3. Number theory and Matrices

Section 3.4: The Integers and Division

<u>Division:</u>

Let $a, b \in \mathbf{Z}$ with $a \neq 0$.

- $a \mid b \equiv$ "*a* **divides** *b*".

  We say that "*a* is a **factor** of *b*", "*a* is a **divisor** of *b*", and "*b* is a **multiple** of *a*".

- a does not divide b is denoted by $a \nmid b$.

- We can express $a \mid b$ using the quantifier

$$\exists\, c\ (b = ac),\ \text{Domain} = \mathbf{Z}.$$

$3 \mid -12 \Leftrightarrow$ **True**, but $3 \mid 7 \Leftrightarrow$ **False**.

The Divides Relations

- For every $a, b, c \in \mathbf{Z}$, we have
  1. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
  2. If $a \mid b$, then $a \mid bc$.
  3. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Examples:

- $3 \mid 12$ and $3 \mid 9 \rightarrow 3 \mid (12 + 9) \rightarrow 3 \mid 21 \ (21 \div 3 = 7)$
- $2 \mid 6 \rightarrow 2 \mid (6 \times 3) \rightarrow 2 \mid 18 \ (18 \div 2 = 9)$
- $4 \mid 8$ and $8 \mid 64 \rightarrow 4 \mid 64 \ (64 \div 4 = 16)$

The Division Algorithm

- let a be an integer and d a positive integer, then there exist unique integers q and r such that:

$$a = d \times q + r \quad , 0 \leq r < d \, .$$

- d is called **divisor** and a is called **dividend.**
- q is the **quotient** and r is the **remainder** (**positive integer**).

$$\boldsymbol{q = a \text{ div } d \quad , \quad r = a \text{ mod } d \, .}$$

Examples

- What are the quotient and remainder when 101 is divided by 11?

$$101 = 11 \times 9 + 2,$$

q = 101 div 11 = 9, r = 101 – 11 × 9 = 2 = 101 mod 9

- What are the quotient and the remainder when −11 is divided by 3?

$$-11 = 3 \times (-4) + 1 \;, \quad \mathbf{q = -4 \,, r = 1}$$

$$q = -11 \operatorname{div} 3 = \left\lfloor \frac{-11}{3} \right\rfloor = \lfloor -3.6 \rfloor = -4$$

$$r = -11 - (-4) \times 3 = 1 = -11 \bmod 3$$

- **Note**:

-11 ≠ 3 × (-3) - 2 because r can't be negative.

Examples

- Find a and b if :

$$2a + b = 46 \bmod 7 \quad \text{and} \quad a + 2b = 47 \operatorname{div} 9.$$

$$46 = 6 \times 7 + \mathbf{4} \quad \text{and} \quad 47 = \mathbf{5} \times 9 + 2$$

$$46 \bmod 7 = 4 \quad \text{and} \quad 47 \operatorname{div} 9 = 5$$

$$2a + b = 4 \ (1) \quad \text{and} \ a + 2b = 5 \ (2)$$

$$(1) - 2\,(2): \quad -3b = -6$$

$$b = 2 \text{ and } a = 1.$$

Section 3.5: Primes and Greatest Common Divisors

- A positive integer $p > 1$ is **prime** if the only positive factors of p are 1 and p.

Some primes: 2, 3, 5, 7, 11, 13, 17, ...

- Non-prime integer greater than 1 are called **composite**, because they can be **composed** by multiplying two integers greater than 1.

Fundamental Theorem of Arithmetic

- Every positive integer greater than 1 has a unique representation as a prime or as the <u>product of two or more primes</u> where the <u>prime factors</u> are written in order of non-decreasing size. (tree or division)

  $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$

  $13 = 13$

  $1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

Its "Prime Factorization"

Theorem

- If n is a **composite** integer, then n has prime divisor $\leq \sqrt{n}.$

  e.g. 49 → prime numbers less than $\sqrt{49}$ are 2, 3, 5, 7

  16 → prime numbers less than $\sqrt{16}$ are 2, 3.

- An integer n is **prime** if it is not divisible by any prime $\leq \sqrt{n}.$

  e.g. 13 where $\sqrt{13}$ = 3.6 so the prime numbers are 2, 3 but non of them divides 13 so 13 is prime.

Prime Factorization Technique

- To find the prime factor of an integer n :

1. Find $\sqrt{n}$.
2. List all primes $\leq \sqrt{n}$,

   2, 3, 5, 7, … , up to $\sqrt{n}$.
3. Find all prime factors that divides n.

Example 1

Ex: Show that 100 is composite?

Sol.

1) $\sqrt{100} = 10$

2) So the number may be divided by: **2, 3, 5, 7** only (all primes less than 10)

3) $2 \mid 100$ since $100/2 = 50$

$\therefore$ The number 100 is not prime, So it is composite.

Example 2

Ex: Show that 101 is prime?

Sol.

1) $\sqrt{101} \approx 10$

2) So the number may be divided by: **2, 3, 5, 7** only (all primes less than 10)

3) $2 \nmid 101$ $\quad 3 \nmid 101$ $\quad 5 \nmid 101$ $\quad 7 \nmid 101$

101 is not divided by 2, 3, 4, 5, or 7

$\therefore$ The number 101 is prime

Example 3

Ex: find the prime factors of 7007?

1) $\sqrt{7007} \approx 83$

2) So the number may be divided by: 2, 3, 5, 7, 11, 13, 17, 19 …< 83 (all primes less than 83)

3) $\dfrac{7007}{7} = 1001 \qquad \dfrac{1001}{7} = 143 \qquad \dfrac{143}{11} = 13 \qquad \dfrac{13}{13} = 1$

$7007 = 7 \times 7 \times 11 \times 13 = 7^2 \times 11 \times 13$

Discrete Mathematics

Matrices

Section 3.8: Matrices

- An $m \times n$ **matrix** is a rectangular array of mn objects (usually numbers) arranged in m horizontal rows and n vertical columns.

- An $n \times n$ matrix is called a **square** matrix, whose **order** is n.

$$\begin{bmatrix} 2 & 3 \\ 5 & -1 \\ 7 & 0 \end{bmatrix}_{3\times 2} \qquad \begin{bmatrix} 2 & 1 \\ 3 & 1 \end{bmatrix}_{2\times 2}$$

Matrix Equality

- Two matrices *A* and *B* are equal if and only if they have the same number of rows, the same number of columns, and all corresponding elements are equal.

$$\begin{bmatrix} 3 & 2 \\ -1 & 6 \end{bmatrix} \neq \begin{bmatrix} 3 & 2 & 0 \\ -1 & 6 & 0 \end{bmatrix}$$

Row and Column Order

- The rows in a matrix are usually indexed 1 to m from top to bottom. The columns are usually indexed 1 to n from left to right. Elements are indexed by row, then column.

$$A = [a_{ij}] = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

Matrix Sums

- The **sum** $A + B$ of two matrices A, B (which must have the **same** number of rows, and the **same** number of columns) is the matrix given by adding corresponding elements.
- $A + B = [a_{ij} + b_{ij}]$

$$\begin{bmatrix} 2 & 6 \\ 0 & -8 \\ 1 & 2 \end{bmatrix} + \begin{bmatrix} 7 & -5 \\ 4 & -1 \\ 3 & 6 \end{bmatrix} = \begin{bmatrix} 9 & 1 \\ 4 & -9 \\ 4 & 8 \end{bmatrix}$$

Matrix Products

For an $m\times k$ matrix A and a $k\times n$ matrix B, the **product** AB is the $m\times n$ matrix:

$$AB = C = [c_{ij}] \equiv \left[\sum_{p=1}^{k} a_{ip} b_{pj} \right]$$

i.e. The element (i, j) of AB is given by the vector *dot product* of the i^{th} row of A and the j^{th} column of B (considered as vectors).

Note: Matrix multiplication is not commutative!

Matrix Product Example

$$\underset{2\times 3}{\begin{bmatrix} 0 & 1 & -1 \\ 2 & 0 & 3 \end{bmatrix}}\underset{3\times 4}{\begin{bmatrix} 0 & -1 & 1 & 0 \\ 2 & 0 & -2 & 0 \\ 1 & 0 & 3 & 1 \end{bmatrix}} = \underset{2\times 4}{\begin{bmatrix} 1 & 0 & -5 & -1 \\ 3 & -2 & 11 & 3 \end{bmatrix}}$$

Identity Matrices

- The **identity matrix of order *n***, I_n, is the order-n matrix with 1's along the upper-left to lower-right diagonal and 0's everywhere else.
- $A\,I_n = A$

$$I_n = \left[\begin{cases} 1 \text{ if } i = j \\ 0 \text{ if } i \neq j \end{cases}\right] = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

Powers of Matrices

- If A is an $n\times n$ square matrix and $p \geq 0$, then:

$$A^p \equiv \underbrace{AAA \cdots A}_{p \text{ times}} \quad (A^0 \equiv I_n)$$

$$\begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix}^3 = \begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 3 & 2 \\ -2 & -1 \end{bmatrix} = \begin{bmatrix} 4 & 3 \\ -3 & -2 \end{bmatrix}$$

Matrix Transposition

- If A is an $m\times n$ matrix, then the **transpose** of A is the $n\times m$ matrix A^T given by interchanging the rows and the columns of A.

$$A=\begin{bmatrix} 2 & 1 & 3 \\ 0 & -1 & -2 \end{bmatrix} \Rightarrow A^T=\begin{bmatrix} 2 & 0 \\ 1 & -1 \\ 3 & -2 \end{bmatrix}$$

Symmetric Matrices

- A square matrix A is **symmetric** if and only if $A^T = A$.
- Which is symmetric?

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{bmatrix} \qquad B = \begin{bmatrix} -2 & 1 & 3 \\ 1 & 0 & -1 \\ 3 & -1 & 2 \end{bmatrix} \qquad C = \begin{bmatrix} 3 & 0 & 1 \\ 0 & 2 & -1 \\ 1 & 1 & -2 \end{bmatrix}$$

Zero-One Matrices

All elements of a **zero-one** matrix are 0 or 1, representing **False** & **True** respectively.

- The **join** of A and B (both $m \times n$ zero-one matrices) is

$$A \vee B :\equiv [a_{ij} \vee b_{ij}].$$

- The **meet** of A and B is:

$$A \wedge B \equiv [a_{ij} \wedge b_{ij}].$$

Example

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \qquad B = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

- The **join** between A and B is $A \vee B = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$
- The **meet** between A and B is $A \wedge B = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$

Boolean Products

- Let A be an $m \times k$ zero-one matrix and B be a $k \times n$ zero-one matrix,
- The **Boolean product** $A \odot B$ of A and B is like normal matrix product, **but using $\vee$ instead $+$ and using $\wedge$ instead $\times$.**

Boolean Powers

- For a square zero-one matrix A, and any $k \geq 0$, the k^{th} **Boolean power** *of* A is simply the Boolean product of k copies of A.

$$A^{[k]} \equiv \underbrace{A \odot A \odot \ldots \odot A}_{k \text{ times}}$$

Example

Let $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$

$$A \odot B = \begin{bmatrix} (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \\ (0 \wedge 1) \vee (1 \wedge 0) & (0 \wedge 1) \vee (1 \wedge 1) & (0 \wedge 0) \vee (1 \wedge 1) \\ (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$