§1.3, 1.4: Congruences and Integers Modulo n

Shaoyun Yi

MATH 546/701I

University of South Carolina

Spring 2022

Greatest Common Divisor

For $a, b \in \mathbf{Z}$, a is called a **multiple** of b if $a = bq$ for some integer q. In this case, we also say that b is a **divisor** of a, and we write $b|a$.

If $a, b \in \mathbf{Z}$, not both zero, and d is a positive integer, then d is called the **greatest common divisor** of a and b (write $d = \gcd(a, b)$ or (a, b)) if

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

For example, $(4, 6) = 2$, $(12, 30) = 6$.

A **linear combination** of a and b has the form $ma + nb$, where $m, n \in \mathbf{Z}$.

Theorem 1

The $d = \gcd(a, b)$ is the **smallest** *positive linear combination of a and b. And an integer is a linear combination of a and b* **iff** *it is a multiple of d.*

Euclidean Algorithm

Division Algorithm: For any $a, b \in \mathbf{Z}$ with $b > 0$, there exist unique integers q (*quotient*) and r (*remainder*) s.t. $a = bq + r$ with $0 \leq r < b$.

$(a, b) = (b, r)$: To show $(b, r)|(a, b)$ and $(a, b)|(b, r)$. (Use Theorem 1)

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

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

In particular, if $r_1 = 0$, then $b|a$, and so $(a, b) = b$.

Since $r_1 > r_2 > \ldots$, after a finite number of steps we obtain a remainder $r_{n+1} = 0$, i.e., the algorithm ends with the equation $r_{n-1} = r_n q_{n+1} + 0$.

This gives us the greatest common divisor

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

Example: Use the Euclidean algorithm to find $(126, 35)$.

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

$\rightsquigarrow (126, 35) = (35, 21) = (21, 14) = (14, 7) = (7, 0) = 7$ □

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

Idea: Reverse the Euclidean algorithm:

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

$\rightsquigarrow$ The desired linear combination is $2 \cdot 126 + (-7) \cdot 35 = 7$. □

Matrix Form of the Euclidean Algorithm

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

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

The procedure continues until one of entries in the right-hand column is 0.

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: $(126, 35) = 7$

$$\begin{bmatrix} 1 & 0 & 126 \\ 0 & 1 & 35 \end{bmatrix} \qquad (126 = 35 \cdot 3 + 21)$$

$$\rightsquigarrow \begin{bmatrix} 1 & -3 & 21 \\ 0 & 1 & 35 \end{bmatrix} \qquad (35 = 21 \cdot 1 + 14)$$

$$\rightsquigarrow \begin{bmatrix} 1 & -3 & 21 \\ -1 & 4 & 14 \end{bmatrix} \qquad (21 = 14 \cdot 1 + 7)$$

$$\rightsquigarrow \begin{bmatrix} 2 & -7 & 7 \\ -1 & 4 & 14 \end{bmatrix} \qquad (14 = 7 \cdot 2 + 0)$$

$$\rightsquigarrow \begin{bmatrix} 2 & -7 & 7 \\ -5 & 18 & 0 \end{bmatrix}$$

$\rightsquigarrow (126, 35) = 7$ and the linear combination $2 \cdot 126 + (-7) \cdot 35 = 7$. ✓

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

Relatively Prime

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

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

Theorem 1: (a, b) is the smallest positive linear combination of a and b □

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

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

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

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

i) Write $1 = (a, b) = ma + nb \quad \Rightarrow c = 1 \cdot c = mac + ncb \quad \Rightarrow b|c$

ii) Write $a = bq \quad \Rightarrow c|bq \quad \Rightarrow c|q$ [Why?] Thus, $bc|a$ since $a = bq$.

iii) "$\Rightarrow$:" Write $ma + nbc = 1 \quad \Rightarrow ma + (nb)c = ma + (nc)b = 1$

"$\Leftarrow$:" $m_1 a + n_1 b = 1, m_2 a + n_2 c = 1 \quad \Rightarrow (m_1 a + n_1 b)(m_2 a + n_2 c) = 1$

$\Rightarrow (\cdots)a + (n_1 n_2)bc = 1 \quad \Rightarrow (a, bc) = 1$ □

Least Common Multiple

If a and b are nonzero integers, and m is a positive integer, then m is called the **least common multiple** of a and b (write $m = \mathrm{lcm}[a, b]$ or $[a, b]$) if

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

For example, $[4, 6] = 12$, $[12, 30] = 60$. Recall $(4, 6) = 2$, $(12, 30) = 6$.

Let a and b be positive integers. Then $(a, b) \cdot [a, b] = ab$.

Proof: By prime factorizations, we let $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ and $b = p_1^{\beta_1} \cdots p_n^{\beta_n}$. For each $i \in \{1, \dots, n\}$, we let

$$\delta_i = \min\{\alpha_i, \beta_i\} \quad \text{and} \quad \mu_i = \max\{\alpha_i, \beta_i\}.$$

Then

$$(a, b) = p_1^{\delta_1} \cdots p_n^{\delta_n} \quad \text{and} \quad [a, b] = p_1^{\mu_1} \cdots p_n^{\mu_n}.$$

Observing that $\delta_i + \mu_i = \alpha_i + \beta_i$ for each i, we have $(a, b) \cdot [a, b] = ab$. □

Congruences

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. We write

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

The integer n is called the **modulus**.

Write $a = nq + r$, where $0 \le r < n$. Observing $r = n \cdot 0 + r$, it follows that

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

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

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 $a - b = n(q_1 - q_2)$.

$(\Leftarrow)$: $n|(a-b) \quad \Rightarrow a - b = nk$ for some $k \in \mathbf{Z}$. Write $a = nq + r$, then

$$b = a - nk = nq + r - nk = n(q-k) + r.$$

Thus, a and b have the same remainder r when divided by n. □

Properties of Congruences

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad n \mid (a-b)$$

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

Moreover, the following properties 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 $c \equiv d \pmod{n}$.

1) & 2) ✓. 3) $ac \equiv ad \pmod{n} \Rightarrow n \mid a(c-d) \Rightarrow n \mid (c-d)$ [Why?] □

Example 2

$$101 \equiv 5 \pmod 8, 142 \equiv 6 \pmod 8: \begin{cases} 101 + 142 \equiv 5 + 6 \equiv 3 \pmod 8 \\ 101 - 142 \equiv 5 - 6 \equiv 7 \pmod 8 \\ 101 \cdot 142 \equiv 5 \cdot 6 \equiv 6 \pmod 8 \end{cases}$$

In 3), the condition $(a, n) = 1$ is **necessary!**

Example 3

$30 \equiv 6 \pmod 8$, dividing both sides by 6 gives $5 \equiv 1 \pmod 8$: False!

Since $(3, 8) = 1$, dividing both sides by 3 gives $10 \equiv 2 \pmod 8$: True.

Linear Congruences

Let a and $n > 1$ be integers.

There exists $b \in \mathbf{Z}$ such that $ab \equiv 1 \pmod{n}$ if and only if $(a, n) = 1$.

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

$(\Leftarrow)$: $sa + tn = 1$ for some $s, t \in \mathbf{Z}$. Then s is the desired integer. □

That is to say, $ax \equiv 1 \pmod{n}$ has a solution if and only if $(a, n) = 1$.

Use the **Euclidean algorithm** to get the solution by writing $1 = ab + nq$.

Q: What about a linear congruence of the form $ax \equiv b \pmod{n}$?

(1) Let $d = (a, n)$. Then $ax \equiv b \pmod{n}$ has a solution if and only if $d|b$.

(2) If $d|b$, then there are d distinct solutions modulo n. These solutions are congruent modulo n/d.

An Algorithm for Solving $ax \equiv b \pmod{n}$

i) Find $d = (a, n)$. If $d | b$, then $ax \equiv b \pmod{n}$ has a solution.

ii) Divide both sides by d:

$$a_1 x \equiv b_1 \pmod{n_1} \quad \text{with } (a_1, n_1) = 1,$$

where $a_1 = a/d, b_1 = b/d$, and $n_1 = n/d$.

iii) Find $c \in \mathbf{Z}$ such that $a_1 c \equiv 1 \pmod{n_1}$.

- Euclidean algorithm;
- trial and error (*quicker for a small modulus*).

iv) Multiplying both sides of $a_1 x \equiv b_1 \pmod{n_1}$ by c gives the solution

$$x \equiv b_1 c \equiv s_0 \pmod{n_1} \quad \text{with } 0 \leq s_0 < n_1.$$

v) The solution modulo n_1 determines d **distinct solutions modulo** n:

$$x \equiv s_0 + kn_1 \pmod{n}, \quad \text{where } k = 0, 1, \ldots, d-1.$$

Example: Solve $60x \equiv 90 \pmod{105}$

i) $d = (60, 105) = (60, 45) = (45, 15) = (15, 0) = 15 | 90$ ✓

ii) Dividing both sides by 15:

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

iii) Find an integer c such that $4c \equiv 1 \pmod{7}$.

- Euclidean algorithm;
- trial and error: $c = 2$.

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

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

v) There are 15 **distinct solutions modulo** 105.

$$x \equiv 5 + 7k \pmod{105}, \quad \text{where } k = 0, 1, \ldots, 14.$$

Or

$$x \equiv 5, 12, 19, 26, 33, 40, 47, 54, 61, 68, 75, 82, 89, 96, 103 \pmod{105}.$$

Congruence Classes Modulo n

Let a and $n > 0$ be integers. The **congruence class of a modulo n**

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

An element of $[a]_n$ is called a **representative of the congruence class**.

Each congruence class $[a]_n$ has a unique non-negative representative that is smaller than n, i.e., the remainder when a is divided by n.

Thus, there are exactly n distinct congruence classes modulo n. We write

$\mathbf{Z}_n := \{[0]_n, [1]_n, \ldots, [n-1]_n\}$, which is the **set of integers modulo n**.

For example, the congruence classes modulo 3 are

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

That is, $\mathbf{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$.

Example 4

$\mathbf{Z}_2 = \{[0]_2, [1]_2\}$: $[0]_2$ (resp. $[1]_2$) is the set of even (resp. odd) numbers.

The below are the addition and multiplication tables in $\mathbf{Z}_2$.

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

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

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**:

$$[a]_n + [b]_n = [a+b]_n \qquad \text{and} \qquad [a]_n \cdot [b]_n = [ab]_n.$$

Properties of Addition and Multiplication for $\mathbf{Z}_n$

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: $[a]_n + [b]_n = [b]_n + [a]_n$

$$[a]_n \cdot [b]_n = [b]_n \cdot [a]_n$$

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

Identities: $[a]_n + [0]_n = [a]_n$

$$[a]_n \cdot [1]_n = [a]_n$$

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

Q: What about **Multiplicative inverses**? **A:** Not always

No cancellation law for $\cdot$: e.g., $[6]_8 \cdot [5]_8 = [6]_8 \cdot [1]_8$, but $[5]_8 \neq [1]_8$.

Divisor of Zero and Unit in $\mathbf{Z}_n$

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

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

Proof: $[a]_n([b]_n - [c]_n) = [a]_n[b-c]_n = [0]_n \quad \Rightarrow [b]_n - [c]_n = [0]_n$. □

If $[a]_n \in \mathbf{Z}_n$ and $[a]_n[b]_n = [1]_n$ for some $[b]_n$, then $[b]_n = [a]_n^{-1}$ is called a **multiplicative inverse** of $[a]_n$. In this case, $[a]_n$ is called a **unit** of $\mathbf{Z}_n$.

We will omit the subscript on congruence classes if the meaning is clear.

If $[a]$ is a unit of $\mathbf{Z}_n$, then it cannot be a divisor of zero.

Proof: If $[a][b] = [0] \quad \Rightarrow [a]^{-1} \cdot [a][b] = [a]^{-1} \cdot [0] \quad \Rightarrow [b] \overset{!}{=} [0]$ □

i) $[a]$ is a unit of $\mathbf{Z}_n$ if and only if $(a, n) = 1$.

ii) A non-zero element $[a]$ of $\mathbf{Z}_n$ is either a unit or a divisor of zero.

Example: Find $[11]^{-1}$ in $\mathbf{Z}_{16}$

i) Use 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 implies $[11]^{-1} = [3]$.

ii) Take successive powers of $[11]$:

$$\begin{aligned} [11]^2 =& [-5]^2 = [25] = [9], \\ [11]^3 =& [11]^2[11] = [9][11] = [99] = [3], \\ [11]^4 =& [11]^3[11] = [3][11] = [33] = [1]. \end{aligned}$$

Thus $[11]^{-1} = [11]^3 = [3]$.

Euler's Totient Function

Let n be a positive integer. **Euler's φ-function**, or the **totient function**

$$\varphi(n) = \#\{a \in \mathbf{Z} \colon (a, n) = 1 \text{ and } 1 \leq a \leq n\}.$$

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

If the prime factorization of n is $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ with $\alpha_i > 0$, then

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

In particular, $\varphi(p) = p - 1$ for any prime number p.

Example 5

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

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

The set of units of $\mathbf{Z}_n$ is $\mathbf{Z}_n^\times = \{[a] \colon (a, n) = 1\}$. $\rightsquigarrow |\mathbf{Z}_n^\times| = \varphi(n)$

$\mathbf{Z}_n^\times$ is closed under multiplication.

$$[a], [b] \in \mathbf{Z}_n^\times \ \Rightarrow (a, n) = (b, n) = 1 \ \Rightarrow (ab, n) = 1 \ \Rightarrow [a][b] = [ab] \in \mathbf{Z}_n^\times$$

In fact, $\mathbf{Z}_n^\times$ is a **group** under multiplication of congruence class.

Euler's Theorem

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

We will give a single-sentence proof later by using group theory! □