§1.3, 1.4: Congruences and Integers Modulo n

Shaoyun Yi

MATH 546/701I

University of South Carolina

May 11, 2020

Preliminary

Definition 1

An integer a is called a **multiple** of an integer b if $a = bq$ for some integer q. In this case we also say that b is a **divisor** of a, and we use the notation $b|a$.

Preliminary

Definition 1

An integer a is called a **multiple** of an integer b if $a = bq$ for some integer q. In this case we also say that b is a **divisor** of a, and we use the notation $b|a$.

Axiom. 1 (Well-Ordering Principle)

Every nonempty set of natural numbers contains a smallest element.

Preliminary

Definition 1

An integer a is called a **multiple** of an integer b if $a = bq$ for some integer q. In this case we also say that b is a **divisor** of a, and we use the notation $b|a$.

Axiom. 1 (Well-Ordering Principle)

Every nonempty set of natural numbers contains a smallest element.

Theorem 2 (Division Algorithm)

For any integers a and b, with $b > 0$, there exist unique integers q (the **quotient***) and r (the* **remainder***) such that*

$$a = bq + r, \quad \text{with } 0 \leq r < b.$$

Greatest Common Divisor

Definition 3

Let a and b be integers, not both zero. A positive integer d is called the **greatest common divisor** of a and b if

1. d is a divisor of both a and b, and
2. any divisor of both a and b is also a divisor of d.

The greatest common divisor of a and b will be denoted by $\gcd(a, b)$ or (a, b).

Greatest Common Divisor

Definition 3

Let a and b be integers, not both zero. A positive integer d is called the **greatest common divisor** of a and b if

1. d is a divisor of both a and b, and
2. any divisor of both a and b is also a divisor of d.

The greatest common divisor of a and b will be denoted by $\gcd(a, b)$ or (a, b).

Definition 4 (shortened version)

If a and b are integers, not both zero, and d is a positive integer, then $d = \gcd(a, b)$ if

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

Greatest Common Divisor vs. Linear Combination

If a and b are integers, then we will refer to any integer of the form $ma + nb$, where $m, n \in \mathbf{Z}$, as a **linear combination** of a and b.

Greatest Common Divisor vs. Linear Combination

If a and b are integers, then we will refer to any integer of the form $ma + nb$, where $m, n \in \mathbf{Z}$, as a **linear combination** of a and b.

Theorem 5

Let a and b be integers, not both zero. Then a and b have a greatest common divisor, which can be expressed as the smallest positive linear combination of a and b.
Moreover, an integer is a linear combination of a and b if and only if it is a multiple of their greatest common divisor.

Euclidean algorithm

Given integers $a > b > 0$, the **Euclidean algorithm** uses the division algorithm repeatedly to obtain

$$\begin{aligned} a =& bq_1 + r_1 && \text{with} && 0 \le r_1 < b \\ b =& r_1 q_2 + r_2 && \text{with} && 0 \le r_2 < r_1 \\ r_1 =& r_2 q_3 + r_3 && \text{with} && 0 \le r_3 < r_2 \\ & && \text{etc.} && \end{aligned}$$

If $r_1 = 0$, then $b|a$, and so $(a, b) = b$. Since $r_1 > r_2 > \ldots$, the remainders get smaller and smaller, and after a finite number of steps we obtain a remainder $r_{n+1} = 0$. The algorithm ends with the equation

$$r_{n-1} = r_n q_{n+1} + 0.$$

Euclidean algorithm

Given integers $a > b > 0$, the **Euclidean algorithm** uses the division algorithm repeatedly to obtain

$$\begin{aligned} a &= bq_1 + r_1 && \text{with} && 0 \leq r_1 < b \\ b &= r_1 q_2 + r_2 && \text{with} && 0 \leq r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3 && \text{with} && 0 \leq r_3 < r_2 \\ & && \text{etc.} && \end{aligned}$$

If $r_1 = 0$, then $b|a$, and so $(a, b) = b$. Since $r_1 > r_2 > \ldots$, the remainders get smaller and smaller, and after a finite number of steps we obtain a remainder $r_{n+1} = 0$. The algorithm ends with the equation

$$r_{n-1} = r_n q_{n+1} + 0.$$

This gives us the greatest common divisor:

$$(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = (r_n, 0) = r_n.$$

Example

In finding $(126, 35)$, we can arrange the work in the following manner:

Example

In finding $(126, 35)$, we can arrange the work in the following manner:

$$\begin{aligned} 126 =& 35 \cdot 3 + 21 \qquad & (126, 35) = (35, 21) \\ 35 =& 21 \cdot 1 + 14 \qquad & (35, 21) = (21, 14) \\ 21 =& 14 \cdot 1 + 7 \qquad & (21, 14) = (14, 7) \\ 14 =& 7 \cdot 2 + 0 \qquad & (14, 7) = (7, 0) = 7 \end{aligned}$$

Example

In finding $(126, 35)$, we can arrange the work in the following manner:

$$\begin{aligned} 126 =& 35 \cdot 3 + 21 & \qquad (126, 35) = (35, 21) \\ 35 =& 21 \cdot 1 + 14 & \qquad (35, 21) = (21, 14) \\ 21 =& 14 \cdot 1 + 7 & \qquad (21, 14) = (14, 7) \\ 14 =& 7 \cdot 2 + 0 & \qquad (14, 7) = (7, 0) = 7 \end{aligned}$$

Find the linear combination of 126 and 35 that gives $(126, 35) = 7$:

Example

In finding $(126, 35)$, we can arrange the work in the following manner:

$$\begin{aligned} 126 =& 35 \cdot 3 + 21 \qquad && (126, 35) = (35, 21) \\ 35 =& 21 \cdot 1 + 14 && (35, 21) = (21, 14) \\ 21 =& 14 \cdot 1 + 7 && (21, 14) = (14, 7) \\ 14 =& 7 \cdot 2 + 0 && (14, 7) = (7, 0) = 7 \end{aligned}$$

Find the linear combination of 126 and 35 that gives $(126, 35) = 7$:
Step 1: Solve for the nonzero remainder in each of the equations

$$\begin{aligned} 7 =& 21 + 14 \cdot (-1) \\ 14 =& 35 + 21 \cdot (-1) \\ 21 =& 126 + 35 \cdot (-3) \end{aligned}$$

Example

In finding $(126, 35)$, we can arrange the work in the following manner:

$$\begin{aligned} 126 =& 35 \cdot 3 + 21 & \qquad (126, 35) = (35, 21) \\ 35 =& 21 \cdot 1 + 14 & (35, 21) = (21, 14) \\ 21 =& 14 \cdot 1 + 7 & (21, 14) = (14, 7) \\ 14 =& 7 \cdot 2 + 0 & (14, 7) = (7, 0) = 7 \end{aligned}$$

Find the linear combination of 126 and 35 that gives $(126, 35) = 7$:

Step 1: Solve for the nonzero remainder in each of the equations

$$\begin{aligned} 7 =& 21 + 14 \cdot (-1) \\ 14 =& 35 + 21 \cdot (-1) \\ 21 =& 126 + 35 \cdot (-3) \end{aligned}$$

Step 2: Substitute for the intermediate remainders:

$$\begin{aligned} 7 =& 21 + (-1) \cdot [35 + 21 \cdot (-1)] \\ =& (-1) \cdot 35 + 2 \cdot [126 + 35 \cdot (-3)] \\ =& 2 \cdot 126 + (-7) \cdot 35 \end{aligned}$$

Matrix form of the Euclidean algorithm

To find (a, b): Beginning with the matrix

$$\begin{aligned}
&\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \end{bmatrix} \\
\rightsquigarrow &\begin{bmatrix} 1 & -q_1 & r_1 \\ 0 & 1 & b \end{bmatrix} \qquad (a = bq_1 + r_1) \\
\rightsquigarrow &\begin{bmatrix} 1 & -q_1 & r_1 \\ -q_2 & 1 + q_1 q_2 & r_2 \end{bmatrix} \qquad (b = r_1 q_2 + r_2) \\
&\vdots
\end{aligned}$$

The procedure is continued until one of the entries in the right-hand column is zero.

Matrix form of the Euclidean algorithm

To find (a, b): Beginning with the matrix

$$\begin{aligned}
&\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \end{bmatrix} \\
\rightsquigarrow &\begin{bmatrix} 1 & -q_1 & r_1 \\ 0 & 1 & b \end{bmatrix} \qquad (a = bq_1 + r_1) \\
\rightsquigarrow &\begin{bmatrix} 1 & -q_1 & r_1 \\ -q_2 & 1 + q_1 q_2 & r_2 \end{bmatrix} \qquad (b = r_1 q_2 + r_2) \\
&\vdots
\end{aligned}$$

The procedure is continued until one of the entries in the right-hand column is zero. Then the other entry in this column is the greatest common divisor, and its row contains the coefficients of the desired linear combination.

Example revisited

$$
\begin{aligned}
&\begin{bmatrix} 1 & 0 & 126 \\ 0 & 1 & 35 \end{bmatrix} \\
\rightsquigarrow &\begin{bmatrix} 1 & -3 & 21 \\ 0 & 1 & 35 \end{bmatrix} \qquad (126 = 35 \cdot 3 + 21) \\
\rightsquigarrow &\begin{bmatrix} 1 & -3 & 21 \\ -1 & 4 & 14 \end{bmatrix} \qquad (35 = 21 \cdot 1 + 14) \\
\rightsquigarrow &\begin{bmatrix} 2 & -7 & 7 \\ -1 & 4 & 14 \end{bmatrix} \qquad (21 = 14 \cdot 1 + 7) \\
\rightsquigarrow &\begin{bmatrix} {\color{blue}2} & {\color{blue}-7} & {\color{red}7} \\ -5 & 18 & 0 \end{bmatrix} \qquad (14 = 7 \cdot 2 + 0)
\end{aligned}
$$

Thus, $(126, 35) = {\color{red}7}$ and a linear combination is ${\color{blue}2} \cdot 126 + {\color{blue}(-7)} \cdot 35 = {\color{red}7}$.

Example revisited

$$
\begin{aligned}
&\begin{bmatrix} 1 & 0 & 126 \\ 0 & 1 & 35 \end{bmatrix} \\
\rightsquigarrow &\begin{bmatrix} 1 & -3 & 21 \\ 0 & 1 & 35 \end{bmatrix} \qquad (126 = 35 \cdot 3 + 21) \\
\rightsquigarrow &\begin{bmatrix} 1 & -3 & 21 \\ -1 & 4 & 14 \end{bmatrix} \qquad (35 = 21 \cdot 1 + 14) \\
\rightsquigarrow &\begin{bmatrix} 2 & -7 & 7 \\ -1 & 4 & 14 \end{bmatrix} \qquad (21 = 14 \cdot 1 + 7) \\
\rightsquigarrow &\begin{bmatrix} 2 & -7 & 7 \\ -5 & 18 & 0 \end{bmatrix} \qquad (14 = 7 \cdot 2 + 0)
\end{aligned}
$$

Thus, $(126, 35) = 7$ and a linear combination is $2 \cdot 126 + (-7) \cdot 35 = 7$.

Moreover, we can see that $(-5) \cdot 126 + 18 \cdot 35 = 0$ from the other row.

Relatively prime

Definition 6

The nonzero integers a and b are said to be **relatively prime** if $(a, b) = 1$.

Relatively prime

Definition 6

The nonzero integers a and b are said to be **relatively prime** if $(a, b) = 1$.

Proposition. 1

$(a, b) = 1$ *if and only if there exist integers* m, n *such that* $ma + nb = 1$.

Relatively prime

Definition 6

The nonzero integers a and b are said to be **relatively prime** if $(a, b) = 1$.

Proposition. 1

$(a, b) = 1$ *if and only if there exist integers* m, n *such that* $ma + nb = 1$.

Proposition. 2

Let a, b, c *be integers, where* $a \neq 0$ *or* $b \neq 0$.

(a) *If* $b|ac$, *then* $b|(a, b) \cdot c$.

(b) *If* $b|ac$ *and* $(a, b) = 1$, *then* $b|c$.

(c) *If* $b|a, c|a$ *and* $(b, c) = 1$, *then* $bc|a$.

(d) $(a, bc) = 1$ *if and only if* $(a, b) = 1$ *and* $(a, c) = 1$.

Relatively prime

Definition 6

The nonzero integers a and b are said to be **relatively prime** if $(a, b) = 1$.

Proposition. 1

$(a, b) = 1$ if and only if there exist integers m, n such that $ma + nb = 1$.

Proposition. 2

Let a, b, c be integers, where $a \neq 0$ or $b \neq 0$.

(a) *If $b|ac$, then $b|(a, b) \cdot c$.*

(b) *If $b|ac$ and $(a, b) = 1$, then $b|c$.*

(c) *If $b|a, c|a$ and $(b, c) = 1$, then $bc|a$.*

(d) *$(a, bc) = 1$ if and only if $(a, b) = 1$ and $(a, c) = 1$.*

(a): Write $(a, b) = am + bn$; (b) follows from (a).

Relatively prime

Definition 6

The nonzero integers a and b are said to be **relatively prime** if $(a, b) = 1$.

Proposition. 1

$(a, b) = 1$ if and only if there exist integers m, n such that $ma + nb = 1$.

Proposition. 2

Let a, b, c be integers, where $a \neq 0$ or $b \neq 0$.

(a) *If $b|ac$, then $b|(a, b) \cdot c$.*

(b) *If $b|ac$ and $(a, b) = 1$, then $b|c$.*

(c) *If $b|a$, $c|a$ and $(b, c) = 1$, then $bc|a$.*

(d) *$(a, bc) = 1$ if and only if $(a, b) = 1$ and $(a, c) = 1$.*

(a): Write $(a, b) = am + bn$; (b) follows from (a).

(c): Write $a = bq$, so $c|bq$ and $(b, c) = 1$. Thus $c|q$ follows from (b).

Relatively prime

Definition 6

The nonzero integers a and b are said to be **relatively prime** if $(a, b) = 1$.

Proposition. 1

$(a, b) = 1$ if and only if there exist integers m, n such that $ma + nb = 1$.

Proposition. 2

Let a, b, c be integers, where $a \neq 0$ or $b \neq 0$.

(a) *If $b|ac$, then $b|(a, b) \cdot c$.*

(b) *If $b|ac$ and $(a, b) = 1$, then $b|c$.*

(c) *If $b|a$, $c|a$ and $(b, c) = 1$, then $bc|a$.*

(d) *$(a, bc) = 1$ if and only if $(a, b) = 1$ and $(a, c) = 1$.*

(a): Write $(a, b) = am + bn$; (b) follows from (a).
(c): Write $a = bq$, so $c|bq$ and $(b, c) = 1$. Thus $c|q$ follows from (b).
(d): "$\Leftarrow$:" $am_1 + bn_1 = 1, am_2 + cn_2 = 1 \Rightarrow (am_1 + bn_1)(am_2 + cn_2) = 1$.

Relatively prime

Definition 6

The nonzero integers a and b are said to be **relatively prime** if $(a, b) = 1$.

Proposition. 1

$(a, b) = 1$ if and only if there exist integers m, n such that $ma + nb = 1$.

Proposition. 2

Let a, b, c be integers, where $a \neq 0$ or $b \neq 0$.

(a) *If $b|ac$, then $b|(a, b) \cdot c$.*

(b) *If $b|ac$ and $(a, b) = 1$, then $b|c$.*

(c) *If $b|a, c|a$ and $(b, c) = 1$, then $bc|a$.*

(d) *$(a, bc) = 1$ if and only if $(a, b) = 1$ and $(a, c) = 1$.*

(a): Write $(a, b) = am + bn$; (b) follows from (a).
(c): Write $a = bq$, so $c|bq$ and $(b, c) = 1$. Thus $c|q$ follows from (b).
(d): "$\Leftarrow$:" $am_1 + bn_1 = 1, am_2 + cn_2 = 1 \Rightarrow (am_1 + bn_1)(am_2 + cn_2) = 1$.
"$\Rightarrow$:" Write $am + bcn = 1$, then $am + b(cn) = am + c(bn) = 1$ & Prop. 1.

Least Common Multiple

Definition 7

A positive integer m is called the **least common multiple** of the nonzero integers a and b if

1. m is a multiple of both a and b, and
2. any multiple of both a and b is also a multiple of m.

We will use the notation $\mathrm{lcm}[a, b]$ or $[a, b]$ for the least common multiple of a and b.

Least Common Multiple

Definition 7

A positive integer m is called the **least common multiple** of the nonzero integers a and b if

1. m is a multiple of both a and b, and
2. any multiple of both a and b is also a multiple of m.

We will use the notation $\mathrm{lcm}[a, b]$ or $[a, b]$ for the least common multiple of a and b.

Definition 8 (shortened version)

If a and b are nonzero integers, and m is a positive integer, then $m = \mathrm{lcm}[a, b]$ if

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

Least Common Multiple

Definition 7

A positive integer m is called the **least common multiple** of the nonzero integers a and b if

1. m is a multiple of both a and b, and
2. any multiple of both a and b is also a multiple of m.

We will use the notation $\mathrm{lcm}[a, b]$ or $[a, b]$ for the least common multiple of a and b.

Definition 8 (shortened version)

If a and b are nonzero integers, and m is a positive integer, then $m = \mathrm{lcm}[a, b]$ if

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

Note that $\gcd(a, b) \cdot \mathrm{lcm}[a, b] = ab$.

Congruences

Definition 9

Let n be a positive integer. Integers a and b are said to be **congruent modulo** n if they have the same remainder when divided by n. This is denoted by writing $a \equiv b \pmod{n}$.

Congruences

Definition 9

Let n be a positive integer. Integers a and b are said to be **congruent modulo** n if they have the same remainder when divided by n. This is denoted by writing $a \equiv b \pmod{n}$.

Write $a = nq + r$, where $0 \leq r < n$, then $r = n \cdot 0 + r$. It follows that

$$a \equiv r \pmod{n}.$$

Any integer is congruent modulo n to one of the integers $0, 1, 2, \ldots, n-1$.

Congruences

Definition 9

Let n be a positive integer. Integers a and b are said to be **congruent modulo** n if they have the same remainder when divided by n. This is denoted by writing $a \equiv b \pmod{n}$.

Write $a = nq + r$, where $0 \leq r < n$, then $r = n \cdot 0 + r$. It follows that

$$a \equiv r \pmod{n}.$$

Any integer is congruent modulo n to one of the integers $0, 1, 2, \ldots, n-1$.

Proposition. 3

Let $a, b, n \in \mathbf{Z}$ *and* $n > 0$. *Then* $a \equiv b \pmod{n}$ *if and only if* $n | (a - b)$.

Congruences

Definition 9

Let n be a positive integer. Integers a and b are said to be **congruent modulo** n if they have the same remainder when divided by n. This is denoted by writing $a \equiv b \pmod{n}$.

Write $a = nq + r$, where $0 \leq r < n$, then $r = n \cdot 0 + r$. It follows that

$$a \equiv r \pmod{n}.$$

Any integer is congruent modulo n to one of the integers $0, 1, 2, \ldots, n-1$.

Proposition. 3

Let $a, b, n \in \mathbf{Z}$ *and* $n > 0$. *Then* $a \equiv b \pmod{n}$ *if and only if* $n | (a - b)$.

$(\Rightarrow)$: Write $a = nq_1 + r$ and $b = nq_2 + r$, thus $a - b = n(q_1 - q_2)$.

Congruences

Definition 9

Let n be a positive integer. Integers a and b are said to be **congruent modulo** n if they have the same remainder when divided by n. This is denoted by writing $a \equiv b \pmod{n}$.

Write $a = nq + r$, where $0 \leq r < n$, then $r = n \cdot 0 + r$. It follows that

$$a \equiv r \pmod{n}.$$

Any integer is congruent modulo n to one of the integers $0, 1, 2, \ldots, n-1$.

Proposition. 3

Let $a, b, n \in \mathbf{Z}$ and $n > 0$. Then $a \equiv b \pmod{n}$ if and only if $n | (a - b)$.

$(\Rightarrow)$: Write $a = nq_1 + r$ and $b = nq_2 + r$, thus $a - b = n(q_1 - q_2)$.

$(\Leftarrow)$: Write $a - b = nk$ for some $k \in \mathbf{Z}$, hence $a = nk + b$.

Congruences

Definition 9

Let n be a positive integer. Integers a and b are said to be **congruent modulo** n if they have the same remainder when divided by n. This is denoted by writing $a \equiv b \pmod{n}$.

Write $a = nq + r$, where $0 \leq r < n$, then $r = n \cdot 0 + r$. It follows that

$$a \equiv r \pmod{n}.$$

Any integer is congruent modulo n to one of the integers $0, 1, 2, \ldots, n-1$.

Proposition. 3

Let $a, b, n \in \mathbf{Z}$ and $n > 0$. Then $a \equiv b \pmod{n}$ if and only if $n|(a-b)$.

$(\Rightarrow)$: Write $a = nq_1 + r$ and $b = nq_2 + r$, thus $a - b = n(q_1 - q_2)$.

$(\Leftarrow)$: Write $a - b = nk$ for some $k \in \mathbf{Z}$, hence $a = nk + b$.
Apply the division algorithm to write $a = nq + r$, with $0 \leq r < n$, then $b = a - nk = n(q-k) + r$. Thus, a and b have the same remainder r.

Properties of congruences

When working with congruence modulo n, the integer n is called the **modulus**.

Properties of congruences

When working with congruence modulo n, the integer n is called the **modulus**. Let a, b, c be integers. Then

(i) $a \equiv a \pmod{n}$;

(ii) if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$;

(iii) if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Properties of congruences

When working with congruence modulo n, the integer n is called the **modulus**.
Let a, b, c be integers. Then

(i) $a \equiv a \pmod{n}$;

(ii) if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$;

(iii) if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Proposition. 4

Let $n > 0$ be an integer. Then the following hold for all integers a, b, c, d:

1. *If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then $a \pm b \equiv c \pm d \pmod{n}$, and $ab \equiv cd \pmod{n}$.*
2. *If $a + c \equiv a + d \pmod{n}$, then $c \equiv d \pmod{n}$.*
3. *If $ac \equiv ad \pmod{n}$ and $(a, n) = 1$, then $c \equiv d \pmod{n}$.*

Properties of congruences

When working with congruence modulo n, the integer n is called the **modulus**. Let a, b, c be integers. Then

(i) $a \equiv a \pmod{n}$;

(ii) if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$;

(iii) if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Proposition. 4

Let $n > 0$ be an integer. Then the following hold for all integers a, b, c, d:

1. *If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then $a \pm b \equiv c \pm d \pmod{n}$, and $ab \equiv cd \pmod{n}$.*
2. *If $a + c \equiv a + d \pmod{n}$, then $c \equiv d \pmod{n}$.*
3. *If $ac \equiv ad \pmod{n}$ and $(a, n) = 1$, then $c \equiv d \pmod{n}$.*

The first two assertions easily follow from the previous proposition.

Properties of congruences

When working with congruence modulo n, the integer n is called the **modulus**.
Let a, b, c be integers. Then

(i) $a \equiv a \pmod{n}$;

(ii) if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$;

(iii) if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Proposition. 4

Let $n > 0$ be an integer. Then the following hold for all integers a, b, c, d:

1. *If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then $a \pm b \equiv c \pm d \pmod{n}$, and $ab \equiv cd \pmod{n}$.*
2. *If $a + c \equiv a + d \pmod{n}$, then $c \equiv d \pmod{n}$.*
3. *If $ac \equiv ad \pmod{n}$ and $(a, n) = 1$, then $c \equiv d \pmod{n}$.*

The first two assertions easily follow from the previous proposition.
For the third one: If $ac \equiv ad \pmod{n}$, then $n | a(c - d)$, and since $(n, a) = 1$, it follows from Proposition. 2 (b) that $n | (c - d)$.

Examples

I. You may divide both sides of a congruence by an integer a only if $(a, n) = 1$.

Examples

I. You may divide both sides of a congruence by an integer a only if $(a, n) = 1$.

Example. 1

$30 \equiv 6 \pmod 8$, *but dividing both sides by* 6 *gives* $5 \equiv 1 \pmod 8$, *which is certainly false because* $(6, 8) = 2 \neq 1$.

Examples

I. You may divide both sides of a congruence by an integer a only if $(a, n) = 1$.

Example. 1

$30 \equiv 6 \pmod 8$, *but dividing both sides by* 6 *gives* $5 \equiv 1 \pmod 8$, *which is certainly false because* $(6, 8) = 2 \neq 1$. *On the other hand, since* $(3, 8) = 1$, *we may divide both sides by* 3 *to get* $10 \equiv 2 \pmod 8$.

Examples

I. You may divide both sides of a congruence by an integer a only if $(a, n) = 1$.

Example. 1

$30 \equiv 6 \pmod 8$, *but dividing both sides by* 6 *gives* $5 \equiv 1 \pmod 8$, *which is certainly false because* $(6, 8) = 2 \neq 1$. *On the other hand, since* $(3, 8) = 1$, *we may divide both sides by* 3 *to get* $10 \equiv 2 \pmod 8$.

II. Proposition. 4 shows that the remainder upon division by n of $a + b$ or ab can be found by adding or multiplying the remainders of a and b when divided by n and then dividing by n again if necessary.

Examples

I. You may divide both sides of a congruence by an integer a only if $(a, n) = 1$.

Example. 1

$30 \equiv 6 \pmod 8$, *but dividing both sides by 6 gives* $5 \equiv 1 \pmod 8$, *which is certainly false because* $(6, 8) = 2 \neq 1$. *On the other hand, since* $(3, 8) = 1$, *we may divide both sides by 3 to get* $10 \equiv 2 \pmod 8$.

II. Proposition. 4 shows that the remainder upon division by n of $a + b$ or ab can be found by adding or multiplying the remainders of a and b when divided by n and then dividing by n again if necessary.

Example. 2

$101 \equiv 5 \pmod 8$ *and* $142 \equiv 6 \pmod 8 \Rightarrow 101 \cdot 142 \equiv 5 \cdot 6 \equiv 6 \pmod 8$.

Examples

I. You may divide both sides of a congruence by an integer a only if $(a, n) = 1$.

Example. 1

$30 \equiv 6 \pmod 8$, *but dividing both sides by* 6 *gives* $5 \equiv 1 \pmod 8$, *which is certainly false because* $(6, 8) = 2 \neq 1$. *On the other hand, since* $(3, 8) = 1$, *we may divide both sides by* 3 *to get* $10 \equiv 2 \pmod 8$.

II. Proposition. 4 shows that the remainder upon division by n of $a + b$ or ab can be found by adding or multiplying the remainders of a and b when divided by n and then dividing by n again if necessary.

Example. 2

$101 \equiv 5 \pmod 8$ *and* $142 \equiv 6 \pmod 8 \Rightarrow 101 \cdot 142 \equiv 5 \cdot 6 \equiv 6 \pmod 8$.

Example. 3

$2^2 \equiv 4 \pmod 7, 2^3 \equiv 2^2 2 \equiv 4 \cdot 2 \equiv 1 \pmod 7, 2^4 \equiv 2^3 2 \equiv 1 \cdot 2 \equiv 2 \pmod 7$.

Linear congruences, I

Proposition. 5

Let a and $n > 1$ be integers. There exists an integer b such that $ab \equiv 1 \pmod{n}$ if and only if $(a, n) = 1$.

Linear congruences, I

Proposition. 5

Let a and $n > 1$ be integers. There exists an integer b such that $ab \equiv 1 \pmod{n}$ if and only if $(a, n) = 1$.

$(\Rightarrow)$: Write $ab = 1 + qn$, then $b \cdot a + (-q) \cdot n = 1$, and so $(a, n) = 1$.

Linear congruences, I

Proposition. 5

Let a and $n > 1$ be integers. There exists an integer b such that $ab \equiv 1 \pmod{n}$ if and only if $(a, n) = 1$.

$(\Rightarrow)$: Write $ab = 1 + qn$, then $b \cdot a + (-q) \cdot n = 1$, and so $(a, n) = 1$.
$(\Leftarrow)$: Write $sa + tn = 1$, for some $s, t \in \mathbf{Z}$. Letting $b = s$ and proof is done.

Linear congruences, I

Proposition. 5

Let a and $n > 1$ be integers. There exists an integer b such that $ab \equiv 1 \pmod{n}$ if and only if $(a, n) = 1$.

$(\Rightarrow)$: Write $ab = 1 + qn$, then $b \cdot a + (-q) \cdot n = 1$, and so $(a, n) = 1$.
$(\Leftarrow)$: Write $sa + tn = 1$, for some $s, t \in \mathbf{Z}$. Letting $b = s$ and proof is done.

This proposition shows that the congruence

$$ax \equiv 1 \pmod{n}$$

has a solution if and only if $(a, n) = 1$.

Linear congruences, I

Proposition. 5

Let a and $n > 1$ be integers. There exists an integer b such that $ab \equiv 1 \pmod{n}$ if and only if $(a, n) = 1$.

$(\Rightarrow)$: Write $ab = 1 + qn$, then $b \cdot a + (-q) \cdot n = 1$, and so $(a, n) = 1$.
$(\Leftarrow)$: Write $sa + tn = 1$, for some $s, t \in \mathbf{Z}$. Letting $b = s$ and proof is done.

This proposition shows that the congruence

$$ax \equiv 1 \pmod{n}$$

has a solution if and only if $(a, n) = 1$.
And the solution can be obtained by using the **Euclidean algorithm** to write $1 = ab + nq$ for some $b, q \in \mathbf{Z}$, since then $1 \equiv ab \pmod{n}$.

Linear congruences, I

Proposition. 5

Let a and $n > 1$ be integers. There exists an integer b such that $ab \equiv 1 \pmod{n}$ if and only if $(a, n) = 1$.

$(\Rightarrow)$: Write $ab = 1 + qn$, then $b \cdot a + (-q) \cdot n = 1$, and so $(a, n) = 1$.
$(\Leftarrow)$: Write $sa + tn = 1$, for some $s, t \in \mathbf{Z}$. Letting $b = s$ and proof is done.

This proposition shows that the congruence

$$ax \equiv 1 \pmod{n}$$

has a solution if and only if $(a, n) = 1$.
And the solution can be obtained by using the **Euclidean algorithm** to write $1 = ab + nq$ for some $b, q \in \mathbf{Z}$, since then $1 \equiv ab \pmod{n}$.

Question. 1

How about the solutions of a linear congruence of the form $ax \equiv b \pmod{n}$?

Linear congruences, I

Proposition. 5

Let a and $n > 1$ be integers. There exists an integer b such that $ab \equiv 1 \pmod{n}$ if and only if $(a, n) = 1$.

$(\Rightarrow)$: Write $ab = 1 + qn$, then $b \cdot a + (-q) \cdot n = 1$, and so $(a, n) = 1$.
$(\Leftarrow)$: Write $sa + tn = 1$, for some $s, t \in \mathbf{Z}$. Letting $b = s$ and proof is done.

This proposition shows that the congruence

$$ax \equiv 1 \pmod{n}$$

has a solution if and only if $(a, n) = 1$.
And the solution can be obtained by using the **Euclidean algorithm** to write $1 = ab + nq$ for some $b, q \in \mathbf{Z}$, since then $1 \equiv ab \pmod{n}$.

Question. 1

How about the solutions of a linear congruence of the form $ax \equiv b \pmod{n}$?

We say that two solutions r and s to the congruence $ax \equiv b \pmod{n}$ are **distinct solutions modulo** n if r and s are not congruent modulo n.

Linear congruences, II

Theorem 10

Let a, b and $n > 1$ be integers.
(1) *The congruence $ax \equiv b \pmod{n}$ has a solution if and only if b is divisible by d, where $d = (a, n)$.*
(2) *If $d|b$, then there are d distinct solutions modulo n, and these solutions are congruent modulo n/d.*

Linear congruences, II

Theorem 10

Let a, b and $n > 1$ be integers.
(1) *The congruence $ax \equiv b \pmod{n}$ has a solution if and only if b is divisible by d, where $d = (a, n)$.*
(2) *If $d|b$, then there are d distinct solutions modulo n, and these solutions are congruent modulo n/d.*

(1) $ax \equiv b \pmod{n}$ has a solution if and only if $as = b + nq$, for some $s, q \in \mathbf{Z}$; i.e., $sa + (-q)n = b$. It implies that b can be expressed as a linear combination of a and n.

Linear congruences, II

Theorem 10

Let a, b and $n > 1$ be integers.
(1) *The congruence $ax \equiv b \pmod{n}$ has a solution if and only if b is divisible by d, where $d = (a, n)$.*
(2) *If $d|b$, then there are d distinct solutions modulo n, and these solutions are congruent modulo n/d.*

(1) $ax \equiv b \pmod{n}$ has a solution if and only if $as = b + nq$, for some $s, q \in \mathbf{Z}$; i.e., $sa + (-q)n = b$. It implies that b can be expressed as a linear combination of a and n. By Theorem 5 the linear combinations of a and n are precisely the multiples of d, so there is a solution if and only if $d|b$.

Linear congruences, II

Theorem 10

Let a, b and $n > 1$ be integers.
(1) The congruence $ax \equiv b \pmod{n}$ has a solution if and only if b is divisible by d, where $d = (a, n)$.
(2) If $d|b$, then there are d distinct solutions modulo n, and these solutions are congruent modulo n/d.

(1) $ax \equiv b \pmod{n}$ has a solution if and only if $as = b + nq$, for some $s, q \in \mathbf{Z}$; i.e., $sa + (-q)n = b$. It implies that b can be expressed as a linear combination of a and n. By Theorem 5 the linear combinations of a and n are precisely the multiples of d, so there is a solution if and only if $d|b$.

(2) Let $m = n/d$. Suppose x_1 and x_2 are solutions, $\Rightarrow ax_1 \equiv ax_2 \pmod{n}$. Then $n|a(x_1 - x_2)$, it follows from Proposition. 2 (a) that $n|d(x_1 - x_2)$. Thus $m|(x_1 - x_2)$, and so $x_1 \equiv x_2 \pmod{m}$.

Linear congruences, II

Theorem 10

Let a, b and $n > 1$ be integers.
(1) The congruence $ax \equiv b \pmod{n}$ has a solution if and only if b is divisible by d, where $d = (a, n)$.
(2) If $d|b$, then there are d distinct solutions modulo n, and these solutions are congruent modulo n/d.

(1) $ax \equiv b \pmod{n}$ has a solution if and only if $as = b + nq$, for some $s, q \in \mathbf{Z}$; i.e., $sa + (-q)n = b$. It implies that b can be expressed as a linear combination of a and n. By Theorem 5 the linear combinations of a and n are precisely the multiples of d, so there is a solution if and only if $d|b$.

(2) Let $m = n/d$. Suppose x_1 and x_2 are solutions, $\Rightarrow ax_1 \equiv ax_2 \pmod{n}$. Then $n|a(x_1 - x_2)$, it follows from Proposition. 2 (a) that $n|d(x_1 - x_2)$. Thus $m|(x_1 - x_2)$, and so $x_1 \equiv x_2 \pmod{m}$. On the other hand, if $x_1 \equiv x_2 \pmod{m} \Rightarrow m|(x_1 - x_2) \Rightarrow n|d(x_1 - x_2) \Rightarrow n|a(x_1 - x_2) \Rightarrow ax_1 \equiv ax_2 \pmod{n}$.

Linear congruences, II

Theorem 10

Let a, b and $n > 1$ be integers.
(1) The congruence $ax \equiv b \pmod{n}$ has a solution if and only if b is divisible by d, where $d = (a, n)$.
(2) If $d|b$, then there are d distinct solutions modulo n, and these solutions are congruent modulo n/d.

(1) $ax \equiv b \pmod{n}$ has a solution if and only if $as = b + nq$, for some $s, q \in \mathbf{Z}$; i.e., $sa + (-q)n = b$. It implies that b can be expressed as a linear combination of a and n. By Theorem 5 the linear combinations of a and n are precisely the multiples of d, so there is a solution if and only if $d|b$.

(2) Let $m = n/d$. Suppose x_1 and x_2 are solutions, $\Rightarrow ax_1 \equiv ax_2 \pmod{n}$. Then $n|a(x_1 - x_2)$, it follows from Proposition. 2 (a) that $n|d(x_1 - x_2)$. Thus $m|(x_1 - x_2)$, and so $x_1 \equiv x_2 \pmod{m}$. On the other hand, if $x_1 \equiv x_2 \pmod{m} \Rightarrow m|(x_1 - x_2) \Rightarrow n|d(x_1 - x_2) \Rightarrow n|a(x_1 - x_2) \Rightarrow ax_1 \equiv ax_2 \pmod{n}$. Given one such solution, we can find all others in the set by adding multiples of n/d, giving a total of d distinct solutions.

An algorithm for solving linear congruences

To linear congruences of the form $ax \equiv b \pmod{n}$:

An algorithm for solving linear congruences

To linear congruences of the form $ax \equiv b \pmod{n}$:

(i) Compute $d = (a, n)$, and if $d|b$, then we can write $ax = b + qn$.

An algorithm for solving linear congruences

To linear congruences of the form $ax \equiv b \pmod{n}$:

(i) Compute $d = (a, n)$, and if $d|b$, then we can write $ax = b + qn$.

(ii) Further, we get $a_1 x = b_1 + qm$, where $a_1 = a/d, b_1 = b/d, m = n/d$. This yields the congruence

$$a_1 x \equiv b_1 \pmod{m}, \quad \text{where } (a_1, m) = 1.$$

An algorithm for solving linear congruences

To linear congruences of the form $ax \equiv b \pmod{n}$:

(i) Compute $d = (a, n)$, and if $d | b$, then we can write $ax = b + qn$.

(ii) Further, we get $a_1 x = b_1 + qm$, where $a_1 = a/d, b_1 = b/d, m = n/d$. This yields the congruence

$$a_1 x \equiv b_1 \pmod{m}, \quad \text{where } (a_1, m) = 1.$$

(iii) Apply the Euclidean algorithm to find $c \in \mathbf{Z}$ s.t. $a_1 c \equiv 1 \pmod{m}$.

An algorithm for solving linear congruences

To linear congruences of the form $ax \equiv b \pmod{n}$:

(i) Compute $d = (a, n)$, and if $d|b$, then we can write $ax = b + qn$.

(ii) Further, we get $a_1 x = b_1 + qm$, where $a_1 = a/d, b_1 = b/d, m = n/d$. This yields the congruence

$$a_1 x \equiv b_1 \pmod{m}, \quad \text{where } (a_1, m) = 1.$$

(iii) Apply the Euclidean algorithm to find $c \in \mathbf{Z}$ s.t. $a_1 c \equiv 1 \pmod{m}$.

(iv) Multiplying both sides of the congruence $a_1 x \equiv b_1 \pmod{m}$ by c gives the solution

$$x \equiv c b_1 \pmod{m}.$$

An algorithm for solving linear congruences

To linear congruences of the form $ax \equiv b \pmod{n}$:

(i) Compute $d = (a, n)$, and if $d|b$, then we can write $ax = b + qn$.

(ii) Further, we get $a_1 x = b_1 + qm$, where $a_1 = a/d, b_1 = b/d, m = n/d$. This yields the congruence

$$a_1 x \equiv b_1 \pmod{m}, \quad \text{where } (a_1, m) = 1.$$

(iii) Apply the Euclidean algorithm to find $c \in \mathbf{Z}$ s.t. $a_1 c \equiv 1 \pmod{m}$.

(iv) Multiplying both sides of the congruence $a_1 x \equiv b_1 \pmod{m}$ by c gives the solution

$$x \equiv c b_1 \pmod{m}.$$

(v) The solution modulo m determines d distinct solutions modulo n. In particular, the solutions have the form

$$s_0 + km,$$

where s_0 is any particular solution of $x \equiv cb_1 \pmod{m}$ and k is any integer.

Example 1: Homogeneous linear congruences

Consider the special case of a linear homogeneous congruence

$$ax \equiv 0 \pmod{n}.$$

Example 1: Homogeneous linear congruences

Consider the special case of a linear homogeneous congruence

$$ax \equiv 0 \pmod{n}.$$

(i) Compute $d = (a, n)$.

Example 1: Homogeneous linear congruences

Consider the special case of a linear homogeneous congruence

$$ax \equiv 0 \pmod{n}.$$

(i) Compute $d = (a, n)$.

(ii) Consider $a_1 x \equiv 0 \pmod{n_1}$, where $a_1 = a/d$ and $n_1 = n/d$.

Example 1: Homogeneous linear congruences

Consider the special case of a linear homogeneous congruence

$$ax \equiv 0 \pmod{n}.$$

(i) Compute $d = (a, n)$.

(ii) Consider $a_1 x \equiv 0 \pmod{n_1}$, where $a_1 = a/d$ and $n_1 = n/d$.

(iii) Since $(a_1, n_1) = 1$, by Proposition. 4 (3) we can cancel a_1 to obtain

$$x \equiv 0 \pmod{n_1}, \quad \text{with } n_1 = \frac{n}{\gcd(a, n)}.$$

Example 1: Homogeneous linear congruences

Consider the special case of a linear homogeneous congruence

$$ax \equiv 0 \pmod{n}.$$

(i) Compute $d = (a, n)$.

(ii) Consider $a_1 x \equiv 0 \pmod{n_1}$, where $a_1 = a/d$ and $n_1 = n/d$.

(iii) Since $(a_1, n_1) = 1$, by Proposition. 4 (3) we can cancel a_1 to obtain

$$x \equiv 0 \pmod{n_1}, \quad \text{with } n_1 = \frac{n}{\gcd(a, n)}.$$

(iv) We have d distinct solutions modulo n.

Example 1: Homogeneous linear congruences

Consider the special case of a linear homogeneous congruence

$$ax \equiv 0 \pmod{n}.$$

(i) Compute $d = (a, n)$.

(ii) Consider $a_1 x \equiv 0 \pmod{n_1}$, where $a_1 = a/d$ and $n_1 = n/d$.

(iii) Since $(a_1, n_1) = 1$, by Proposition. 4 (3) we can cancel a_1 to obtain

$$x \equiv 0 \pmod{n_1}, \quad \text{with } n_1 = \frac{n}{\gcd(a, n)}.$$

(iv) We have d distinct solutions modulo n.

Example. 4

$28x \equiv 0 \pmod{48} \Rightarrow x \equiv 0 \pmod{12} \Rightarrow x \equiv 0, 12, 24, 36 \pmod{48}.$

Example 2

To solve the congruence

$$60x \equiv 90 \pmod{105}.$$

Example 2

To solve the congruence

$$60x \equiv 90 \pmod{105}.$$

(i) $d = (60, 105) = 15, \Rightarrow 15|90$ ✓: There will indeed be a solution.

Example 2

To solve the congruence

$$60x \equiv 90 \pmod{105}.$$

(i) $d = (60, 105) = 15, \Rightarrow 15|90$ ✓: There will indeed be a solution.
(ii) Reduces to the congruence

$$4x \equiv 6 \pmod{7}.$$

Example 2

To solve the congruence

$$60x \equiv 90 \pmod{105}.$$

(i) $d = (60, 105) = 15, \Rightarrow 15|90$ ✓: There will indeed be a solution.

(ii) Reduces to the congruence

$$4x \equiv 6 \pmod{7}.$$

(iii) Find an integer c with $c \cdot 4 \equiv 1 \pmod{7}$.

   (a) Euclidean algorithm

   (b) trial and error (is quicker for a small modulus) $\Rightarrow c = 2$.

Example 2

To solve the congruence

$$60x \equiv 90 \pmod{105}.$$

(i) $d = (60, 105) = 15, \Rightarrow 15|90$ ✓: There will indeed be a solution.
(ii) Reduces to the congruence

$$4x \equiv 6 \pmod{7}.$$

(iii) Find an integer c with $c \cdot 4 \equiv 1 \pmod{7}$.
  (a) Euclidean algorithm
  (b) trial and error (is quicker for a small modulus) $\Rightarrow c = 2$.
(iv) Multiply both sides of the congruence $4x \equiv 6 \pmod{7}$ by 2 to get

$$x \equiv 12 \equiv 5 \pmod{7}.$$

Example 2

To solve the congruence

$$60x \equiv 90 \pmod{105}.$$

(i) $d = (60, 105) = 15, \Rightarrow 15|90$ ✓: There will indeed be a solution.

(ii) Reduces to the congruence

$$4x \equiv 6 \pmod{7}.$$

(iii) Find an integer c with $c \cdot 4 \equiv 1 \pmod{7}$.
  (a) Euclidean algorithm
  (b) trial and error (is quicker for a small modulus) $\Rightarrow c = 2$.

(iv) Multiply both sides of the congruence $4x \equiv 6 \pmod{7}$ by 2 to get

$$x \equiv 12 \equiv 5 \pmod{7}.$$

(v) The solutions have the form $x = 5 + 7k$, so $x \equiv 5 + 7k \pmod{105}$.

Example 2

To solve the congruence

$$60x \equiv 90 \pmod{105}.$$

(i) $d = (60, 105) = 15, \Rightarrow 15|90$ ✓: There will indeed be a solution.

(ii) Reduces to the congruence

$$4x \equiv 6 \pmod{7}.$$

(iii) Find an integer c with $c \cdot 4 \equiv 1 \pmod{7}$.

   (a) Euclidean algorithm

   (b) trial and error (is quicker for a small modulus) $\Rightarrow c = 2$.

(iv) Multiply both sides of the congruence $4x \equiv 6 \pmod{7}$ by 2 to get

$$x \equiv 12 \equiv 5 \pmod{7}.$$

(v) The solutions have the form $x = 5 + 7k$, so $x \equiv 5 + 7k \pmod{105}$. There are 15 distinct solutions modulo 105, so we have $x \equiv 5, 12, 19, 26, 33, 40, 47, 54, 61, 68, 75, 82, 89, 96, 103 \pmod{105}$.

Chinese Remainder Theorem

Theorem 11 (Chinese Remainder Theorem)

Let n and m be positive integers, with $(n, m) = 1$. Then the system of congruences

$$x \equiv a \pmod{n} \qquad x \equiv b \pmod{m}$$

has a solution. Moreover, any two solutions are congruent modulo mn.

Chinese Remainder Theorem

Theorem 11 (Chinese Remainder Theorem)

Let n and m be positive integers, with $(n, m) = 1$. Then the system of congruences

$$x \equiv a \pmod{n} \qquad x \equiv b \pmod{m}$$

has a solution. Moreover, any two solutions are congruent modulo mn.

Since $(n, m) = 1$, there exist integers r and s such that $rm + sn = 1$. Then $rm \equiv 1 \pmod{n}$ and $sn \equiv 1 \pmod{m}$. Let

$$x = arm + bsn.$$

Then a direct computation verifies that x is a desired solution.

Chinese Remainder Theorem

Theorem 11 (Chinese Remainder Theorem)

Let n and m be positive integers, with $(n, m) = 1$. Then the system of congruences

$$x \equiv a \pmod{n} \qquad x \equiv b \pmod{m}$$

has a solution. Moreover, any two solutions are congruent modulo mn.

Since $(n, m) = 1$, there exist integers r and s such that $rm + sn = 1$. Then $rm \equiv 1 \pmod{n}$ and $sn \equiv 1 \pmod{m}$. Let

$$x = arm + bsn.$$

Then a direct computation verifies that x is a desired solution.

If x is solution, then adding any multiple of mn is obviously still a solution.

Chinese Remainder Theorem

Theorem 11 (Chinese Remainder Theorem)

Let n and m be positive integers, with $(n, m) = 1$. *Then the system of congruences*

$$x \equiv a \pmod{n} \qquad x \equiv b \pmod{m}$$

has a solution. Moreover, any two solutions are congruent modulo mn.

Since $(n, m) = 1$, there exist integers r and s such that $rm + sn = 1$. Then $rm \equiv 1 \pmod{n}$ and $sn \equiv 1 \pmod{m}$. Let

$$x = arm + bsn.$$

Then a direct computation verifies that x is a desired solution.

If x is solution, then adding any multiple of mn is obviously still a solution. Conversely, if x_1 and x_2 are two solutions, then they must be congruent modulo n and modulo m. Thus $n|(x_1 - x_2)$ and $m|(x_1 - x_2)$., so $mn|(x_1 - x_2)$ since $(n, m) = 1$. Therefore $x_1 \equiv x_2 \pmod{mn}$.

Example

Solve the system of congruences

$$x \equiv 7 \pmod{8} \qquad x \equiv 3 \pmod{5}.$$

Example

Solve the system of congruences

$$x \equiv 7 \pmod{8} \qquad x \equiv 3 \pmod{5}.$$

(a) Use the Euclidean algorithm to write $2 \cdot 8 + (-3) \cdot 5 = 1$.

Example

Solve the system of congruences

$$x \equiv 7 \pmod{8} \qquad\qquad x \equiv 3 \pmod{5}.$$

(a) Use the Euclidean algorithm to write $2 \cdot 8 + (-3) \cdot 5 = 1$.
(b) Then $x = 7(-3)5 + 3(2)(8) = -57$ is a solution.

Example

Solve the system of congruences

$$x \equiv 7 \pmod 8 \qquad x \equiv 3 \pmod 5.$$

(a) Use the Euclidean algorithm to write $2 \cdot 8 + (-3) \cdot 5 = 1$.

(b) Then $x = 7(-3)5 + 3(2)(8) = -57$ is a solution.

(c) The general solution is $x = -57 + 40t$.

Example

Solve the system of congruences

$$x \equiv 7 \pmod{8} \qquad x \equiv 3 \pmod{5}.$$

(a) Use the Euclidean algorithm to write $2 \cdot 8 + (-3) \cdot 5 = 1$.

(b) Then $x = 7(-3)5 + 3(2)(8) = -57$ is a solution.

(c) The general solution is $x = -57 + 40t$. The smallest nonnegative solution is therefore 23, so we have

$$x \equiv 23 \pmod{40}.$$

Another proof of the existence of a solution in CRT

Given the congruences

$$x \equiv a \pmod{n} \qquad x \equiv b \pmod{m}.$$

Another proof of the existence of a solution in CRT

Given the congruences

$$x \equiv a \pmod{n} \qquad x \equiv b \pmod{m}.$$

(i) Rewrite the first congruence as $x = a + qn$ for some $q \in \mathbf{Z}$.

Another proof of the existence of a solution in CRT

Given the congruences

$$x \equiv a \pmod{n} \qquad x \equiv b \pmod{m}.$$

(i) Rewrite the first congruence as $x = a + qn$ for some $q \in \mathbf{Z}$.
(ii) Substitute this expression for x in the second congruence, giving

$$a + qn \equiv b \pmod{m}, \quad \text{or} \quad qn \equiv b - a \pmod{m}.$$

Another proof of the existence of a solution in CRT

Given the congruences

$$x \equiv a \pmod{n} \qquad x \equiv b \pmod{m}.$$

(i) Rewrite the first congruence as $x = a + qn$ for some $q \in \mathbf{Z}$.

(ii) Substitute this expression for x in the second congruence, giving

$$a + qn \equiv b \pmod{m}, \quad \text{or} \quad qn \equiv b - a \pmod{m}.$$

(iii) Since $(n, m) = 1$, we can solve the congruence $nz \equiv 1 \pmod{m}$.

Another proof of the existence of a solution in CRT

Given the congruences

$$x \equiv a \pmod{n} \qquad x \equiv b \pmod{m}.$$

(i) Rewrite the first congruence as $x = a + qn$ for some $q \in \mathbf{Z}$.

(ii) Substitute this expression for x in the second congruence, giving

$$a + qn \equiv b \pmod{m}, \quad \text{or} \quad qn \equiv b - a \pmod{m}.$$

(iii) Since $(n, m) = 1$, we can solve the congruence $nz \equiv 1 \pmod{m}$.

(iv) Using this solution we can solve for q in $qn \equiv b - a \pmod{m}$.
In particular, $q \equiv (b - a)z \pmod{m} \Rightarrow x = a + ((b - a)z + km)n$.
That is,

$$x \equiv a + (b - a)zn \pmod{mn}.$$

Example revisited

Solve the system of congruences

$$x \equiv 7 \pmod{8} \qquad\qquad x \equiv 3 \pmod{5}.$$

Example revisited

Solve the system of congruences

$$x \equiv 7 \pmod{8} \qquad x \equiv 3 \pmod{5}.$$

(i) $x = 7 + 8q$.

Example revisited

Solve the system of congruences

$$x \equiv 7 \pmod{8} \qquad x \equiv 3 \pmod{5}.$$

(i) $x = 7 + 8q$.

(ii) $7 + 8q \equiv 3 \pmod{5} \Leftrightarrow 3q \equiv -4 \equiv 1 \pmod{5}$.

Example revisited

Solve the system of congruences

$$x \equiv 7 \pmod{8} \qquad x \equiv 3 \pmod{5}.$$

(i) $x = 7 + 8q$.

(ii) $7 + 8q \equiv 3 \pmod{5} \Leftrightarrow 3q \equiv -4 \equiv 1 \pmod{5}$.

(iii) Trial and error: $q \equiv 2 \pmod{5}$.

Example revisited

Solve the system of congruences

$$x \equiv 7 \pmod{8} \qquad\qquad x \equiv 3 \pmod{5}.$$

(i) $x = 7 + 8q$.

(ii) $7 + 8q \equiv 3 \pmod{5} \Leftrightarrow 3q \equiv -4 \equiv 1 \pmod{5}$.

(iii) Trial and error: $q \equiv 2 \pmod{5}$.

(iv) The particular solution $x = 7 + 8 \cdot 2 = 23$.

Example revisited

Solve the system of congruences

$$x \equiv 7 \pmod{8} \qquad x \equiv 3 \pmod{5}.$$

(i) $x = 7 + 8q$.

(ii) $7 + 8q \equiv 3 \pmod{5} \Leftrightarrow 3q \equiv -4 \equiv 1 \pmod{5}$.

(iii) Trial and error: $q \equiv 2 \pmod{5}$.

(iv) The particular solution $x = 7 + 8 \cdot 2 = 23$. So we have

$$x \equiv 23 \pmod{40}.$$

Congruence classes modulo n

Definition 12

Let a and $n > 0$ be integers. The set of all integers which have the same remainder as a when divided by n is called the **congruence class of** a **modulo** n, and is denoted by $[a]_n$, where

$$[a]_n = \{x \in \mathbf{Z} \mid x \equiv a \pmod{n}\}.$$

Congruence classes modulo n

Definition 12

Let a and $n > 0$ be integers. The set of all integers which have the same remainder as a when divided by n is called the **congruence class of a modulo n**, and is denoted by $[a]_n$, where

$$[a]_n = \{x \in \mathbf{Z} \mid x \equiv a \pmod{n}\}.$$

The collection of all congruence classes modulo n is called the **set of integers modulo n**, denoted by $\mathbf{Z}_n$.

Congruence classes modulo n

Definition 12

Let a and $n > 0$ be integers. The set of all integers which have the same remainder as a when divided by n is called the **congruence class of a modulo n**, and is denoted by $[a]_n$, where

$$[a]_n = \{x \in \mathbf{Z} \mid x \equiv a \pmod{n}\}.$$

The collection of all congruence classes modulo n is called the **set of integers modulo n**, denoted by $\mathbf{Z}_n$.

Note that $[a]_n = [b]_n$ if and only if $a \equiv b \pmod{n}$.

Congruence classes modulo n

Definition 12

Let a and $n > 0$ be integers. The set of all integers which have the same remainder as a when divided by n is called the **congruence class of a modulo n**, and is denoted by $[a]_n$, where

$$[a]_n = \{x \in \mathbf{Z} \mid x \equiv a \pmod{n}\}.$$

The collection of all congruence classes modulo n is called the **set of integers modulo n**, denoted by $\mathbf{Z}_n$.

Note that $[a]_n = [b]_n$ if and only if $a \equiv b \pmod{n}$.

We say that an element of $[a]_n$ is a **representative of the congruence class**. Each congruence class $[a]_n$ has a unique nonnegative representative that is smaller than n, namely, the remainder when a is divided by n.

Congruence classes modulo n

Definition 12

Let a and $n > 0$ be integers. The set of all integers which have the same remainder as a when divided by n is called the **congruence class of a modulo n**, and is denoted by $[a]_n$, where

$$[a]_n = \{x \in \mathbf{Z} \mid x \equiv a \pmod{n}\}.$$

The collection of all congruence classes modulo n is called the **set of integers modulo n**, denoted by $\mathbf{Z}_n$.

Note that $[a]_n = [b]_n$ if and only if $a \equiv b \pmod{n}$.

We say that an element of $[a]_n$ is a **representative of the congruence class**. Each congruence class $[a]_n$ has a unique nonnegative representative that is smaller than n, namely, the remainder when a is divided by n.

This shows that there are exactly n distinct congruence classes modulo n.

Example

Example. 5

The congruence classes modulo 3 can be represented by 0, 1, and 2.

$$[0]_3 = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$
$$[1]_3 = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$$
$$[2]_3 = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$$

Example

Example. 5

The congruence classes modulo 3 can be represented by 0, 1, and 2.

$$
\begin{aligned}
[0]_3 =& \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} \\
[1]_3 =& \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\} \\
[2]_3 =& \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}
\end{aligned}
$$

In general, each integer belongs to a unique congruence class modulo n. Hence we have

$$\mathbf{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}.$$

Addition and Multiplication of congruence classes, I

The set $\mathbf{Z}_2$ consists of $[0]_2$ and $[1]_2$, where $[0]_2$ is the set of even numbers and $[1]_2$ is the set of odd numbers.

Addition and Multiplication of congruence classes, I

The set $\mathbf{Z}_2$ consists of $[0]_2$ and $[1]_2$, where $[0]_2$ is the set of even numbers and $[1]_2$ is the set of odd numbers.

Example. 6 (Addition and Multiplication in $\mathbf{Z}_2$)

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

Addition and Multiplication of congruence classes, I

The set $\mathbf{Z}_2$ consists of $[0]_2$ and $[1]_2$, where $[0]_2$ is the set of even numbers and $[1]_2$ is the set of odd numbers.

Example. 6 (Addition and Multiplication in $\mathbf{Z}_2$)

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

Addition and Multiplication of congruence classes, I

The set $\mathbf{Z}_2$ consists of $[0]_2$ and $[1]_2$, where $[0]_2$ is the set of even numbers and $[1]_2$ is the set of odd numbers.

Example. 6 (Addition and Multiplication in $\mathbf{Z}_2$)

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

Proposition. 6

Let n be a positive integer, and let a, b be any integers. Then the addition and multiplication of congruence classes given below are well-defined:

$$[a]_n + [b]_n = [a+b]_n, \qquad [a]_n \cdot [b]_n = [ab]_n.$$

Addition and Multiplication of congruence classes, II

For any elements $[a]_n, [b]_n, [c]_n \in \mathbf{Z}_n$, the following laws hold.

Associativity: $([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)$

$$([a]_n \cdot [b]_n) \cdot [c]_n = [a]_n \cdot ([b]_n \cdot [c]_n)$$

Commutativity: $[a]_n + [b]_n = [b]_n + [a]_n \qquad [a]_n \cdot [b]_n = [b]_n \cdot [a]_n$

Distributivity: $[a]_n \cdot ([b]_n + [c]_n) = [a]_n \cdot [b]_n + [a]_n \cdot [c]_n$

Identities: $[a]_n + [0]_n = [a]_n \qquad [a]_n \cdot [1]_n = [a]_n$

Additive inverses: $[a]_n + [-a]_n = [0]_n$

Addition and Multiplication of congruence classes, II

For any elements $[a]_n, [b]_n, [c]_n \in \mathbf{Z}_n$, the following laws hold.

Associativity: $$([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)$$
$$([a]_n \cdot [b]_n) \cdot [c]_n = [a]_n \cdot ([b]_n \cdot [c]_n)$$

Commutativity: $[a]_n + [b]_n = [b]_n + [a]_n \qquad [a]_n \cdot [b]_n = [b]_n \cdot [a]_n$

Distributivity: $[a]_n \cdot ([b]_n + [c]_n) = [a]_n \cdot [b]_n + [a]_n \cdot [c]_n$

Identities: $[a]_n + [0]_n = [a]_n \qquad [a]_n \cdot [1]_n = [a]_n$

Additive inverses: $[a]_n + [-a]_n = [0]_n$

Proof of distributive law:

$$\begin{aligned} [a]_n \cdot ([b]_n + [c]_n) =& [a]_n \cdot ([b+c]_n) = [a(b+c)]_n \\ =& [ab+ac]_n = [ab]_n + [ac]_n \\ =& [a]_n \cdot [b]_n + [a]_n \cdot [c]_n. \end{aligned}$$

Addition and Multiplication of congruence classes, II

For any elements $[a]_n, [b]_n, [c]_n \in \mathbf{Z}_n$, the following laws hold.

Associativity: $$([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)$$
$$([a]_n \cdot [b]_n) \cdot [c]_n = [a]_n \cdot ([b]_n \cdot [c]_n)$$

Commutativity: $[a]_n + [b]_n = [b]_n + [a]_n \qquad [a]_n \cdot [b]_n = [b]_n \cdot [a]_n$

Distributivity: $[a]_n \cdot ([b]_n + [c]_n) = [a]_n \cdot [b]_n + [a]_n \cdot [c]_n$

Identities: $[a]_n + [0]_n = [a]_n \qquad [a]_n \cdot [1]_n = [a]_n$

Additive inverses: $[a]_n + [-a]_n = [0]_n$

Proof of distributive law:

$$\begin{aligned} [a]_n \cdot ([b]_n + [c]_n) =& [a]_n \cdot ([b+c]_n) = [a(b+c)]_n \\ =& [ab+ac]_n = [ab]_n + [ac]_n \\ =& [a]_n \cdot [b]_n + [a]_n \cdot [c]_n. \end{aligned}$$

No cancellation law: For example, $[6]_8 \cdot [5]_8 = [6]_8 \cdot [1]_8$, but $[5]_8 \neq [1]_8$.

Divisor of zero vs. Unit in $\mathbf{Z}_n$, I

Definition 13

If $[a]_n \in \mathbf{Z}_n$, and $[a]_n[b]_n = [0]_n$ for some nonzero congruence class $[b]_n$, then $[a]_n$ is called a **divisor of zero**.

Divisor of zero vs. Unit in $\mathbf{Z}_n$, I

Definition 13

If $[a]_n \in \mathbf{Z}_n$, and $[a]_n[b]_n = [0]_n$ for some nonzero congruence class $[b]_n$, then $[a]_n$ is called a **divisor of zero**.

If $[a]_n$ is not a divisor of zero, then $[a]_n[b]_n = [a]_n[c]_n \Rightarrow [b]_n = [c]_n$.

Divisor of zero vs. Unit in $\mathbf{Z}_n$, I

Definition 13

If $[a]_n \in \mathbf{Z}_n$, and $[a]_n[b]_n = [0]_n$ for some nonzero congruence class $[b]_n$, then $[a]_n$ is called a **divisor of zero**.

If $[a]_n$ is not a divisor of zero, then $[a]_n[b]_n = [a]_n[c]_n \Rightarrow [b]_n = [c]_n$.
Proof: $[a]_n([b]_n - [c]_n) = [a]_n[b-c]_n = [0]_n \Rightarrow [b]_n - [c]_n$ must be zero.

Divisor of zero vs. Unit in $\mathbf{Z}_n$, I

Definition 13

If $[a]_n \in \mathbf{Z}_n$, and $[a]_n[b]_n = [0]_n$ for some nonzero congruence class $[b]_n$, then $[a]_n$ is called a **divisor of zero**.

If $[a]_n$ is not a divisor of zero, then $[a]_n[b]_n = [a]_n[c]_n \Rightarrow [b]_n = [c]_n$.
Proof: $[a]_n([b]_n - [c]_n) = [a]_n[b-c]_n = [0]_n \Rightarrow [b]_n - [c]_n$ must be zero.

Definition 14

If $[a]_n \in \mathbf{Z}_n$, and $[a]_n[b]_n = [1]_n$ for some congruence class $[b]_n$, then $[b]_n$ is called a **multiplicative inverse** of $[a]_n$ and is denoted by $[a]_n^{-1}$. In this case, we say that $[a]_n$ is an **invertible** element of $\mathbf{Z}_n$, or a **unit** of $\mathbf{Z}_n$.

Divisor of zero vs. Unit in $\mathbf{Z}_n$, I

Definition 13

If $[a]_n \in \mathbf{Z}_n$, and $[a]_n[b]_n = [0]_n$ for some nonzero congruence class $[b]_n$, then $[a]_n$ is called a **divisor of zero**.

If $[a]_n$ is not a divisor of zero, then $[a]_n[b]_n = [a]_n[c]_n \Rightarrow [b]_n = [c]_n$.
Proof: $[a]_n([b]_n - [c]_n) = [a]_n[b-c]_n = [0]_n \Rightarrow [b]_n - [c]_n$ must be zero.

Definition 14

If $[a]_n \in \mathbf{Z}_n$, and $[a]_n[b]_n = [1]_n$ for some congruence class $[b]_n$, then $[b]_n$ is called a **multiplicative inverse** of $[a]_n$ and is denoted by $[a]_n^{-1}$. In this case, we say that $[a]_n$ is an **invertible** element of $\mathbf{Z}_n$, or a **unit** of $\mathbf{Z}_n$.

From this point on, if the meaning is clear from the context we will omit the subscript on congruence classes.

Divisor of zero vs. Unit in $\mathbf{Z}_n$, I

Definition 13

If $[a]_n \in \mathbf{Z}_n$, and $[a]_n[b]_n = [0]_n$ for some nonzero congruence class $[b]_n$, then $[a]_n$ is called a **divisor of zero**.

If $[a]_n$ is not a divisor of zero, then $[a]_n[b]_n = [a]_n[c]_n \Rightarrow [b]_n = [c]_n$.
Proof: $[a]_n([b]_n - [c]_n) = [a]_n[b-c]_n = [0]_n \Rightarrow [b]_n - [c]_n$ must be zero.

Definition 14

If $[a]_n \in \mathbf{Z}_n$, and $[a]_n[b]_n = [1]_n$ for some congruence class $[b]_n$, then $[b]_n$ is called a **multiplicative inverse** of $[a]_n$ and is denoted by $[a]_n^{-1}$. In this case, we say that $[a]_n$ is an **invertible** element of $\mathbf{Z}_n$, or a **unit** of $\mathbf{Z}_n$.

From this point on, if the meaning is clear from the context we will omit the subscript on congruence classes.

In $\mathbf{Z}_n$, if $[a]$ has a multiplicative inverse, then it cannot be a divisor of zero.

Divisor of zero vs. Unit in $\mathbf{Z}_n$, I

Definition 13

If $[a]_n \in \mathbf{Z}_n$, and $[a]_n[b]_n = [0]_n$ for some nonzero congruence class $[b]_n$, then $[a]_n$ is called a **divisor of zero**.

If $[a]_n$ is not a divisor of zero, then $[a]_n[b]_n = [a]_n[c]_n \Rightarrow [b]_n = [c]_n$.
Proof: $[a]_n([b]_n - [c]_n) = [a]_n[b-c]_n = [0]_n \Rightarrow [b]_n - [c]_n$ must be zero.

Definition 14

If $[a]_n \in \mathbf{Z}_n$, and $[a]_n[b]_n = [1]_n$ for some congruence class $[b]_n$, then $[b]_n$ is called a **multiplicative inverse** of $[a]_n$ and is denoted by $[a]_n^{-1}$. In this case, we say that $[a]_n$ is an **invertible** element of $\mathbf{Z}_n$, or a **unit** of $\mathbf{Z}_n$.

From this point on, if the meaning is clear from the context we will omit the subscript on congruence classes.

In $\mathbf{Z}_n$, if $[a]$ has a multiplicative inverse, then it cannot be a divisor of zero.
Proof: $[a][b] = [0] \Rightarrow [b] = [a]^{-1}[a] \cdot [b] = [a]^{-1}([a][b]) = [a]^{-1}[0] = [0]$.

Divisor of zero vs. Unit in $\mathbf{Z}_n$, II

Proposition. 7

(a) $[a]_n$ *has a multiplicative inverse in* $\mathbf{Z}_n$ *if and only if* $(a, n) = 1$.

(b) *A nonzero element of* $\mathbf{Z}_n$ *is either a unit or a divisor of zero.*

Divisor of zero vs. Unit in $\mathbf{Z}_n$, II

Proposition. 7

(a) $[a]_n$ *has a multiplicative inverse in* $\mathbf{Z}_n$ *if and only if* $(a, n) = 1$.

(b) *A nonzero element of* $\mathbf{Z}_n$ *is either a unit or a divisor of zero.*

(a) $(\Rightarrow)$ Say $[a]^{-1} = [b]$, then $[a][b] = [1] \Rightarrow ab \equiv 1 \pmod{n} \Rightarrow (a, n) = 1$

Divisor of zero vs. Unit in $\mathbf{Z}_n$, II

Proposition. 7

(a) $[a]_n$ *has a multiplicative inverse in* $\mathbf{Z}_n$ *if and only if* $(a, n) = 1$.

(b) *A nonzero element of* $\mathbf{Z}_n$ *is either a unit or a divisor of zero.*

(a) $(\Rightarrow)$ Say $[a]^{-1} = [b]$, then $[a][b] = [1] \Rightarrow ab \equiv 1 \pmod{n} \Rightarrow (a, n) = 1$
$(\Leftarrow)$ Write $ab + qn = 1$ for $b, q \in \mathbf{Z}$. So $ab \equiv 1 \pmod{n} \Rightarrow [b] = [a]^{-1}$.

Divisor of zero vs. Unit in $\mathbf{Z}_n$, II

Proposition. 7

(a) *$[a]_n$ has a multiplicative inverse in $\mathbf{Z}_n$ if and only if $(a, n) = 1$.*

(b) *A nonzero element of $\mathbf{Z}_n$ is either a unit or a divisor of zero.*

(a) ($\Rightarrow$) Say $[a]^{-1} = [b]$, then $[a][b] = [1] \Rightarrow ab \equiv 1 \pmod{n} \Rightarrow (a, n) = 1$
($\Leftarrow$) Write $ab + qn = 1$ for $b, q \in \mathbf{Z}$. So $ab \equiv 1 \pmod{n} \Rightarrow [b] = [a]^{-1}$.
(b) "nonzero" $\Rightarrow n \nmid a$.

Divisor of zero vs. Unit in $\mathbf{Z}_n$, II

Proposition. 7

(a) $[a]_n$ *has a multiplicative inverse in* $\mathbf{Z}_n$ *if and only if* $(a, n) = 1$.

(b) *A nonzero element of* $\mathbf{Z}_n$ *is either a unit or a divisor of zero.*

(a) $(\Rightarrow)$ Say $[a]^{-1} = [b]$, then $[a][b] = [1] \Rightarrow ab \equiv 1 \pmod{n} \Rightarrow (a, n) = 1$
$(\Leftarrow)$ Write $ab + qn = 1$ for $b, q \in \mathbf{Z}$. So $ab \equiv 1 \pmod{n} \Rightarrow [b] = [a]^{-1}$.
(b) "nonzero" $\Rightarrow n \nmid a$. If $(a, n) = 1$, then $[a]$ is a unit.

Divisor of zero vs. Unit in $\mathbf{Z}_n$, II

Proposition. 7

(a) *$[a]_n$ has a multiplicative inverse in $\mathbf{Z}_n$ if and only if $(a, n) = 1$.*

(b) *A nonzero element of $\mathbf{Z}_n$ is either a unit or a divisor of zero.*

(a) ($\Rightarrow$) Say $[a]^{-1} = [b]$, then $[a][b] = [1] \Rightarrow ab \equiv 1 \pmod{n} \Rightarrow (a, n) = 1$
($\Leftarrow$) Write $ab + qn = 1$ for $b, q \in \mathbf{Z}$. So $ab \equiv 1 \pmod{n} \Rightarrow [b] = [a]^{-1}$.
(b) "nonzero" $\Rightarrow n \nmid a$. If $(a, n) = 1$, then $[a]$ is a unit. If not, then $(a, n) = d$, where $1 < d < n$.

Divisor of zero vs. Unit in $\mathbf{Z}_n$, II

Proposition. 7

(a) *$[a]_n$ has a multiplicative inverse in $\mathbf{Z}_n$ if and only if $(a, n) = 1$.*

(b) *A nonzero element of $\mathbf{Z}_n$ is either a unit or a divisor of zero.*

(a) ($\Rightarrow$) Say $[a]^{-1} = [b]$, then $[a][b] = [1] \Rightarrow ab \equiv 1 \pmod{n} \Rightarrow (a, n) = 1$
($\Leftarrow$) Write $ab + qn = 1$ for $b, q \in \mathbf{Z}$. So $ab \equiv 1 \pmod{n} \Rightarrow [b] = [a]^{-1}$.
(b) "nonzero" $\Rightarrow n \nmid a$. If $(a, n) = 1$, then $[a]$ is a unit. If not, then $(a, n) = d$, where $1 < d < n$. Write $n = kd$ and $a = bd$. Then $[k] \neq [0]$ in $\mathbf{Z}_n$, but $[a][k] = [ak] = [bdk] = [bn] = [0]$. So $[a]$ is a divisor of zero.

Divisor of zero vs. Unit in $\mathbf{Z}_n$, II

Proposition. 7

(a) *$[a]_n$ has a multiplicative inverse in $\mathbf{Z}_n$ if and only if $(a, n) = 1$.*

(b) *A nonzero element of $\mathbf{Z}_n$ is either a unit or a divisor of zero.*

(a) ($\Rightarrow$) Say $[a]^{-1} = [b]$, then $[a][b] = [1] \Rightarrow ab \equiv 1 \pmod{n} \Rightarrow (a, n) = 1$
($\Leftarrow$) Write $ab + qn = 1$ for $b, q \in \mathbf{Z}$. So $ab \equiv 1 \pmod{n} \Rightarrow [b] = [a]^{-1}$.
(b) "nonzero"$\Rightarrow n \nmid a$. If $(a, n) = 1$, then $[a]$ is a unit. If not, then $(a, n) = d$, where $1 < d < n$. Write $n = kd$ and $a = bd$. Then $[k] \neq [0]$ in $\mathbf{Z}_n$, but $[a][k] = [ak] = [bdk] = [bn] = [0]$. So $[a]$ is a divisor of zero.

Corollary 15

The following conditions on the modulus $n > 0$ are equivalent.

(1) *The number n is prime.*

(2) *$\mathbf{Z}_n$ has no divisors of zero, except $[0]_n$.*

(3) *Every nonzero element of $\mathbf{Z}_n$ has a multiplicative inverse.*

Examples: Find the multiplicative inverse $[a]^{-1}$

I. Find $[11]^{-1}$ in $\mathbf{Z}_{16}$ using the matrix form of the Euclidean algorithm:

Examples: Find the multiplicative inverse $[a]^{-1}$

I. Find $[11]^{-1}$ in $\mathbf{Z}_{16}$ using the matrix form of the Euclidean algorithm:

$$\begin{bmatrix} 1 & 0 & 16 \\ 0 & 1 & 11 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 5 \\ 0 & 1 & 11 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 5 \\ -2 & 3 & 1 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 11 & -16 & 0 \\ -2 & 3 & 1 \end{bmatrix}$$

Thus $(-2) \cdot 16 + 3 \cdot 11 = 1$, which shows that $[11]_{16}^{-1} = [3]_{16}$.

Examples: Find the multiplicative inverse $[a]^{-1}$

I. Find $[11]^{-1}$ in $\mathbf{Z}_{16}$ using the matrix form of the Euclidean algorithm:

$$\begin{bmatrix} 1 & 0 & 16 \\ 0 & 1 & 11 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 5 \\ 0 & 1 & 11 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 5 \\ -2 & 3 & 1 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 11 & -16 & 0 \\ -2 & 3 & 1 \end{bmatrix}$$

Thus $(-2) \cdot 16 + 3 \cdot 11 = 1$, which shows that $[11]_{16}^{-1} = [3]_{16}$.

II. Find $[11]^{-1}$ in $\mathbf{Z}_{16}$ by taking successive powers of $[11]$:

Examples: Find the multiplicative inverse $[a]^{-1}$

I. Find $[11]^{-1}$ in $\mathbf{Z}_{16}$ using the matrix form of the Euclidean algorithm:

$$\begin{bmatrix} 1 & 0 & 16 \\ 0 & 1 & 11 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 5 \\ 0 & 1 & 11 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 5 \\ -2 & 3 & 1 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 11 & -16 & 0 \\ -2 & 3 & 1 \end{bmatrix}$$

Thus $(-2) \cdot 16 + 3 \cdot 11 = 1$, which shows that $[11]_{16}^{-1} = [3]_{16}$.

II. Find $[11]^{-1}$ in $\mathbf{Z}_{16}$ by taking successive powers of $[11]$:
List list the powers of $[11]$:
$[11]^2 = [-5]^2 = [25] = [9]$, $\quad [11]^3 = [11]^2[11] = [99] = [3]$, and
$[11]^4 = [11]^3[11] = [33] = [1]$. Thus again we see that $[11]_{16}^{-1} = [3]_{16}$.

Examples: Find the multiplicative inverse $[a]^{-1}$

I. Find $[11]^{-1}$ in $\mathbf{Z}_{16}$ using the matrix form of the Euclidean algorithm:

$$\begin{bmatrix} 1 & 0 & 16 \\ 0 & 1 & 11 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 5 \\ 0 & 1 & 11 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 5 \\ -2 & 3 & 1 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 11 & -16 & 0 \\ -2 & 3 & 1 \end{bmatrix}$$

Thus $(-2) \cdot 16 + 3 \cdot 11 = 1$, which shows that $[11]_{16}^{-1} = [3]_{16}$.

II. Find $[11]^{-1}$ in $\mathbf{Z}_{16}$ by taking successive powers of $[11]$:
List list the powers of $[11]$:
$[11]^2 = [-5]^2 = [25] = [9], \quad [11]^3 = [11]^2[11] = [99] = [3]$, and
$[11]^4 = [11]^3[11] = [33] = [1]$. Thus again we see that $[11]_{16}^{-1} = [3]_{16}$.

II. Find $[11]^{-1}$ in $\mathbf{Z}_{16}$ using trial and error (for small numbers):

Examples: Find the multiplicative inverse $[a]^{-1}$

I. Find $[11]^{-1}$ in $\mathbf{Z}_{16}$ using the matrix form of the Euclidean algorithm:

$$\begin{bmatrix} 1 & 0 & 16 \\ 0 & 1 & 11 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 5 \\ 0 & 1 & 11 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 5 \\ -2 & 3 & 1 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 11 & -16 & 0 \\ -2 & 3 & 1 \end{bmatrix}$$

Thus $(-2) \cdot 16 + 3 \cdot 11 = 1$, which shows that $[11]_{16}^{-1} = [3]_{16}$.

II. Find $[11]^{-1}$ in $\mathbf{Z}_{16}$ by taking successive powers of $[11]$:
List list the powers of $[11]$:
$[11]^2 = [-5]^2 = [25] = [9]$, $\quad [11]^3 = [11]^2[11] = [99] = [3]$, and
$[11]^4 = [11]^3[11] = [33] = [1]$. Thus again we see that $[11]_{16}^{-1} = [3]_{16}$.

II. Find $[11]^{-1}$ in $\mathbf{Z}_{16}$ using trial and error (for small numbers):
$\{(a, 16) = 1, a > 0\} = \{1, 3, 5, 7, 9, 11, 13, 15\}$.

Examples: Find the multiplicative inverse $[a]^{-1}$

I. Find $[11]^{-1}$ in $\mathbf{Z}_{16}$ using the matrix form of the Euclidean algorithm:

$$\begin{bmatrix} 1 & 0 & 16 \\ 0 & 1 & 11 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 5 \\ 0 & 1 & 11 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 5 \\ -2 & 3 & 1 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 11 & -16 & 0 \\ -2 & 3 & 1 \end{bmatrix}$$

Thus $(-2) \cdot 16 + 3 \cdot 11 = 1$, which shows that $[11]_{16}^{-1} = [3]_{16}$.

II. Find $[11]^{-1}$ in $\mathbf{Z}_{16}$ by taking successive powers of $[11]$:
List list the powers of $[11]$:
$[11]^2 = [-5]^2 = [25] = [9]$, $\quad [11]^3 = [11]^2[11] = [99] = [3]$, and
$[11]^4 = [11]^3[11] = [33] = [1]$. Thus again we see that $[11]_{16}^{-1} = [3]_{16}$.

II. Find $[11]^{-1}$ in $\mathbf{Z}_{16}$ using trial and error (for small numbers):
$\{(a, 16) = 1, a > 0\} = \{1, 3, 5, 7, 9, 11, 13, 15\}$.
It is easier to use the representatives $\pm 1, \pm 3, \pm 5, \pm 7$.

Examples: Find the multiplicative inverse $[a]^{-1}$

I. Find $[11]^{-1}$ in $\mathbf{Z}_{16}$ using the matrix form of the Euclidean algorithm:

$$\begin{bmatrix} 1 & 0 & 16 \\ 0 & 1 & 11 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 5 \\ 0 & 1 & 11 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 5 \\ -2 & 3 & 1 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 11 & -16 & 0 \\ -2 & 3 & 1 \end{bmatrix}$$

Thus $(-2) \cdot 16 + 3 \cdot 11 = 1$, which shows that $[11]_{16}^{-1} = [3]_{16}$.

II. Find $[11]^{-1}$ in $\mathbf{Z}_{16}$ by taking successive powers of $[11]$:
List list the powers of $[11]$:
$[11]^2 = [-5]^2 = [25] = [9]$, $\quad [11]^3 = [11]^2[11] = [99] = [3]$, and
$[11]^4 = [11]^3[11] = [33] = [1]$. Thus again we see that $[11]_{16}^{-1} = [3]_{16}$.

II. Find $[11]^{-1}$ in $\mathbf{Z}_{16}$ using trial and error (for small numbers):
$\{(a, 16) = 1, a > 0\} = \{1, 3, 5, 7, 9, 11, 13, 15\}$.
It is easier to use the representatives $\pm 1, \pm 3, \pm 5, \pm 7$.
$[3][5] = [15] = [-1] \Rightarrow [3][-5] = [3][11] = [1]$ since $[11] = [-5]$.
Thus again we obtain $[11]_{16}^{-1} = [3]_{16}$.

Euler's totient function

Definition 16

Let n be a positive integer. The number of positive integers less than or equal to n which are relatively prime to n will be denoted by $\varphi(n)$. This function is called **Euler's φ-function**, or the **totient function**.

Note that $\varphi(1) = 1$.

Euler's totient function

Definition 16

Let n be a positive integer. The number of positive integers less than or equal to n which are relatively prime to n will be denoted by $\varphi(n)$. This function is called **Euler's φ-function**, or the **totient function**.

Note that $\varphi(1) = 1$.

Proposition. 8

If the prime factorization of n is $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, where $\alpha_i > 0$ for $1 \le i \le k$, then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Euler's totient function

Definition 16

Let n be a positive integer. The number of positive integers less than or equal to n which are relatively prime to n will be denoted by $\varphi(n)$. This function is called **Euler's φ-function**, or the **totient function**.

Note that $\varphi(1) = 1$.

Proposition. 8

If the prime factorization of n is $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, where $\alpha_i > 0$ for $1 \leq i \leq k$, then

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Example. 7

$$\varphi(10) = 10 \left(\frac{1}{2}\right) \left(\frac{4}{5}\right) = 4 \qquad \text{and} \qquad \varphi(36) = 36 \left(\frac{1}{2}\right) \left(\frac{2}{3}\right) = 12.$$

The set of units: $\mathbf{Z}_n^\times$

Definition 17

The set of units of $\mathbf{Z}_n$, the congruence classes $[a]$ such that $(a, n) = 1$, will be denoted by $\mathbf{Z}_n^\times$.

The set of units: $\mathbf{Z}_n^\times$

Definition 17

The set of units of $\mathbf{Z}_n$, the congruence classes $[a]$ such that $(a, n) = 1$, will be denoted by $\mathbf{Z}_n^\times$.

Proposition. 9

The set $\mathbf{Z}_n^\times$ of units of $\mathbf{Z}_n$ is closed under multiplication.

The set of units: $\mathbf{Z}_n^\times$

Definition 17

The set of units of $\mathbf{Z}_n$, the congruence classes $[a]$ such that $(a, n) = 1$, will be denoted by $\mathbf{Z}_n^\times$.

Proposition. 9

The set $\mathbf{Z}_n^\times$ of units of $\mathbf{Z}_n$ is closed under multiplication.

Note that the number of elements of $\mathbf{Z}_n^\times$ is given by $\varphi(n)$.

The set of units: $\mathbf{Z}_n^\times$

Definition 17

The set of units of $\mathbf{Z}_n$, the congruence classes $[a]$ such that $(a, n) = 1$, will be denoted by $\mathbf{Z}_n^\times$.

Proposition. 9

The set $\mathbf{Z}_n^\times$ of units of $\mathbf{Z}_n$ is closed under multiplication.

Note that the number of elements of $\mathbf{Z}_n^\times$ is given by $\varphi(n)$.

Theorem 18 (Euler)

If $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

The set of units: $\mathbf{Z}_n^\times$

Definition 17

The set of units of $\mathbf{Z}_n$, the congruence classes $[a]$ such that $(a, n) = 1$, will be denoted by $\mathbf{Z}_n^\times$.

Proposition. 9

The set $\mathbf{Z}_n^\times$ of units of $\mathbf{Z}_n$ is closed under multiplication.

Note that the number of elements of $\mathbf{Z}_n^\times$ is given by $\varphi(n)$.

Theorem 18 (Euler)

If $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Note that if $(a, n) = 1$, then $[a]^{-1} = [a]^{\varphi(n)-1}$.

The set of units: $\mathbf{Z}_n^\times$

Definition 17

The set of units of $\mathbf{Z}_n$, the congruence classes $[a]$ such that $(a, n) = 1$, will be denoted by $\mathbf{Z}_n^\times$.

Proposition. 9

The set $\mathbf{Z}_n^\times$ of units of $\mathbf{Z}_n$ is closed under multiplication.

Note that the number of elements of $\mathbf{Z}_n^\times$ is given by $\varphi(n)$.

Theorem 18 (Euler)

If $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Note that if $(a, n) = 1$, then $[a]^{-1} = [a]^{\varphi(n)-1}$.

Corollary 19 (Fermat)

If p is a prime number, then for any integer a we have $a^p \equiv a \pmod{p}$.

The set of units: $\mathbf{Z}_n^\times$

Definition 17

The set of units of $\mathbf{Z}_n$, the congruence classes $[a]$ such that $(a, n) = 1$, will be denoted by $\mathbf{Z}_n^\times$.

Proposition. 9

The set $\mathbf{Z}_n^\times$ of units of $\mathbf{Z}_n$ is closed under multiplication.

Note that the number of elements of $\mathbf{Z}_n^\times$ is given by $\varphi(n)$.

Theorem 18 (Euler)

If $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Note that if $(a, n) = 1$, then $[a]^{-1} = [a]^{\varphi(n)-1}$.

Corollary 19 (Fermat)

If p is a prime number, then for any integer a we have $a^p \equiv a \pmod{p}$.

If $p|a$: trivial.

The set of units: $\mathbf{Z}_n^\times$

Definition 17

The set of units of $\mathbf{Z}_n$, the congruence classes $[a]$ such that $(a, n) = 1$, will be denoted by $\mathbf{Z}_n^\times$.

Proposition. 9

The set $\mathbf{Z}_n^\times$ of units of $\mathbf{Z}_n$ is closed under multiplication.

Note that the number of elements of $\mathbf{Z}_n^\times$ is given by $\varphi(n)$.

Theorem 18 (Euler)

If $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Note that if $(a, n) = 1$, then $[a]^{-1} = [a]^{\varphi(n)-1}$.

Corollary 19 (Fermat)

If p is a prime number, then for any integer a we have $a^p \equiv a \pmod{p}$.

If $p|a$: trivial. If $p \nmid a$, then $(a, p) = 1$. $\Rightarrow a^{\varphi(p)} \equiv a^{p-1} \equiv 1 \pmod{p}$. □