Solving Congruences

Rosen Section 4.4

Tom Michoel

MNF130V2020 – Week 9

Relative prime

Definition

Two integers m and n are **relatively prime** if they have *no* common positive divisor other than 1, that is, if $\gcd(m, n) = 1$.

Theorem

For m a positive integer and a, b, n integers, if $an \equiv bn \pmod{m}$ and $\gcd(m, n) = 1$, then $a \equiv b \pmod{m}$.

Lemma

If a, b, c are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Proof.

$\square$

Lemma

If a, b, c are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Proof.

- If $\gcd(a, b) = 1$ then there exist integers s, t such that

$$\begin{aligned} sa + tb &= 1 \\ sac + tbc &= c \end{aligned}$$

$\square$

Lemma

If a, b, c are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Proof.

- If $\gcd(a, b) = 1$ then there exist integers s, t such that

$$\begin{aligned} sa + tb &= 1 \\ sac + tbc &= c \end{aligned}$$

- We have $a \mid sac$, and by the assumption that $a \mid bc$ also $a \mid tbc$.

$\square$

Lemma

If a, b, c are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Proof.

- If $\gcd(a, b) = 1$ then there exist integers s, t such that

$$\begin{aligned} sa + tb &= 1 \\ sac + tbc &= c \end{aligned}$$

- We have $a \mid sac$, and by the assumption that $a \mid bc$ also $a \mid tbc$.
- Hence $a \mid (sac + tbc) = c$.

$\square$

Theorem

For m a positive integer and a, b, n integers, if $an \equiv bn \pmod{m}$ and $\gcd(m, n) = 1$, then $a \equiv b \pmod{m}$.

Proof.

$\square$

Theorem

For m a positive integer and a, b, n integers, if $an \equiv bn \pmod{m}$ and $\gcd(m, n) = 1$, then $a \equiv b \pmod{m}$.

Proof.

- If $an \equiv bn \pmod{m}$, then by definition $m \mid (an - bn) = (a - b)n$.

$\square$

Theorem

For m a positive integer and a, b, n integers, if $an \equiv bn \pmod{m}$ and $\gcd(m, n) = 1$, then $a \equiv b \pmod{m}$.

Proof.

- If $an \equiv bn \pmod{m}$, then by definition $m \mid (an - bn) = (a - b)n$.
- By the previous lemma, $\gcd(m, n) = 1$ and $m \mid (a - b)n$ implies that $m \mid (a - b)$, and hence $a \equiv b \pmod{m}$.

$\square$

Linear congruences

A **linear conruence** is an equation

$$ax \equiv b \pmod{m} \tag{1}$$

in an integer variable x, with m a positive integer and a, b integers.

Linear congruences

A **linear conruence** is an equation

$$ax \equiv b \pmod{m} \tag{1}$$

in an integer variable x, with m a positive integer and a, b integers.

Example

The linear congruence with $2x \equiv 1 \pmod{3}$ has the solution $x \equiv 2 \pmod{3}$.

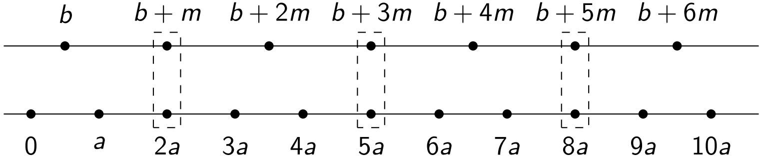

Figure 1: Linear congruence with $a = 2$, $b = 1$ and $m = 3$.

Inverse modulo m

Definition

An **inverse of an integer a modulo m** is an integer $\bar{a}$ such that $a\bar{a} \equiv 1 \pmod{m}$.

Theorem

If integers a, m are relatively prime, $\gcd(a, m) = 1$, then there exists a unique inverse of a modulo m.

Proof.

$\square$

Inverse modulo m

Definition

An **inverse of an integer a modulo m** is an integer $\bar{a}$ such that $a\bar{a} \equiv 1 \pmod{m}$.

Theorem

If integers a, m *are relatively prime,* $\gcd(a, m) = 1$*, then there exists a unique inverse of a modulo m.*

Proof.

- If $\gcd(a, m) = 1$, then there exist integers s, t such that $sa + tm = 1$, and hence $sa + tm \equiv 1 \pmod{m}$.

□

Inverse modulo m

Definition

An **inverse of an integer a modulo m** is an integer $\bar{a}$ such that $a\bar{a} \equiv 1 \pmod{m}$.

Theorem

If integers a, m are relatively prime, $\gcd(a, m) = 1$, then there exists a unique inverse of a modulo m.

Proof.

- If $\gcd(a, m) = 1$, then there exist integers s, t such that $sa + tm = 1$, and hence $sa + tm \equiv 1 \pmod{m}$.
- Because $tm \equiv 0 \pmod{m}$, it follows that $sa \equiv 1 \pmod{m}$, and s is an inverse of a modulo m.

□

Inverse modulo m

Definition

An **inverse of an integer a modulo m** is an integer $\bar{a}$ such that $a\bar{a} \equiv 1 \pmod{m}$.

Theorem

If integers a, m are relatively prime, $\gcd(a, m) = 1$, then there exists a unique inverse of a modulo m.

Proof.

- If $\gcd(a, m) = 1$, then there exist integers s, t such that $sa + tm = 1$, and hence $sa + tm \equiv 1 \pmod{m}$.
- Because $tm \equiv 0 \pmod{m}$, it follows that $sa \equiv 1 \pmod{m}$, and s is an inverse of a modulo m.
- Assume there exists another inverse r of a modulo m. Because $sa \equiv 1 \pmod{m}$, there exists q such that $sa = qm + 1$. Likewise there exists p such that $ra = pm + 1$.

□

Inverse modulo m

Definition

An **inverse of an integer a modulo m** is an integer $\bar{a}$ such that $a\bar{a} \equiv 1 \pmod{m}$.

Theorem

If integers a, m *are relatively prime,* $\gcd(a, m) = 1$*, then there exists a unique inverse of* a *modulo* m*.*

Proof.

- If $\gcd(a, m) = 1$, then there exist integers s, t such that $sa + tm = 1$, and hence $sa + tm \equiv 1 \pmod{m}$.
- Because $tm \equiv 0 \pmod{m}$, it follows that $sa \equiv 1 \pmod{m}$, and s is an inverse of a modulo m.
- Assume there exists another inverse r of a modulo m. Because $sa \equiv 1 \pmod{m}$, there exists q such that $sa = qm + 1$. Likewise there exists p such that $ra = pm + 1$.
- Hence $(s - r)a = (q - p)m$ and $m \mid (s - r)a$.

□

Inverse modulo m

Definition

An **inverse of an integer a modulo m** is an integer $\bar{a}$ such that $a\bar{a} \equiv 1 \pmod{m}$.

Theorem

If integers a, m are relatively prime, $\gcd(a, m) = 1$, then there exists a unique inverse of a modulo m.

Proof.

- If $\gcd(a, m) = 1$, then there exist integers s, t such that $sa + tm = 1$, and hence $sa + tm \equiv 1 \pmod{m}$.
- Because $tm \equiv 0 \pmod{m}$, it follows that $sa \equiv 1 \pmod{m}$, and s is an inverse of a modulo m.
- Assume there exists another inverse r of a modulo m. Because $sa \equiv 1 \pmod{m}$, there exists q such that $sa = qm + 1$. Likewise there exists p such that $ra = pm + 1$.
- Hence $(s - r)a = (q - p)m$ and $m \mid (s - r)a$.
- Because $\gcd(a, m) = 1$ it follows that $m \mid (s - r)$, or $s \equiv r \pmod{m}$. That is, s is unique modulo m.

□

Example

Do 7 and 6 have inverses modulo 8?

Example

Do 7 and 6 have inverses modulo 8?

- Test all possible values for an inverse:

$$\begin{aligned} 7 \bmod 8 &= 7 \\ 2 \cdot 7 \bmod 8 &= 6 \\ 3 \cdot 7 \bmod 8 &= 5 \\ 4 \cdot 7 \bmod 8 &= 4 \\ 5 \cdot 7 \bmod 8 &= 3 \\ 6 \cdot 7 \bmod 8 &= 2 \\ {\color{red}7} \cdot 7 \bmod 8 &= 1 \\ 8 \cdot 7 \bmod 8 &= 0 \end{aligned}$$

$$\begin{aligned} 6 \bmod 8 &= 7 \\ 2 \cdot 6 \bmod 8 &= 4 \\ 3 \cdot 6 \bmod 8 &= 2 \\ 4 \cdot 6 \bmod 8 &= 0 \end{aligned}$$

Example

Do 7 and 6 have inverses modulo 8?

- Test all possible values for an inverse:

$$\begin{aligned} 7 \bmod 8 &= 7 \\ 2 \cdot 7 \bmod 8 &= 6 \\ 3 \cdot 7 \bmod 8 &= 5 \\ 4 \cdot 7 \bmod 8 &= 4 \\ 5 \cdot 7 \bmod 8 &= 3 \\ 6 \cdot 7 \bmod 8 &= 2 \\ {\color{red}7} \cdot 7 \bmod 8 &= 1 \\ 8 \cdot 7 \bmod 8 &= 0 \end{aligned}$$

$$\begin{aligned} 6 \bmod 8 &= 7 \\ 2 \cdot 6 \bmod 8 &= 4 \\ 3 \cdot 6 \bmod 8 &= 2 \\ 4 \cdot 6 \bmod 8 &= 0 \end{aligned}$$

- Once we reach 0, the numbers repeat.

Example

Do 7 and 6 have inverses modulo 8?

- Test all possible values for an inverse:

$$\begin{aligned} 7 \bmod 8 &= 7 \\ 2 \cdot 7 \bmod 8 &= 6 \\ 3 \cdot 7 \bmod 8 &= 5 \\ 4 \cdot 7 \bmod 8 &= 4 \\ 5 \cdot 7 \bmod 8 &= 3 \\ 6 \cdot 7 \bmod 8 &= 2 \\ 7 \cdot 7 \bmod 8 &= 1 \\ 8 \cdot 7 \bmod 8 &= 0 \end{aligned} \qquad \begin{aligned} 6 \bmod 8 &= 7 \\ 2 \cdot 6 \bmod 8 &= 4 \\ 3 \cdot 6 \bmod 8 &= 2 \\ 4 \cdot 6 \bmod 8 &= 0 \end{aligned}$$

- Once we reach 0, the numbers repeat.

Intuition

If $\gcd(a, m) = 1$, all values $0 \leq r < m$, including $r = 1$, are encountered in this process, but if $\gcd(a, m) > 1$ the process terminates early and $r = 1$ is not encountered.

We can make this argument more precise:

Let a and m be arbitrary positive integers.

We can make this argument more precise:

Let a and m be arbitrary positive integers.

- Because $(x+m)a \equiv xa \pmod{m}$, an inverse $\bar{a}$ of a modulo m must satisfy $\bar{a} \in \{1, \ldots, m-1\}$.

We can make this argument more precise:

Let a and m be arbitrary positive integers.

- Because $(x + m)a \equiv xa \pmod{m}$, an inverse $\bar{a}$ of a modulo m must satisfy $\bar{a} \in \{1, \ldots, m - 1\}$.
- If $\gcd(a, m) = 1$, then none of xa for $x \in \{1, \ldots, m - 1\}$ are a multiple of m, and all values of $xa \bmod m$ are different.

We can make this argument more precise:

Let a and m be arbitrary positive integers.

- Because $(x + m)a \equiv xa \pmod{m}$, an inverse $\bar{a}$ of a modulo m must satisfy $\bar{a} \in \{1, \ldots, m - 1\}$.
- If $\gcd(a, m) = 1$, then none of xa for $x \in \{1, \ldots, m - 1\}$ are a multiple of m, and all values of $xa \bmod m$ are different.
- Because the only values in $\mathbb{Z}_m$ are $\{0, \ldots, m - 1\}$, $xa \bmod m$ for $x \in \{1, \ldots, m - 1\}$ must take all non-zero values in $\mathbb{Z}_m$, including 1, and an inverse of a modulo m exists.

We can make this argument more precise:

Let a and m be arbitrary positive integers.

- Because $(x + m)a \equiv xa \pmod{m}$, an inverse $\bar{a}$ of a modulo m must satisfy $\bar{a} \in \{1, \ldots, m - 1\}$.
- If $\gcd(a, m) = 1$, then none of xa for $x \in \{1, \ldots, m - 1\}$ are a multiple of m, and all values of $xa \bmod m$ are different.
- Because the only values in $\mathbb{Z}_m$ are $\{0, \ldots, m - 1\}$, $xa \bmod m$ for $x \in \{1, \ldots, m - 1\}$ must take all non-zero values in $\mathbb{Z}_m$, including 1, and an inverse of a modulo m exists.
- If $\gcd(a, m) = c > 1$, there exist integers k and l such that $a = kc$ and $m = lc$, with k and l in $\{2, \ldots, \lfloor m/2 \rfloor\}$.

We can make this argument more precise:

Let a and m be arbitrary positive integers.

- Because $(x+m)a \equiv xa \pmod{m}$, an inverse $\bar{a}$ of a modulo m must satisfy $\bar{a} \in \{1, \ldots, m-1\}$.
- If $\gcd(a, m) = 1$, then none of xa for $x \in \{1, \ldots, m-1\}$ are a multiple of m, and all values of $xa \bmod m$ are different.
- Because the only values in $\mathbb{Z}_m$ are $\{0, \ldots, m-1\}$, $xa \bmod m$ for $x \in \{1, \ldots, m-1\}$ must take all non-zero values in $\mathbb{Z}_m$, including 1, and an inverse of a modulo m exists.
- If $\gcd(a, m) = c > 1$, there exist integers k and l such that $a = kc$ and $m = lc$, with k and l in $\{2, \ldots, \lfloor m/2 \rfloor\}$.
- This means that $la = klc = km$ is a multiple of m, or $la \equiv 0 \pmod{m}$.

We can make this argument more precise:

Let a and m be arbitrary positive integers.

- Because $(x+m)a \equiv xa \pmod{m}$, an inverse $\bar{a}$ of a modulo m must satisfy $\bar{a} \in \{1, \ldots, m-1\}$.
- If $\gcd(a, m) = 1$, then none of xa for $x \in \{1, \ldots, m-1\}$ are a multiple of m, and all values of $xa \bmod m$ are different.
- Because the only values in $\mathbb{Z}_m$ are $\{0, \ldots, m-1\}$, $xa \bmod m$ for $x \in \{1, \ldots, m-1\}$ must take all non-zero values in $\mathbb{Z}_m$, including 1, and an inverse of a modulo m exists.
- If $\gcd(a, m) = c > 1$, there exist integers k and l such that $a = kc$ and $m = lc$, with k and l in $\{2, \ldots, \lfloor m/2 \rfloor\}$.
- This means that $la = klc = km$ is a multiple of m, or $la \equiv 0 \pmod{m}$.
- Hence $xa \bmod m$ for $x \in \{1, \ldots, m-1\}$ does **not** take all values in $\{1, \ldots, m-1\}$.

We can make this argument more precise:

Let a and m be arbitrary positive integers.

- Because $(x+m)a \equiv xa \pmod{m}$, an inverse $\bar{a}$ of a modulo m must satisfy $\bar{a} \in \{1, \ldots, m-1\}$.
- If $\gcd(a, m) = 1$, then none of xa for $x \in \{1, \ldots, m-1\}$ are a multiple of m, and all values of $xa \bmod m$ are different.
- Because the only values in $\mathbb{Z}_m$ are $\{0, \ldots, m-1\}$, $xa \bmod m$ for $x \in \{1, \ldots, m-1\}$ must take all non-zero values in $\mathbb{Z}_m$, including 1, and an inverse of a modulo m exists.
- If $\gcd(a, m) = c > 1$, there exist integers k and l such that $a = kc$ and $m = lc$, with k and l in $\{2, \ldots, \lfloor m/2 \rfloor\}$.
- This means that $la = klc = km$ is a multiple of m, or $la \equiv 0 \pmod{m}$.
- Hence $xa \bmod m$ for $x \in \{1, \ldots, m-1\}$ does **not** take all values in $\{1, \ldots, m-1\}$.
- In particular, $xa \bmod m$ will never be equal to 1, because $xa \bmod m = 1$ implies that there exists an integer q such that $xa = qm + 1$, or $(xk - ql)c = 1$, or $c \mid 1$, which is a contradiction.

Theorem

If a has an inverse $\bar{a}$ modulo m, then the solutions to the linear congruence $ax \equiv b \pmod{m}$ are all integers x such that $x \equiv \bar{a}b \pmod{m}$.

Proof.

$\square$

Theorem

If a has an inverse $\bar{a}$ modulo m, then the solutions to the linear congruence $ax \equiv b \pmod{m}$ are all integers x such that $x \equiv \bar{a}b \pmod{m}$.

Proof.

- Let x be a solution to $ax \equiv b \pmod{m}$. Then

$$\begin{aligned} \bar{a}b \bmod m &= (\bar{a} \bmod m)(b \bmod m) \bmod m \\ &= (\bar{a} \bmod m)(ax \bmod m) \bmod m \\ &= \bar{a}ax \bmod m \\ &= (\bar{a}a \bmod m)(x \bmod m) \bmod m \\ &= (x \bmod m) \bmod m \\ &= x \bmod m \end{aligned}$$

or $x \equiv \bar{a}b \pmod{m}$

$\square$

The Chinese remainder theorem

The **Chinese remainder theorem** states that when the moduli of a system of linear congruences are pairwise relatively prime, then there is a unique solution of the system modulo the product of the moduli.

It is named after the Chinese heritage of problems involving systems of linear congruences.

Example (Sun-Tsu, 1st century)

There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; and when divided by 7, the remainder is 2. What will be the number of things?

The Chinese remainder theorem

The **Chinese remainder theorem** states that when the moduli of a system of linear congruences are pairwise relatively prime, then there is a unique solution of the system modulo the product of the moduli.

It is named after the Chinese heritage of problems involving systems of linear congruences.

Example (Sun-Tsu, 1st century)

There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; and when divided by 7, the remainder is 2. What will be the number of things?

Answer: 23

The Chinese remainder theorem

THE CHINESE REMAINDER THEOREM Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\ \ \vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$. (That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

The Chinese remainder theorem (special case)

Theorem

Let a, m_1, m_2 *be integers and* $\gcd(m_1, m_2) = 1$*. Then*

$$x \equiv a \pmod{m_1 m_2}$$

is a solution to the system of linear congruences

$$\begin{aligned} x &\equiv a \pmod{m_1} \\ x &\equiv a \pmod{m_2} \end{aligned}$$

The Chinese remainder theorem (special case)

Theorem

Let a, m_1, m_2 *be integers and* $\gcd(m_1, m_2) = 1$*. Then*

$$x \equiv a \pmod{m_1 m_2}$$

is a solution to the system of linear congruences

$$\begin{aligned} x &\equiv a \pmod{m_1} \\ x &\equiv a \pmod{m_2} \end{aligned}$$

Remark

$x \equiv a \pmod{m_1 m_2}$ is in fact the **unique** solution to this system of linear congruences, but we will not prove this fact.

Proof.

$\square$

Proof.

- Because $\gcd(m_1, m_2) = 1$, there exist integers s and t such that $sm_1 + tm_2 = 1$.

$\square$

Proof.

- Because $\gcd(m_1, m_2) = 1$, there exist integers s and t such that $sm_1 + tm_2 = 1$.
- Hence $sm_1 \equiv 1 \pmod{m_2}$ and $tm_2 \equiv 1 \pmod{m_1}$.

$\square$

Proof.

- Because $\gcd(m_1, m_2) = 1$, there exist integers s and t such that $sm_1 + tm_2 = 1$.
- Hence $sm_1 \equiv 1 \pmod{m_2}$ and $tm_2 \equiv 1 \pmod{m_1}$.
- Let $x \equiv a \pmod{m_1 m_2}$.

$\square$

Proof.

- Because $\gcd(m_1, m_2) = 1$, there exist integers s and t such that $sm_1 + tm_2 = 1$.
- Hence $sm_1 \equiv 1 \pmod{m_2}$ and $tm_2 \equiv 1 \pmod{m_1}$.
- Let $x \equiv a \pmod{m_1 m_2}$.
- Then $x = a + km_1 m_2$ for some integer k.

$\square$

Proof.

- Because $\gcd(m_1, m_2) = 1$, there exist integers s and t such that $sm_1 + tm_2 = 1$.
- Hence $sm_1 \equiv 1 \pmod{m_2}$ and $tm_2 \equiv 1 \pmod{m_1}$.
- Let $x \equiv a \pmod{m_1 m_2}$.
- Then $x = a + km_1 m_2$ for some integer k.
- Hence $x = a(sm_1 + tm_2) + km_1 m_2$, and

$$\begin{aligned} x \bmod m_1 &= (atm_2) \bmod m_1 = \big[(a \bmod m_1)((tm_2) \bmod m_1)\big] \bmod m_1 \\ &= a \bmod m_1 \end{aligned}$$

$\square$

Proof.

- Because $\gcd(m_1, m_2) = 1$, there exist integers s and t such that $sm_1 + tm_2 = 1$.
- Hence $sm_1 \equiv 1 \pmod{m_2}$ and $tm_2 \equiv 1 \pmod{m_1}$.
- Let $x \equiv a \pmod{m_1 m_2}$.
- Then $x = a + km_1 m_2$ for some integer k.
- Hence $x = a(sm_1 + tm_2) + km_1 m_2$, and

$$\begin{aligned} x \bmod m_1 &= (atm_2) \bmod m_1 = \big[(a \bmod m_1)((tm_2) \bmod m_1)\big] \bmod m_1 \\ &= a \bmod m_1 \end{aligned}$$

- Likewise

$$\begin{aligned} x \bmod m_2 &= (asm_1) \bmod m_2 = \big[(a \bmod m_2)((sm_1) \bmod m_2)\big] \bmod m_2 \\ &= a \bmod m_2 \end{aligned}$$

□

Proof.

- Because $\gcd(m_1, m_2) = 1$, there exist integers s and t such that $sm_1 + tm_2 = 1$.
- Hence $sm_1 \equiv 1 \pmod{m_2}$ and $tm_2 \equiv 1 \pmod{m_1}$.
- Let $x \equiv a \pmod{m_1 m_2}$.
- Then $x = a + km_1 m_2$ for some integer k.
- Hence $x = a(sm_1 + tm_2) + km_1 m_2$, and

$$\begin{aligned} x \bmod m_1 &= (atm_2) \bmod m_1 = \left[(a \bmod m_1)((tm_2) \bmod m_1)\right] \bmod m_1 \\ &= a \bmod m_1 \end{aligned}$$

- Likewise

$$\begin{aligned} x \bmod m_2 &= (asm_1) \bmod m_2 = \left[(a \bmod m_2)((sm_1) \bmod m_2)\right] \bmod m_2 \\ &= a \bmod m_2 \end{aligned}$$

- Hence $x \equiv a \pmod{m_1 m_2}$ is a solution to the system of congruences.

$\square$

Practice makes perfect

Solve Practice Quiz "Ch 04 – Modular inverses and linear congruences":

`https://mitt.uib.no/courses/21678/quizzes/10439`