positive integer k. The base case $k = 1$ is immediate from our assumption that $a \equiv b \pmod{n}$. Now let k be a positive integer and assume that $a^k \equiv b^k \pmod{n}$. Recall our assumption that $a \equiv b \pmod{n}$. Now by (4) above, we have $a^k \cdot a \equiv b^k \cdot b \pmod{n}$, that is, $a^{k+1} \equiv b^{k+1} \pmod{n}$.

Intro to Congruences

Proof.

(4) Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $n|a-b$ and $n|c-d$. By the Divisibility Theorem, $n|a-b+c-d = (a+c)-(b+d)$. This proves that $a+c \equiv b+d \pmod{n}$. Also by the Div. Thm., $n|c(a-b) = ac-bc$ and $n|b(c-d) = bc-bd$. By the Div. Thm. yet again, $n|ac-bc+bc-bd = ac-bd$. This proves that $ac \equiv bd \pmod{n}$.

(5) Assume that $a \equiv b \pmod{n}$. Then $n|a-b = (a+c)-(b+c)$. This proves the first assertion. Second, since $n|a-b$, then by the Div. Thm., $n|c(a-b) = ac-bc$. This proves that $ac \equiv bc \pmod{n}$.

(6) Assume that $a \equiv b \pmod{n}$. We will prove that $a^k \equiv b^k \pmod{n}$ via induction for every positive integer k. The base case $k = 1$ is immediate from our assumption that $a \equiv b \pmod{n}$. Now let k be a positive integer and assume that $a^k \equiv b^k \pmod{n}$. Recall our assumption that $a \equiv b \pmod{n}$. Now by (4) above, we have $a^k \cdot a \equiv b^k \cdot b \pmod{n}$, that is, $a^{k+1} \equiv b^{k+1} \pmod{n}$. This concludes the proof. □

Intro to Congruences

We now pause to give a couple of applications of the theory presented above.

Intro to Congruences

We now pause to give a couple of applications of the theory presented above.

Example

Show that for any positive integer n, the remainder upon dividing 10^n by 3 is 1.

Intro to Congruences

We now pause to give a couple of applications of the theory presented above.

Example

Show that for any positive integer n, the remainder upon dividing 10^n by 3 is 1.

Proof.

Let n be a positive integer.

Intro to Congruences

We now pause to give a couple of applications of the theory presented above.

Example

Show that for any positive integer n, the remainder upon dividing 10^n by 3 is 1.

Proof.

Let n be a positive integer. Note first that $10 \equiv 1 \pmod{3}$ (take a second to process this).

Intro to Congruences

We now pause to give a couple of applications of the theory presented above.

Example

Show that for any positive integer n, the remainder upon dividing 10^n by 3 is 1.

Proof.

Let n be a positive integer. Note first that $10 \equiv 1 \pmod 3$ (take a second to process this). Now by (6) of the Congruences Theorem, we see that $10^n \equiv 1^n \pmod 3$, that is, $10^n \equiv 1 \pmod 3$.

Intro to Congruences

We now pause to give a couple of applications of the theory presented above.

Example

Show that for any positive integer n, the remainder upon dividing 10^n by 3 is 1.

Proof.

Let n be a positive integer. Note first that $10 \equiv 1 \pmod 3$ (take a second to process this). Now by (6) of the Congruences Theorem, we see that $10^n \equiv 1^n \pmod 3$, that is, $10^n \equiv 1 \pmod 3$. By the Characterization of Congruences Theorem, the remainder upon dividing 10^n by 3 is the same as the remainder upon dividing 1 by 3, which is 1. □

Intro to Congruences

We now pause to give a couple of applications of the theory presented above.

Example

Show that for any positive integer n, the remainder upon dividing 10^n by 3 is 1.

Proof.

Let n be a positive integer. Note first that $10 \equiv 1 \pmod 3$ (take a second to process this). Now by (6) of the Congruences Theorem, we see that $10^n \equiv 1^n \pmod 3$, that is, $10^n \equiv 1 \pmod 3$. By the Characterization of Congruences Theorem, the remainder upon dividing 10^n by 3 is the same as the remainder upon dividing 1 by 3, which is 1. □

Intro to Congruences

Example

Find the remainder upon dividing $1! + 2! + \cdots + 10!$ by 6.

Intro to Congruences

Example

Find the remainder upon dividing $1! + 2! + \cdots + 10!$ by 6.

Solution.

Note that 3!, 4!, 5!, ..., 10! are divisible by 6, that is, $n! \equiv 0 \pmod 6$ for $3 \leq n \leq 10$.

Intro to Congruences

Example

Find the remainder upon dividing $1! + 2! + \cdots + 10!$ by 6.

Solution.

Note that 3!, 4!, 5!, ..., 10! are divisible by 6, that is, $n! \equiv 0 \pmod 6$ for $3 \leq n \leq 10$. By (4) of the Congruences Theorem, it follows that $3! + \cdots + 10! \equiv 0 \pmod 6$.

Intro to Congruences

Example

Find the remainder upon dividing $1! + 2! + \cdots + 10!$ by 6.

Solution.

Note that $3!$, $4!$, $5!$, $\ldots$, $10!$ are divisible by 6, that is, $n! \equiv 0 \pmod 6$ for $3 \leq n \leq 10$. By (4) of the Congruences Theorem, it follows that $3! + \cdots + 10! \equiv 0 \pmod 6$. By (5) of the same theorem, it follows that $1! + 2! + \cdots + 10! \equiv 1! + 2! \pmod 6$,

Intro to Congruences

Example

Find the remainder upon dividing $1! + 2! + \cdots + 10!$ by 6.

Solution.

Note that $3!, 4!, 5!, \ldots, 10!$ are divisible by 6, that is, $n! \equiv 0 \pmod 6$ for $3 \leq n \leq 10$. By (4) of the Congruences Theorem, it follows that $3! + \cdots + 10! \equiv 0 \pmod 6$. By (5) of the same theorem, it follows that $1! + 2! + \cdots + 10! \equiv 1! + 2! \pmod 6$, that is, $1! + 2! + \cdots + 10! \equiv 3 \pmod 6$.

Intro to Congruences

Example

Find the remainder upon dividing $1! + 2! + \cdots + 10!$ by 6.

Solution.

Note that $3!, 4!, 5!, \ldots, 10!$ are divisible by 6, that is, $n! \equiv 0 \pmod 6$ for $3 \leq n \leq 10$. By (4) of the Congruences Theorem, it follows that $3! + \cdots + 10! \equiv 0 \pmod 6$. By (5) of the same theorem, it follows that $1! + 2! + \cdots + 10! \equiv 1! + 2! \pmod 6$, that is, $1! + 2! + \cdots + 10! \equiv 3 \pmod 6$. Thus the remainder is 3 (by the Char. of Congruences Theorem). □

Intro to Congruences

Example

Find the remainder upon dividing $1! + 2! + \cdots + 10!$ by 6.

Solution.

Note that $3!, 4!, 5!, \ldots, 10!$ are divisible by 6, that is, $n! \equiv 0 \pmod 6$ for $3 \leq n \leq 10$. By (4) of the Congruences Theorem, it follows that $3! + \cdots + 10! \equiv 0 \pmod 6$. By (5) of the same theorem, it follows that $1! + 2! + \cdots + 10! \equiv 1! + 2! \pmod 6$, that is, $1! + 2! + \cdots + 10! \equiv 3 \pmod 6$. Thus the remainder is 3 (by the Char. of Congruences Theorem). □

Intro to Congruences

Our final theorem shows that one may "cancel" in congruence if one appropriately changed the *modulus* (the "n" in mod n).

Intro to Congruences

Our final theorem shows that one may "cancel" in congruence if one appropriately changed the *modulus* (the "n" in mod n).

Theorem

Let $a, b,$ and c be integers and n be a positive integer.

Intro to Congruences

Our final theorem shows that one may "cancel" in congruence if one appropriately changed the *modulus* (the "n" in mod n).

Theorem

Let a, b, and c be integers and n be a positive integer. If $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$.

Intro to Congruences

Our final theorem shows that one may "cancel" in congruence if one appropriately changed the *modulus* (the "n" in mod n).

Theorem

Let a, b, and c be integers and n be a positive integer. If $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$.

Proof.

Let a, b, and c be integers and n be a positive integer.

Intro to Congruences

Our final theorem shows that one may "cancel" in congruence if one appropriately changed the *modulus* (the "n" in mod n).

Theorem

Let a, b, and c be integers and n be a positive integer. If $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$.

Proof.

Let a, b, and c be integers and n be a positive integer. Assume that $ac \equiv bc \pmod{n}$.

Intro to Congruences

Our final theorem shows that one may "cancel" in congruence if one appropriately changed the *modulus* (the "n" in mod n).

Theorem

Let a, b, and c be integers and n be a positive integer. If $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$.

Proof.

Let a, b, and c be integers and n be a positive integer. Assume that $ac \equiv bc \pmod{n}$. Then $n | ac - bc$.

Intro to Congruences

Our final theorem shows that one may "cancel" in congruence if one appropriately changed the *modulus* (the "n" in mod n).

Theorem

Let a, b, and c be integers and n be a positive integer. If $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$.

Proof.

Let a, b, and c be integers and n be a positive integer. Assume that $ac \equiv bc \pmod{n}$. Then $n|ac - bc$. Since $n > 0$, note that $d = \gcd(c, n)$ exists.

Intro to Congruences

Our final theorem shows that one may "cancel" in congruence if one appropriately changed the *modulus* (the "n" in mod n).

Theorem

Let a, b, and c be integers and n be a positive integer. If $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$.

Proof.

Let a, b, and c be integers and n be a positive integer. Assume that $ac \equiv bc \pmod{n}$. Then $n|ac - bc$. Since $n > 0$, note that $d = \gcd(c, n)$ exists. We must show that $a \equiv b \pmod{n/d}$, that is, $n/d|a - b$ (note that $d|n$, so n/d is a positive integer).

Intro to Congruences

Our final theorem shows that one may "cancel" in congruence if one appropriately changed the *modulus* (the "n" in mod n).

Theorem

Let a, b, and c be integers and n be a positive integer. If $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$.

Proof.

Let a, b, and c be integers and n be a positive integer. Assume that $ac \equiv bc \pmod{n}$. Then $n|ac - bc$. Since $n > 0$, note that $d = \gcd(c, n)$ exists. We must show that $a \equiv b \pmod{n/d}$, that is, $n/d|a - b$ (note that $d|n$, so n/d is a positive integer). But this is equivalent to $n|ad - bd$.

Intro to Congruences

Our final theorem shows that one may "cancel" in congruence if one appropriately changed the *modulus* (the "n" in mod n).

Theorem

Let a, b, and c be integers and n be a positive integer. If $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$.

Proof.

Let a, b, and c be integers and n be a positive integer. Assume that $ac \equiv bc \pmod{n}$. Then $n|ac - bc$. Since $n > 0$, note that $d = \gcd(c, n)$ exists. We must show that $a \equiv b \pmod{n/d}$, that is, $n/d|a - b$ (note that $d|n$, so n/d is a positive integer). But this is equivalent to $n|ad - bd$. We have $dr = c$ and $ds = n$ for some integers r and s.

Intro to Congruences

Our final theorem shows that one may "cancel" in congruence if one appropriately changed the *modulus* (the "n" in mod n).

Theorem

Let a, b, and c be integers and n be a positive integer. If $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$.

Proof.

Let a, b, and c be integers and n be a positive integer. Assume that $ac \equiv bc \pmod{n}$. Then $n|ac - bc$. Since $n > 0$, note that $d = \gcd(c, n)$ exists. We must show that $a \equiv b \pmod{n/d}$, that is, $n/d|a - b$ (note that $d|n$, so n/d is a positive integer). But this is equivalent to $n|ad - bd$. We have $dr = c$ and $ds = n$ for some integers r and s. Thus $n|ac - bc$ becomes $ds|adr - bdr$.

Intro to Congruences

Our final theorem shows that one may "cancel" in congruence if one appropriately changed the *modulus* (the "n" in mod n).

Theorem

Let a, b, and c be integers and n be a positive integer. If $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$.

Proof.

Let a, b, and c be integers and n be a positive integer. Assume that $ac \equiv bc \pmod{n}$. Then $n|ac - bc$. Since $n > 0$, note that $d = \gcd(c, n)$ exists. We must show that $a \equiv b \pmod{n/d}$, that is, $n/d|a - b$ (note that $d|n$, so n/d is a positive integer). But this is equivalent to $n|ad - bd$. We have $dr = c$ and $ds = n$ for some integers r and s. Thus $n|ac - bc$ becomes $ds|adr - bdr$. But then $s|ar - br = (a - b)r$.

Intro to Congruences

Our final theorem shows that one may "cancel" in congruence if one appropriately changed the *modulus* (the "n" in mod n).

Theorem

Let a, b, and c be integers and n be a positive integer. If $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$.

Proof.

Let a, b, and c be integers and n be a positive integer. Assume that $ac \equiv bc \pmod{n}$. Then $n|ac - bc$. Since $n > 0$, note that $d = \gcd(c, n)$ exists. We must show that $a \equiv b \pmod{n/d}$, that is, $n/d|a - b$ (note that $d|n$, so n/d is a positive integer). But this is equivalent to $n|ad - bd$. We have $dr = c$ and $ds = n$ for some integers r and s. Thus $n|ac - bc$ becomes $ds|adr - bdr$. But then $s|ar - br = (a - b)r$. Now, s and r are relatively prime, and thus $s|a - b$ (Euclid's Lemma).

Intro to Congruences

Our final theorem shows that one may "cancel" in congruence if one appropriately changed the *modulus* (the "n" in mod n).

Theorem

Let a, b, and c be integers and n be a positive integer. If $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$.

Proof.

Let a, b, and c be integers and n be a positive integer. Assume that $ac \equiv bc \pmod{n}$. Then $n|ac - bc$. Since $n > 0$, note that $d = \gcd(c, n)$ exists. We must show that $a \equiv b \pmod{n/d}$, that is, $n/d|a - b$ (note that $d|n$, so n/d is a positive integer). But this is equivalent to $n|ad - bd$. We have $dr = c$ and $ds = n$ for some integers r and s. Thus $n|ac - bc$ becomes $ds|adr - bdr$. But then $s|ar - br = (a - b)r$. Now, s and r are relatively prime, and thus $s|a - b$ (Euclid's Lemma). Multiply through by d (justified by the Divisibility Theorem) to get $sd|ad - bd$, that is, $n|ad - bd$, which is what we wanted to show.

Intro to Congruences

Our final theorem shows that one may "cancel" in congruence if one appropriately changed the *modulus* (the "n" in mod n).

Theorem

Let a, b, and c be integers and n be a positive integer. If $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$.

Proof.

Let a, b, and c be integers and n be a positive integer. Assume that $ac \equiv bc \pmod{n}$. Then $n|ac - bc$. Since $n > 0$, note that $d = \gcd(c, n)$ exists. We must show that $a \equiv b \pmod{n/d}$, that is, $n/d|a - b$ (note that $d|n$, so n/d is a positive integer). But this is equivalent to $n|ad - bd$. We have $dr = c$ and $ds = n$ for some integers r and s. Thus $n|ac - bc$ becomes $ds|adr - bdr$. But then $s|ar - br = (a - b)r$. Now, s and r are relatively prime, and thus $s|a - b$ (Euclid's Lemma). Multiply through by d (justified by the Divisibility Theorem) to get $sd|ad - bd$, that is, $n|ad - bd$, which is what we wanted to show. □

Intro to Congruences

Corollary

Let a, b, c be integers and n be a positive integer such that $ac \equiv bc \pmod{n}$.

Intro to Congruences

Corollary

Let a, b, c be integers and n be a positive integer such that $ac \equiv bc \pmod{n}$. Suppose that $\gcd(c, n) = 1$.

Intro to Congruences

Corollary

Let a, b, c be integers and n be a positive integer such that $ac \equiv bc \pmod{n}$. Suppose that $\gcd(c, n) = 1$. Then $a \equiv b \pmod{n}$.

Intro to Congruences

Corollary

Let a, b, c be integers and n be a positive integer such that $ac \equiv bc \pmod{n}$. Suppose that $\gcd(c, n) = 1$. Then $a \equiv b \pmod{n}$.

Proof.

This is immediate from the theorem, since $d = 1$ in this case. □

Intro to Congruences

Corollary

Let a, b, c be integers and n be a positive integer such that $ac \equiv bc \pmod{n}$. Suppose that $\gcd(c, n) = 1$. Then $a \equiv b \pmod{n}$.

Proof.

This is immediate from the theorem, since $d = 1$ in this case. □

Corollary

Let a, b, c be integers and p a prime.

Intro to Congruences

Corollary

Let a, b, c be integers and n be a positive integer such that $ac \equiv bc \pmod{n}$. Suppose that $\gcd(c, n) = 1$. Then $a \equiv b \pmod{n}$.

Proof.

This is immediate from the theorem, since $d = 1$ in this case. □

Corollary

Let a, b, c be integers and p a prime. Suppose that $ca \equiv cb \pmod{p}$.

Intro to Congruences

Corollary

Let a, b, c be integers and n be a positive integer such that $ac \equiv bc \pmod{n}$. Suppose that $\gcd(c, n) = 1$. Then $a \equiv b \pmod{n}$.

Proof.

This is immediate from the theorem, since $d = 1$ in this case. □

Corollary

Let a, b, c be integers and p a prime. Suppose that $ca \equiv cb \pmod{p}$. If $p \nmid c$, then $a \equiv b \pmod{p}$.

Intro to Congruences

Corollary

Let a, b, c be integers and n be a positive integer such that $ac \equiv bc \pmod{n}$. Suppose that $\gcd(c, n) = 1$. Then $a \equiv b \pmod{n}$.

Proof.

This is immediate from the theorem, since $d = 1$ in this case. □

Corollary

Let a, b, c be integers and p a prime. Suppose that $ca \equiv cb \pmod{p}$. If $p \nmid c$, then $a \equiv b \pmod{p}$.

Proof.

Let a, b, c, p be as stated.

Intro to Congruences

Corollary

Let a, b, c be integers and n be a positive integer such that $ac \equiv bc \pmod{n}$. Suppose that $\gcd(c, n) = 1$. Then $a \equiv b \pmod{n}$.

Proof.

This is immediate from the theorem, since $d = 1$ in this case. □

Corollary

Let a, b, c be integers and p a prime. Suppose that $ca \equiv cb \pmod{p}$. If $p \nmid c$, then $a \equiv b \pmod{p}$.

Proof.

Let a, b, c, p be as stated. Suppose $ca \equiv cb \pmod{p}$.

Intro to Congruences

Corollary

Let a, b, c be integers and n be a positive integer such that $ac \equiv bc \pmod{n}$. Suppose that $\gcd(c, n) = 1$. Then $a \equiv b \pmod{n}$.

Proof.

This is immediate from the theorem, since $d = 1$ in this case. □

Corollary

Let a, b, c be integers and p a prime. Suppose that $ca \equiv cb \pmod{p}$. If $p \nmid c$, then $a \equiv b \pmod{p}$.

Proof.

Let a, b, c, p be as stated. Suppose $ca \equiv cb \pmod{p}$. Then $p | ca - cb = c(a - b)$.

Intro to Congruences

Corollary

Let a, b, c be integers and n be a positive integer such that $ac \equiv bc \pmod{n}$. Suppose that $\gcd(c, n) = 1$. Then $a \equiv b \pmod{n}$.

Proof.

This is immediate from the theorem, since $d = 1$ in this case. □

Corollary

Let a, b, c be integers and p a prime. Suppose that $ca \equiv cb \pmod{p}$. If $p \nmid c$, then $a \equiv b \pmod{p}$.

Proof.

Let a, b, c, p be as stated. Suppose $ca \equiv cb \pmod{p}$. Then $p|ca - cb = c(a - b)$. Since $p \nmid c$ and p is prime, p and c are relatively prime.

Intro to Congruences

Corollary

Let a, b, c be integers and n be a positive integer such that $ac \equiv bc \pmod{n}$. Suppose that $\gcd(c, n) = 1$. Then $a \equiv b \pmod{n}$.

Proof.

This is immediate from the theorem, since $d = 1$ in this case. □

Corollary

Let a, b, c be integers and p a prime. Suppose that $ca \equiv cb \pmod{p}$. If $p \nmid c$, then $a \equiv b \pmod{p}$.

Proof.

Let a, b, c, p be as stated. Suppose $ca \equiv cb \pmod{p}$. Then $p|ca - cb = c(a - b)$. Since $p \nmid c$ and p is prime, p and c are relatively prime. Now apply the previous corollary. □