Lecture 8: Euclidean algorithms and Linear Congruences

Table of contents

Prime factorization and great common divisors

- Any integer $n \geq 2$ can be expressed uniquely as

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where $e_1, \ldots, e_k \in \mathbb{Z}^+$ and $p_1 < p_2 < \cdots < p_k$ are primes.

Prime factorization and great common divisors

- Find $\gcd(a, b)$ in 3 steps
  1. Factorize a and b.
  2. Find *common prime factors* of a and b, say $p_1, \ldots, p_k$
     - Assume $p_1^{a_1} \cdots p_k^{a_k}$ is the part of a containing $p_1, \ldots, p_k$
     - Assume $p_1^{b_1} \ldots p_k^{b_k}$ is the part of b containing $p_1, \ldots, p_k$.
  3. Put $c_i = \min\{a_i, b_i\}$ for $i = 1, \ldots, k$. Then

$$\gcd(a, b) = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}.$$

Why need an algorithm for gcd(a,b)?

- Computing the greatest common divisor of two integers directly from their prime factorizations is inefficient.
  To factorize a number, we need to do brute force.
- If integers have large prime factors (say 20-digits primes), it is time-consuming to find such a factor.

Principle of Euclidean algorithm

Let a, b be integers with $b > 0$. Then

- There are *unique integers* q and r such that

$$a = bq + r \text{ with } r \in \{0, \ldots, b-1\}.$$

  b and r are called **quotient** and **remainder** in the division of a by b.

- Further

$$\gcd(a, b) = \gcd(b, r).$$

  We will look at a few examples of this equation.

Examples

$$a = bq + r \Rightarrow \gcd(a, b) = \gcd(b, r)$$

Examples

$$a = bq + r \Rightarrow \gcd(a, b) = \gcd(b, r)$$

- Consider $a = 25$ and $b = 10$

$$25 = 10 \cdot 2 + 5 \text{ and } \gcd(25, 10) = \gcd(10, 5)$$

Examples

$$a = bq + r \Rightarrow \gcd(a, b) = \gcd(b, r)$$

- Consider $a = 25$ and $b = 10$

$$25 = 10 \cdot 2 + 5 \text{ and } \gcd(25, 10) = \gcd(10, 5)$$

- Consider $a = 100$ and $b = 15$

$$100 = 15 \cdot 6 + 10 \text{ and } \gcd(100, 15) = \gcd(15, 10)$$

Assume we don't know anything about prime factorization.

We still can find $\gcd(100, 15)$.

Assume we don't know anything about prime factorization.

We still can find $\gcd(100, 15)$.

- $100 = 15 \cdot 6 + 10 \Rightarrow \gcd(100, 15) = \gcd(15, 10)$
- $15 = 10 \cdot 1 + 5 \Rightarrow \gcd(15, 10) = \gcd(10, 5)$
- $10 = 5 \cdot 2 + 0 \Rightarrow \gcd(10, 5) = \gcd(5, 0) = 5$

  Conclusion

$$\gcd(100, 15) = 5$$

Algorithm for finding $\gcd(\mathbf{a}, \mathbf{b})$

Put $r_0 = a, r_1 = b$. Assume $r_0 > r_1$.

- $r_0 = r_1 q_1 + r_2,\ 0 \leq r_2 \leq r_1 - 1$ (note $\gcd(r_0, r_1) = \gcd(r_1, r_2)$)

Algorithm for finding $\gcd(\mathbf{a}, \mathbf{b})$

Put $r_0 = a, r_1 = b$. Assume $r_0 > r_1$.

- $r_0 = r_1 q_1 + r_2,\ 0 \leq r_2 \leq r_1 - 1$ (note $\gcd(r_0, r_1) = \gcd(r_1, r_2)$)
- $r_1 = r_2 q_2 + r_3,\ 0 \leq r_3 \leq r_2 - 1$ (note $\gcd(r_1, r_2) = \gcd(r_2, r_3)$)

  $\vdots$

Algorithm for finding $\gcd(\mathbf{a}, \mathbf{b})$

Put $r_0 = a, r_1 = b$. Assume $r_0 > r_1$.

- $r_0 = r_1 q_1 + r_2,\ 0 \le r_2 \le r_1 - 1$ (note $\gcd(r_0, r_1) = \gcd(r_1, r_2)$)
- $r_1 = r_2 q_2 + r_3,\ 0 \le r_3 \le r_2 - 1$ (note $\gcd(r_1, r_2) = \gcd(r_2, r_3)$)

  $\vdots$
- $r_{n-2} = r_{n-1} q_{n-1} + r_n,\ 0 \le r_n \le r_{n-1} - 1$ (note $\gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n)$)

Algorithm for finding $\gcd(\mathbf{a}, \mathbf{b})$

Put $r_0 = a, r_1 = b$. Assume $r_0 > r_1$.

- $r_0 = r_1 q_1 + r_2,\ 0 \le r_2 \le r_1 - 1$ (note $\gcd(r_0, r_1) = \gcd(r_1, r_2)$)
- $r_1 = r_2 q_2 + r_3,\ 0 \le r_3 \le r_2 - 1$ (note $\gcd(r_1, r_2) = \gcd(r_2, r_3)$)

  $\vdots$

- $r_{n-2} = r_{n-1} q_{n-1} + r_n,\ 0 \le r_n \le r_{n-1} - 1$ (note $\gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n)$)
- $r_{n-1} = r_n q_n + 0$ (note $\gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$)

Conclusion

$$\gcd(a, b) = r_n.$$

Why the algorithm works?

- We assumed that the algorithm stops after a finite number of steps (n steps).

$$\gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n.$$

- $\gcd(\mathbf{a}, \mathbf{b}) =$ **the last nonzero remainder $\mathbf{r_n}$** in the algorithm.

Why the algorithm works?

- We assumed that the algorithm stops after a finite number of steps (n steps).

$$\gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n.$$

- $\gcd(\mathbf{a}, \mathbf{b})$ = **the last nonzero remainder $\mathbf{r_n}$** in the algorithm.
- Question: Why does the algorithm actually stop after finite steps?

Why the algorithm stops after finite steps?

- The remainders r_i's have the property

$$r_0 > r_1 > \cdots > r_k > \cdots \geq 0$$

- We will get to the point where some remainder is 0.
  The algorithm stops here.

Example 1

Find $\gcd(414, 662)$ and $\gcd(1235, 915)$.

Solution. $\gcd(414, 662)$

Example 1

Find $\gcd(414, 662)$ and $\gcd(1235, 915)$.

Solution. $\gcd(414, 662)$

$$662 = 414 \times 1 + 248$$

Example 1

Find $\gcd(414, 662)$ and $\gcd(1235, 915)$.

Solution. $\gcd(414, 662)$

$$662 = 414 \times 1 + 248$$

$$414 = 248 \times 1 + 166$$

Example 1

Find $\gcd(414, 662)$ and $\gcd(1235, 915)$.

Solution. $\gcd(414, 662)$

$$662 = 414 \times 1 + 248$$

$$414 = 248 \times 1 + 166$$

$$248 = 166 \times 1 + 82$$

$$166 = 82 \times 2 + 2$$

$$82 = 2 \times 41 + 0$$

$\gcd(915, 1235)$

Summary on finding $\gcd(a, b)$

Put $r_0 = \max(a, b)$ and $r_1 = \min(a, b)$.

We iteratively divide r_i by r_{i+1} until we get remainder 0.

$$\begin{array}{lcl}
r_0 & = & r_1 q_1 + r_2 \\
\vdots & \vdots & \vdots \\
r_i & = & r_{i+1} q_{i+1} + r_{i+2} \\
\vdots & \vdots & \vdots \\
r_{n-2} & = & r_{n-1} q_{n-1} + \mathbf{r_n} \\
r_{n-1} & = & r_n q_n + 0
\end{array}$$

Conclusion

$$\gcd(a, b) = \text{last nonzero remainder} = r_n$$

Bezout's identity and Bezout coefficients

Theorem 1

Let a and b be positive integers. Then there exist integers s and t such that

$$as + bt = \gcd(a, b)$$

Bezout's identity and Bezout coefficients

Theorem 1

Let a and b be positive integers. Then there exist integers s and t such that

$$as + bt = \gcd(a, b)$$

- The equation

  $$as + bt = \gcd(a, b)$$

  is called **Bezout's identity** of a and b.
- s are t are called **Bezout coefficients** of a and b.
- Remark: s, t are integers, not necessarily positive integers.

Examples

- $\gcd(4,3) = 1$ and $4 \cdot 1 + 3 \cdot (-1) = 1$.
  The Bezout coefficients of 4 and 3 are 1 and -1.
- $\gcd(9,15) = 3$ and $9 \cdot 2 + 15 \cdot (-1) = 3$.
  The Bezout coefficients of 9 and 15 are 2 and -1.

Example 2

Find Bezout coefficients of 662 and 414, that is, find s and t such that

$$662s + 414t = \gcd(662, 414)$$

Solution. $\gcd(414, 662) = 2$ by Euclidean algorithm.

$$662 = 414 \times 1 + 248$$

$$414 = 248 \times 1 + 166$$

$$248 = 166 \times 1 + 82$$

$$166 = 82 \times 2 + 2$$

$$82 = 2 \times 41 + 0$$

Example 2

- From the second last equation, we work backwards

$$
\begin{aligned}
2 &= 166 + 82 \times (-2) \\
&= 166 + (248 - 166 \times 1) \times (-2) = 248 \times (-2) + 166 \times 3 \\
&= 248 \times (-2) + (414 - 248 \times 1) \times 3 = 414 \times 3 + 248 \times (-5) \\
&= 414 \times 3 + (662 - 414 \times 1) \times (-5) = 662 \times (-5) + 414 \times 8
\end{aligned}
$$

Example 2

- From the second last equation, we work backwards

$$
\begin{aligned}
2 &= 166 + 82 \times (-2) \\
&= 166 + (248 - 166 \times 1) \times (-2) = 248 \times (-2) + 166 \times 3 \\
&= 248 \times (-2) + (414 - 248 \times 1) \times 3 = 414 \times 3 + 248 \times (-5) \\
&= 414 \times 3 + (662 - 414 \times 1) \times (-5) = 662 \times (-5) + 414 \times 8
\end{aligned}
$$

- The Bezout coefficients of 662 and 414 are $s = -5$ and $t = 8$:

$$662 \times (-5) + 414 \times 8 = 2 = \gcd(662, 414)$$

Euclidean algorithm revisited

Put $r_0 = \max(a, b)$ and $r_1 = \min(a, b)$.

Iteratively divide r_i by r_{i+1} until we get remainder 0.

$$\begin{array}{lcl} r_0 & = & r_1 q_1 + r_2 \\ \vdots & \vdots & \vdots \\ r_i & = & r_{i+1} q_{i+1} + r_{i+2} \\ \vdots & \vdots & \vdots \\ r_{n-2} & = & r_{n-1} q_{n-1} + \mathbf{r_n} \\ r_{n-1} & = & r_n q_n + 0 \end{array}$$

Conclusion

$$\gcd(a, b) = \text{last nonzero remainder} = r_n$$

Extended Euclidean algorithm

To find Bezout coefficients s and t of a and b

1. Implement Euclidean algorithm to find $\gcd(a, b)$.

Extended Euclidean algorithm

To find Bezout coefficients s and t of a and b

1. Implement Euclidean algorithm to find $\gcd(a, b)$.
2. From the 2nd last equation, write
$$\gcd(a, b) = r_{n-2} + r_{n-1}(-q_{n-1}). \quad (1)$$
3. Replace r_{n-1} from the 3rd last equation into (1)
$$\begin{aligned} \gcd(a, b) &= r_{n-2} + (r_{n-3} - r_{n-2}q_{n-2})(-q_{n-1}) \\ &= r_{n-3}(-q_{n-1}) + r_{n-2}(1 + q_{n-1}q_{n-2}). \end{aligned}$$

Extended Euclidean algorithm

To find Bezout coefficients s and t of a and b

1. Implement Euclidean algorithm to find $\gcd(a, b)$.
2. From the 2nd last equation, write
$$\gcd(a, b) = r_{n-2} + r_{n-1}(-q_{n-1}). \tag{1}$$
3. Replace r_{n-1} from the 3rd last equation into (1)
$$\begin{aligned}\gcd(a, b) &= r_{n-2} + (r_{n-3} - r_{n-2}q_{n-2})(-q_{n-1}) \\ &= r_{n-3}(-q_{n-1}) + r_{n-2}(1 + q_{n-1}q_{n-2}).\end{aligned}$$
4. Successively carry on the last step (replacing the remainders from the equations) until we go up to the first equation.
$$\gcd(a, b) = r_0 s + r_1 t$$

Example 4

Find Bezout coefficients of 252 and 198, that is, find s and t such that

$$252s + 198t = \gcd(252, 198)$$

Congruence

- **a is congruent to b modulo m** if

$$a - b \text{ is divisible by } m$$

- Write $a \equiv b \pmod{m}$ if a is congruent to b modulo m.
  Write $a \not\equiv b \pmod{m}$ otherwise.

Congruence

- a **is congruent to** b **modulo** m if

$$a - b \text{ is divisible by } m$$

- Write $a \equiv b \pmod{m}$ if a is congruent to b modulo m.
  Write $a \not\equiv b \pmod{m}$ otherwise.
- Examples

$$\begin{aligned} 12 &\equiv 2 \pmod{5} \\ 13 &\equiv 1 \pmod{4} \\ 13 &\not\equiv 2 \pmod{4} \end{aligned}$$

Properties of modular addition and multiplication

Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.

(a) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$\begin{aligned} a - c &\equiv b - d \pmod{m}, \\ a + c &\equiv b + d \pmod{m}, \\ ac &\equiv bd \pmod{m} \end{aligned}$$

(b) If $a \equiv b \pmod{m}$, then

$$a^k \equiv b^k \pmod{m} \text{ for any } k \in \mathbb{Z}^+$$

Modular division does not always work

- The following is not always true.

$$ac \equiv bc \pmod{m} \not\Rightarrow a \equiv b \pmod{m}.$$

Modular division does not always work

- The following is not always true.

$$ac \equiv bc \pmod{m} \not\Rightarrow a \equiv b \pmod{m}.$$

- Here is an example:

$$8 \equiv 2 \pmod{6}, \text{ but } 4 \not\equiv 1 \pmod{6}.$$

- Question: When could we do modular division?

Linear congruence

- A **linear congruence** is a congruence equation of the form

$$ax \equiv b \pmod{m} \tag{2}$$

Linear congruence

- A **linear congruence** is a congruence equation of the form

$$ax \equiv b \pmod{m} \tag{2}$$

- The solution to (2) is given in the form

$$x \equiv c \pmod{n} \text{ for some } c, n \in \mathbb{Z}$$

This means any $x \in \mathbb{Z}$ satisfying (2) must have the form

$$x = c + kn \text{ for some } k \in \mathbb{Z}.$$

Modular inverses

- Integers a, m.
- The **inverse** of a modulo m, denoted by $\mathbf{a^{-1}}$ **mod** $\mathbf{m}$, is the **positive integer b** such that

$$ab \equiv 1 \pmod{m}.$$

Modular inverses

- Integers a, m.
- The **inverse** of a modulo m, denoted by $\mathbf{a^{-1} \bmod m}$, is the **positive integer b** such that

$$ab \equiv 1 \pmod{m}.$$

- **Remark**: $a^{-1} \mod m$ and $\frac{1}{a}$ are different things!

Examples

- $2 \cdot 2 \equiv 1 \pmod 3 \Rightarrow 2^{-1} \mod 3 = 2$
- $3 \times 4 \equiv 1 \pmod{11} \Rightarrow 3^{-1} \mod 11 = 4$

Examples

- $2 \cdot 2 \equiv 1 \pmod 3 \Rightarrow 2^{-1} \mod 3 = 2$
- $3 \times 4 \equiv 1 \pmod{11} \Rightarrow 3^{-1} \mod 11 = 4$
- **Question**: What is $2^{-1} \mod 6$?

Examples

- $2 \cdot 2 \equiv 1 \pmod 3 \Rightarrow 2^{-1} \mod 3 = 2$
- $3 \times 4 \equiv 1 \pmod{11} \Rightarrow 3^{-1} \mod 11 = 4$
- **Question**: What is $2^{-1} \mod 6$?

  It doesn't exist!

$$2 \cdot 0 \equiv 0 \pmod 6 \qquad 2 \cdot 3 \equiv 0 \pmod 6$$
$$2 \cdot 1 \equiv 2 \pmod 6 \qquad 2 \cdot 4 \equiv 2 \pmod 6$$
$$2 \cdot 2 \equiv 4 \pmod 6 \qquad 2 \cdot 5 \equiv 4 \pmod 6$$

Existence of modular inverses

Lemma 1

Let a and m be integers. Then

$$a^{-1} \mod m \quad \text{exists} \ \Leftrightarrow \ \gcd(a, m) = 1.$$

Proof. Optional. See textbook.

Find modular inverse by brute force

How to find $a^{-1} \mod m$?

Find modular inverse by brute force

How to find $a^{-1} \mod m$?

1. Check if $\gcd(a, m) = 1$.
   - If $\gcd(a, m) > 1$, then $a^{-1} \mod m$ doesn't exist.
   - If $\gcd(a, m) = 1$, proceed to the next step.

Find modular inverse by brute force

How to find $a^{-1} \mod m$?

1. Check if $\gcd(a, m) = 1$.
   - If $\gcd(a, m) > 1$, then $a^{-1} \mod m$ doesn't exist.
   - If $\gcd(a, m) = 1$, proceed to the next step.
2. We need to find b such that $ab \equiv 1 \pmod{m}$.
   - One solution: Try all possibilities
   $$b \in \{1, \ldots, m-1\}.$$
   - Problem: If m is large (a 20-digit number for example), this is time-consuming.

Find a^{-1} mod m by extended Euclidean algorithm

1. Find Bezout coefficients s and t of a and m:

$$as + mt = \gcd(a, m) = 1 \tag{3}$$

Find a^{-1} mod m by extended Euclidean algorithm

1. Find Bezout coefficients s and t of a and m:

$$as + mt = \gcd(a, m) = 1 \tag{3}$$

2. The equation (3) implies $as \equiv 1 \pmod{m}$. So

$$s = a^{-1} \mod m$$

Example 5

Find the following modular inverses

(a) 3^{-1} mod 7.

(b) 101^{-1} mod 4620.

Solution

Example 5

Find the following modular inverses

(a) 3^{-1} mod 7.

(b) 101^{-1} mod 4620.

Solution

(a) It is simple to check that

$$3 \cdot 5 \equiv 1 \pmod{7} \Rightarrow 3^{-1} \mod 7 = 5$$

Example 5

Find the following modular inverses
(a) $3^{-1} \mod 7$.
(b) $101^{-1} \mod 4620$.

Solution

(a) It is simple to check that

$$3 \cdot 5 \equiv 1 \pmod 7 \Rightarrow 3^{-1} \mod 7 = 5$$

(b) We need to find $s \in \mathbb{Z}^+$ such that

$$101s \equiv 1 \pmod{4620}$$

We can do this by finding Bezout coefficients of 101 and 4620.

Example 5b solution: $101^{-1} \mod 4620$

- First, we find $\gcd(101, 4620)$ by Euclidean algorithm

$$
\begin{aligned}
4620 &= 101 \times 45 + 75 \\
101 &= 75 \times 1 + 26 \\
75 &= 26 \times 2 + 23 \\
26 &= 23 \times 1 + 3 \\
23 &= 3 \times 7 + 2 \\
3 &= 2 \times 1 + 1 \\
2 &= 1 \times 2 + 0.
\end{aligned}
$$

- $\gcd(101, 4620) = 1 \Rightarrow 101^{-1} \mod 4620$ exists by Lemma 2.

Example 5b: $101^{-1} \mod 4620$

- Starting from the 2nd last equation, we work backwards

$$\begin{aligned}
1 &= 3 + 2 \times (-1) \\
&= 3 - (23 - 3 \times 7) = -23 + 3 \times 8 \\
&= -23 + (26 - 23 \times 1) \times 8 = 26 \times 8 - 23 \times 9 \\
&= 26 \times 8 - (75 - 26 \times 2) \times 9 = -75 \times 9 + 26 \times 26 \\
&= -75 \times 9 + (101 - 75 \times 1) \times 26 = 101 \times 26 - 75 \times 35 \\
&= 101 \times 26 - (4620 - 101 \times 45) \times 35 \\
&= 4620 \times (-35) + 101 \times 1601.
\end{aligned}$$

Example 5b: $101^{-1} \mod 4620$

- Starting from the 2nd last equation, we work backwards

$$
\begin{aligned}
1 &= 3 + 2 \times (-1) \\
&= 3 - (23 - 3 \times 7) = -23 + 3 \times 8 \\
&= -23 + (26 - 23 \times 1) \times 8 = 26 \times 8 - 23 \times 9 \\
&= 26 \times 8 - (75 - 26 \times 2) \times 9 = -75 \times 9 + 26 \times 26 \\
&= -75 \times 9 + (101 - 75 \times 1) \times 26 = 101 \times 26 - 75 \times 35 \\
&= 101 \times 26 - (4620 - 101 \times 45) \times 35 \\
&= 4620 \times (-35) + 101 \times 1601.
\end{aligned}
$$

- $101 \times 1601 + 4620 \times (-35) = 1 \Rightarrow 101 \times 1601 \equiv 1 \pmod{4620}$

$$101^{-1} \mod 4620 = 1601.$$

Solving Linear Congruences

- How to solve $ax = b$?

Solving Linear Congruences

- How to solve $ax = b$?

  Multiply both sides of $ax = b$ by a^{-1}

$$x = ba^{-1}$$

Solving Linear Congruences

- How to solve $ax = b$?

  Multiply both sides of $ax = b$ by a^{-1}

$$x = ba^{-1}$$

- Solve $ax \equiv b \pmod{m}$?
  1. Find $c = a^{-1} \mod m$ (if it exists)
  2. Multiplying both sides of $ax \equiv b \pmod{m}$ by c, we obtain

$$x \equiv bc \pmod{m}$$

Solving Linear Congruences

- How to solve $ax = b$?

  Multiply both sides of $ax = b$ by a^{-1}

$$x = ba^{-1}$$

- Solve $ax \equiv b \pmod{m}$?
  1. Find $c = a^{-1} \mod m$ (if it exists)
  2. Multiplying both sides of $ax \equiv b \pmod{m}$ by c, we obtain

$$x \equiv bc \pmod{m}$$

Problem: If $\gcd(a, m) = 1$, we can find $c = a^{-1} \mod m$ easily by extended Euclidean algorithm. What about $\gcd(a, m) \neq 1$?

Modular division

Lemma 2

Let a, b, c, d, n be integers with $\gcd(c, n) = 1$. The following hold.

(a) If $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.

(b) If $ad \equiv bd \pmod{nd}$, then $a \equiv b \pmod{n}$.

What the lemma says?

Modular division

Lemma 2

Let a, b, c, d, n be integers with $\gcd(c, n) = 1$. The following hold.

(a) If $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.

(b) If $ad \equiv bd \pmod{nd}$, then $a \equiv b \pmod{n}$.

What the lemma says?

(a) We can divide both sides of $ac \equiv bc \pmod{n}$ by c if $\gcd(c, n) = 1$.

(b) We can divide all terms in $ad \equiv bd \pmod{nd}$ by the common factor d .

Example 6

Solve the following linear congruences.

(a) $3x \equiv 4 \pmod 7$

(b) $202x \equiv 2 \pmod{9240}$

Remark. You are free to use $\gcd(202, 9240) = 2$.

Solving $ax \equiv b \pmod{m}$

Theorem 2

Let a, b, m be integers. Then the following hold.

(a) $ax \equiv b \pmod{m}$ has solution $\Leftrightarrow \gcd(a, m) \mid b$.

Solving $ax \equiv b \pmod{m}$

Theorem 2

Let a, b, m be integers. Then the following hold.

(a) $ax \equiv b \pmod{m}$ has solution $\Leftrightarrow \gcd(a, m) \mid b$.

(b) Assume $d = \gcd(a, m) \mid b$. Put $a = da_1, b = db_1, m = dm_1$. Then

$$ax \equiv b \pmod{m} \Leftrightarrow a_1 x \equiv b_1 \pmod{m_1}$$

Furthermore, the solution to $ax \equiv b \pmod{m}$ is

$$x \equiv b_1 a_2 \pmod{m_1},$$

where $a_2 = a_1^{-1} \mod m_1$.

Solving $ax \equiv b \pmod{m}$

To solve $ax \equiv b \pmod{m}$, we do the following

1. Find $d = \gcd(a, m)$.
   - If $d \nmid b$, then the equation has no solution.
   - If $d \mid b$, proceed to the next step.

Solving $ax \equiv b \pmod{m}$

To solve $ax \equiv b \pmod{m}$, we do the following

1. Find $d = \gcd(a, m)$.
   - If $d \nmid b$, then the equation has no solution.
   - If $d \mid b$, proceed to the next step.
2. Write $a = da_1, m = dm_1, b = db_1$.

$$\begin{aligned} ax \equiv b \pmod{m} &\Leftrightarrow da_1 x \equiv db_1 \pmod{dm_1} \\ &\Leftrightarrow a_1 x \equiv b_1 \pmod{m_1} \text{ (Lemma 2b)} \end{aligned}$$

Solving $ax \equiv b \pmod m$

To solve $ax \equiv b \pmod m$, we do the following

1. Find $d = \gcd(a, m)$.
   - If $d \nmid b$, then the equation has no solution.
   - If $d \mid b$, proceed to the next step.
2. Write $a = da_1, m = dm_1, b = db_1$.

$$\begin{aligned} ax \equiv b \pmod m &\Leftrightarrow da_1x \equiv db_1 \pmod{dm_1} \\ &\Leftrightarrow a_1x \equiv b_1 \pmod{m_1} \text{ (Lemma 2b)} \end{aligned}$$

3. Let $a_2 = a_1^{-1} \mod m_1$. The solution to $ax \equiv b \pmod m$ is

$$x \equiv b_1a_2 \pmod{m_1}.$$

Equivalently, $x = b_1a_2 + km_1$ for $k \in \mathbb{Z}$.

Exercise

Solve the following congruences.

(a) $7x \equiv 11 \pmod{56}$.

(b) $7x \equiv 11 \pmod{24}$.

Exercise

(c) $91x \equiv 14 \pmod{847}$.