

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○

Number Theory

○○○○○○○○
○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Some Math Notes

Yuchong Pan

Faculty of Science, University of British Columbia

July 20, 2016

Linear Algebra

oooooooooooooooooooo
oooooooooooo
oooooooooooo

Number Theory

oooooooo
oooooo
oooooooooooo
ooooooo
ooooooo
ooooooo

Numerical Analysis

ooooooo

Happy Birthday to liyang21 !

Linear Algebra

oooooooooooooooooooo
oooooooooooo
oooooooooooo

Number Theory

oooooooo
oooooo
oooooooooooo
ooooooo
ooooooo
oooooooooooo

Numerical Analysis

ooooooo

Outline

1 Linear Algebra

- Gaussian Elimination
- Determinant
- Matrix Product

2 Number Theory

- Divisibility
- Primes
- Congruence Relation
- Chinese Remainder Theorem
- Euler's Totient Function
- Modular Multiplicative Inverse

3 Numerical Analysis

- Lagrange Interpolation

Linear Algebra

oooooooooooooooooooo
oooooooooooo
oooooooooooo

Number Theory

oooooooo
oooooo
oooooooooooo
ooooooo
ooooooo
oooooooooooo

Numerical Analysis

ooooooo

Outline

1 Linear Algebra

- Gaussian Elimination
- Determinant
- Matrix Product

2 Number Theory

- Divisibility
- Primes
- Congruence Relation
- Chinese Remainder Theorem
- Euler's Totient Function
- Modular Multiplicative Inverse

3 Numerical Analysis

- Lagrange Interpolation

Linear Algebra

●○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Gaussian Elimination

Number Theory

○○○○○○○○
○○○○○○
○○○○○○○○○○
○○○○○○○○
○○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Matrix and System of Equations

Linear Algebra

●○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○

Gaussian Elimination

Number Theory

○○○○○○○
○○○○○○○
○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○

Matrix and System of Equations

- A **system of linear equations** consisting of m equations and of n unknown variables is given as

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases}$$

Linear Algebra

○●○○○○○○○○○○○○○○
○○○○○○○○○
○○○○○○○○○○○○

Gaussian Elimination

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Matrix and System of Equations

Gaussian Elimination

Matrix and System of Equations

- The system of equations above can be written as an augmented matrix

$$\left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & & & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array} \right)$$

Linear Algebra

○○●○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Gaussian Elimination

Number Theory

○○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Row Operations

Linear Algebra

○○●○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Gaussian Elimination

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Row Operations

- There are 3 types of elementary row operations:

Linear Algebra

○○●○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Gaussian Elimination

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Row Operations

- There are 3 types of elementary row operations:
- **Type 1:** Swap the positions of two rows.

Linear Algebra

○○●○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Gaussian Elimination

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Row Operations

- There are 3 types of elementary row operations:
- **Type 1:** Swap the positions of two rows.
- **Type 2:** Multiply a row by a nonzero scalar.

Linear Algebra

○○●○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Gaussian Elimination

Number Theory

○○○○○○○○
○○○○○○
○○○○○○○○○○
○○○○○○○○
○○○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○○

Row Operations

- There are 3 types of elementary row operations:
- **Type 1:** Swap the positions of two rows.
- **Type 2:** Multiply a row by a nonzero scalar.
- **Type 3:** Add to one row a scalar multiple of another.

Row Operations

- There are 3 types of elementary row operations:
- **Type 1:** Swap the positions of two rows.
- **Type 2:** Multiply a row by a nonzero scalar.
- **Type 3:** Add to one row a scalar multiple of another.
- If a matrix is associated to a system of linear equations, then these three types of row operations do not change the solution set.

Linear Algebra

○○○●○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Gaussian Elimination

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Row Echelon Form

Gaussian Elimination

Row Echelon Form

- For each row in a matrix, if the row does not consist of only zeros, then the left-most nonzero entry is called the **leading coefficient** (or **pivot**) of that row.

Gaussian Elimination

Row Echelon Form

- For each row in a matrix, if the row does not consist of only zeros, then the left-most nonzero entry is called the **leading coefficient** (or **pivot**) of that row.
- A matrix is in the **row echelon form** if
 - all nonzero rows are above any rows of all zeros, and
 - the leading coefficient of a nonzero row is always strictly to the right of the leading coefficient of the row above it.

Row Echelon Form

- For each row in a matrix, if the row does not consist of only zeros, then the left-most nonzero entry is called the **leading coefficient** (or **pivot**) of that row.
- A matrix is in the **row echelon form** if
 - all nonzero rows are above any rows of all zeros, and
 - the leading coefficient of a nonzero row is always strictly to the right of the leading coefficient of the row above it.
- Hence, the lower left part of the matrix contains only zeros.

Row Echelon Form

- For each row in a matrix, if the row does not consist of only zeros, then the left-most nonzero entry is called the **leading coefficient** (or **pivot**) of that row.
- A matrix is in the **row echelon form** if
 - all nonzero rows are above any rows of all zeros, and
 - the leading coefficient of a nonzero row is always strictly to the right of the leading coefficient of the row above it.
- Hence, the lower left part of the matrix contains only zeros.
- For example, the following matrix is in the row echelon form, and its leading coefficients are shown in red.

$$\begin{pmatrix} 0 & \color{red}{2} & 1 & -1 \\ 0 & 0 & \color{red}{3} & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Linear Algebra

○○○●○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Gaussian Elimination

Gaussian Elimination

Gaussian Elimination

Gaussian Elimination

- The procedure of using the 3 types of the elementary row operations to transform an augmented matrix associated to a system of linear equations to the row echelon form is called **Gaussian elimination** (or **forward elimination**).

Gaussian Elimination

- The procedure of using the 3 types of the elementary row operations to transform an augmented matrix associated to a system of linear equations to the row echelon form is called **Gaussian elimination** (or **forward elimination**).
- If two leading coefficients are in the same column, then a row operation of type 3 could be used to make one of those coefficients zero.

Gaussian Elimination

- The procedure of using the 3 types of the elementary row operations to transform an augmented matrix associated to a system of linear equations to the row echelon form is called **Gaussian elimination** (or **forward elimination**).
- If two leading coefficients are in the same column, then a row operation of type 3 could be used to make one of those coefficients zero.
- Then, by using the row operations of type 1 (i.e., the row swapping operations), one can always order the rows so that, for every nonzero rows, the leading coefficient is to the right of the leading coefficient of the row above.

Linear Algebra

○○○○●○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Gaussian Elimination

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Example

Example

- The original augmented matrix is

$$\left(\begin{array}{ccc|c} 2 & 1 & -1 & 8 \\ -3 & -1 & 2 & -11 \\ -2 & 1 & 2 & -3 \end{array} \right)$$

Linear Algebra

oooooooo●oooooooooooo
oooooooooooo
oooooooooooo

Gaussian Elimination

Number Theory

oooooooo
oooooo
oooooooooooo
ooooooo
ooooooo
oooooooo

Numerical Analysis

oooooooo

Example

- The original augmented matrix is

$$\left(\begin{array}{ccc|c} 2 & 1 & -1 & 8 \\ -3 & -1 & 2 & -11 \\ -2 & 1 & 2 & -3 \end{array} \right)$$

- After the row operations $L_2 + \frac{3}{2}L_1 \rightarrow L_2$ and $L_3 + L_1 \rightarrow L_3$, the augmented matrix is transformed to

$$\left(\begin{array}{ccc|c} 2 & 1 & -1 & 8 \\ 0 & \frac{1}{2} & \frac{1}{2} & 1 \\ 0 & 2 & 1 & 5 \end{array} \right)$$

Linear Algebra

○○○○○●○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Gaussian Elimination

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Example

Linear Algebra

oooooooo●oooooooooooo
oooooooooooo
oooooooooooo

Gaussian Elimination

Number Theory

oooooooooooo
oooooooooooo
oooooooooooo
oooooooooooo
oooooooooooo
oooooooooooo

Numerical Analysis

oooooooooooo

Example

- Then, after the row operation $L_3 - 4L_2 \rightarrow L_3$, the augmented matrix is transformed to

$$\left(\begin{array}{ccc|c} 2 & 1 & -1 & 8 \\ 0 & \frac{1}{2} & \frac{1}{2} & 1 \\ 0 & 0 & -1 & 1 \end{array} \right)$$

Example

- Then, after the row operation $L_3 - 4L_2 \rightarrow L_3$, the augmented matrix is transformed to

$$\left(\begin{array}{ccc|c} 2 & 1 & -1 & 8 \\ 0 & \frac{1}{2} & \frac{1}{2} & 1 \\ 0 & 0 & -1 & 1 \end{array} \right)$$

- The matrix is now in the row echelon form (or the triangular form).

Linear Algebra

○○○○○○○●○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Gaussian Elimination

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Number of Solutions

Gaussian Elimination

Number of Solutions

- If the row echelon form has a row in the following form:

$$(\begin{array}{cccc|c} 0 & 0 & \cdots & 0 & a \end{array})$$

where $a \neq 0$, then this system of linear equations is **inconsistent**, i.e., has no solutions.

Linear Algebra

○○○○○○○●○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Gaussian Elimination

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Number of Solutions

Linear Algebra

○○○○○○○●○○○○○○○
○○○○○○○○○
○○○○○○○○○○○

Gaussian Elimination

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○

Numerical Analysis

○○○○○○○

Number of Solutions

- If the number of variables equals the number of nonzero rows in the row echelon form, then the system of linear equations has a unique solution.

Gaussian Elimination

Number of Solutions

- If the number of variables equals the number of nonzero rows in the row echelon form, then the system of linear equations has a unique solution.
- Otherwise, if the number of nonzero rows in the row echelon form is greater than the number of variables, then the system of linear equations has infinitely many solutions.

Number of Solutions

- If the number of variables equals the number of nonzero rows in the row echelon form, then the system of linear equations has a unique solution.
- Otherwise, if the number of nonzero rows in the row echelon form is greater than the number of variables, then the system of linear equations has infinitely many solutions.
- If the k -th column has no leading coefficients, then the variable x_k is said to be a **free variable**, meaning that x_k can be any real number.

Number of Solutions

- If the number of variables equals the number of nonzero rows in the row echelon form, then the system of linear equations has a unique solution.
- Otherwise, if the number of nonzero rows in the row echelon form is greater than the number of variables, then the system of linear equations has infinitely many solutions.
- If the k -th column has no leading coefficients, then the variable x_k is said to be a **free variable**, meaning that x_k can be any real number.
- Hence, for each given tuple of free variables, the system of linear equations has exactly one solution.

Linear Algebra

○○○○○○○○●○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Gaussian Elimination

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Example

Gaussian Elimination

Example

- For example, the matrix

$$\left(\begin{array}{ccccc|c} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

has infinitely many solutions and 2 variables x_2 and x_4 .

Linear Algebra

○○○○○○○○●○○○○○
○○○○○○○○○
○○○○○○○○○○○

Gaussian Elimination

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Example

Gaussian Elimination

Example

- Given that $x_2 = x_4 = 0$, then $x_5 = 3, x_3 = -6, x_1 = 4$, and hence

$$\begin{cases} x_1 = 4 \\ x_2 = 0 \\ x_3 = -6 \\ x_4 = 0 \\ x_5 = 3 \end{cases}$$

is a solution to the system of equations.

Linear Algebra

○○○○○○○○○●○○○○
○○○○○○○○○
○○○○○○○○○○○

Gaussian Elimination

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Reduced Row Echelon Form

Reduced Row Echelon Form

- A matrix is said to be in the **reduced row echelon form** if
 - it is in the row echelon form,
 - all of the leading coefficients are equal to 1, and
 - in every column containing a leading coefficient, all of the other entries in that column are zero.

Reduced Row Echelon Form

- A matrix is said to be in the **reduced row echelon form** if
 - it is in the row echelon form,
 - all of the leading coefficients are equal to 1, and
 - in every column containing a leading coefficient, all of the other entries in that column are zero.
- The second condition can be achieved by the elementary row operations of type 2, and the third condition can be achieved by the elementary row operations of type 3.

Gaussian Elimination

Reduced Row Echelon Form

- A matrix is said to be in the **reduced row echelon form** if
 - it is in the row echelon form,
 - all of the leading coefficients are equal to 1, and
 - in every column containing a leading coefficient, all of the other entries in that column are zero.
- The second condition can be achieved by the elementary row operations of type 2, and the third condition can be achieved by the elementary row operations of type 3.
- This procedure is called **Gauss-Jordan elimination** (or the **back substitution**).

Reduced Row Echelon Form

- A matrix is said to be in the **reduced row echelon form** if
 - it is in the row echelon form,
 - all of the leading coefficients are equal to 1, and
 - in every column containing a leading coefficient, all of the other entries in that column are zero.
- The second condition can be achieved by the elementary row operations of type 2, and the third condition can be achieved by the elementary row operations of type 3.
- This procedure is called **Gauss-Jordan elimination** (or the **back substitution**).
- The total time complexity of forward elimination and back substitution is $O(n^3)$.

Linear Algebra

○○○○○○○○○○●○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Gaussian Elimination

Number Theory

○○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○○

Example

Example

- Assuming that a matrix has been transformed to the row echelon form as follows.

$$\left(\begin{array}{ccc|c} 2 & 1 & -1 & 8 \\ 0 & \frac{1}{2} & \frac{1}{2} & 1 \\ 0 & 0 & -1 & 1 \end{array} \right)$$

Example

- Assuming that a matrix has been transformed to the row echelon form as follows.

$$\left(\begin{array}{ccc|c} 2 & 1 & -1 & 8 \\ 0 & \frac{1}{2} & \frac{1}{2} & 1 \\ 0 & 0 & -1 & 1 \end{array} \right)$$

- After 2 row operations $L_2 + \frac{1}{2}L_3 \rightarrow L_2$ and $L_1 - L_3 \rightarrow L_1$, then the matrix is transformed to

$$\left(\begin{array}{ccc|c} 2 & 1 & 0 & 7 \\ 0 & \frac{1}{2} & 0 & \frac{3}{2} \\ 0 & 0 & -1 & 1 \end{array} \right)$$

Linear Algebra

○○○○○○○○○○○○●○○○
○○○○○○○○○○
○○○○○○○○○○○○

Gaussian Elimination

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Example

Gaussian Elimination

Example

- Then, after another 2 row operations $2L_2 \rightarrow L_2$ and $-L_3 \rightarrow L_3$, we have

$$\left(\begin{array}{ccc|c} 2 & 1 & 0 & 7 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & -1 \end{array} \right)$$

Gaussian Elimination

Example

- Then, after another 2 row operations $2L_2 \rightarrow L_2$ and $-L_3 \rightarrow L_3$, we have

$$\left(\begin{array}{ccc|c} 2 & 1 & 0 & 7 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & -1 \end{array} \right)$$

- Finally, after $L_1 - L_2 \rightarrow L_1$ and $\frac{1}{2}L_1 \rightarrow L_1$, the matrix is transformed to

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & -1 \end{array} \right)$$

Linear Algebra

○○○○○○○○○○○○●○○
○○○○○○○○○
○○○○○○○○○○

Gaussian Elimination

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Example

Linear Algebra

○○○○○○○○○○○○●○○
○○○○○○○○○
○○○○○○○○○○

Gaussian Elimination

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Example

- The matrix is now in the reduced row echelon form, and we obtain the unique solution to the system of linear equations:

$$\begin{cases} x_1 = 2 \\ x_2 = 3 \\ x_3 = -1 \end{cases}$$

Linear Algebra

○○○○○○○○○○○○○●○
○○○○○○○○○○
○○○○○○○○○○

Gaussian Elimination

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

System of XOR Equations

System of XOR Equations

- A system of XOR equations

$$\begin{cases} a_{11}x_1 \otimes a_{12}x_2 \otimes \cdots \otimes a_{1n}x_n = b_1 \\ a_{21}x_1 \otimes a_{22}x_2 \otimes \cdots \otimes a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 \otimes a_{m2}x_2 \otimes \cdots \otimes a_{mn}x_n = b_m \end{cases}$$

where $a_{ij}, b_i, x_j \in \{0, 1\}$ and \otimes is the XOR operation, can be also written as an augmented matrix

$$\left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & & & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array} \right)$$

Linear Algebra

oooooooooooooooooooo●
oooooooooooo
oooooooooooo

Gaussian Elimination

Number Theory

oooooooo
oooooo
oooooooooooo
ooooooo
ooooooo
oooooooo

Numerical Analysis

ooooooo

System of XOR equations

System of XOR equations

- Since the XOR operation can be regarded as the addition operation on the residue system modulo 2, then the 3 types of the elementary row operations are compatible with systems of XOR equations.

System of XOR equations

- Since the XOR operation can be regarded as the addition operation on the residue system modulo 2, then the 3 types of the elementary row operations are compatible with systems of XOR equations.
- Hence, Gaussian elimination can be applied to solve systems of XOR equations.

Gaussian Elimination

System of XOR equations

- Since the XOR operation can be regarded as the addition operation on the residue system modulo 2, then the 3 types of the elementary row operations are compatible with systems of XOR equations.
- Hence, Gaussian elimination can be applied to solve systems of XOR equations.
- Note that there might be many free variables in a system of XOR equations.

System of XOR equations

- Since the XOR operation can be regarded as the addition operation on the residue system modulo 2, then the 3 types of the elementary row operations are compatible with systems of XOR equations.
- Hence, Gaussian elimination can be applied to solve systems of XOR equations.
- Note that there might be many free variables in a system of XOR equations.
- Furthermore, we can use the bitset to optimize Gaussian elimination, and hence a system of XOR equations can be solved in time $O\left(\frac{n^3}{w}\right)$.

Linear Algebra

○○○○○○○○○○○○○○○○
●○○○○○○○○
○○○○○○○○○○○○

Determinant

2 × 2 Matrices

Number Theory

○○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○

Linear Algebra

○○○○○○○○○○○○○○○○
●○○○○○○○○
○○○○○○○○○○

Determinant

2 × 2 Matrices

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

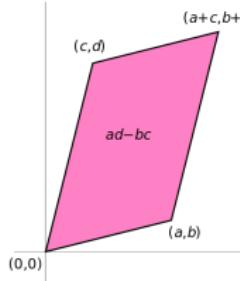
Determinant

2 × 2 Matrices

- The determinant of a 2×2 matrix is defined by

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

- The absolute value of $ad - bc$ is the area of the parallelogram with vertices at $(0,0)$, (a,b) , $(a+c,b+d)$, and (c,d) .



Linear Algebra

oooooooooooooooo
o●oooooooooooo
oooooooooooooooo

Determinant

2 × 2 Matrices

Number Theory

oooooooooooo
oooooooooooo
oooooooooooooooo
oooooooooooo
oooooooooooo
oooooooooooo

Numerical Analysis

oooooooooooo

Linear Algebra

○○○○○○○○○○○○○○○○
○●○○○○○○○○
○○○○○○○○○○○○

Determinant

2 × 2 Matrices

Number Theory

○○○○○○○○
○○○○○○○○
○○○○○○○○○○
○○○○○○○○
○○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Linear Algebra

○○○○○○○○○○○○○○
●○○○○○○○○
○○○○○○○○○○

Determinant

Number Theory

○○○○○○○
○○○○○
○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○

Numerical Analysis

○○○○○○○

2 × 2 Matrices

- Suppose $\vec{a} = (a, b)$ and $\vec{b} = (c, d)$ are two vectors defining the parallelogram.
- Then $ad - bc$ is the **oriented area** of the parallelogram, which is negative when the angle from the first to the second vector defining the parallelogram turns in a clockwise direction, and positive otherwise.

Linear Algebra

○○○○○○○○○○○○○○
●○○○○○○○○
○○○○○○○○○○

Determinant

2 × 2 Matrices

Number Theory

○○○○○○○
○○○○○
○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○

Numerical Analysis

○○○○○○○

- Suppose $\vec{a} = (a, b)$ and $\vec{b} = (c, d)$ are two vectors defining the parallelogram.
- Then $ad - bc$ is the **oriented area** of the parallelogram, which is negative when the angle from the first to the second vector defining the parallelogram turns in a clockwise direction, and positive otherwise.
- The **signed area** can be expressed as

$$\text{Signed Area} = |\vec{a}| |\vec{b}| \sin \theta$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○●○○○○○○
○○○○○○○○○○○○

Determinant

2 × 2 Matrices

Number Theory

○○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○

Linear Algebra

○○○○○○○○○○○○○○○○
○○●○○○○○○
○○○○○○○○○○○○

Determinant

2 × 2 Matrices

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Determinant

2 × 2 Matrices

- Suppose $\theta' = \frac{\pi}{2} - \theta$ is the complementary angle to θ , and $\vec{a}^\perp = (-b, a)$ is the perpendicular vector to \vec{a} .
- Hence,

$$\begin{aligned} \text{Signed Area} &= |\vec{a}| |\vec{b}| \sin \theta = |\vec{a}^\perp| |\vec{b}| \cos \theta' \\ &= \begin{pmatrix} -b \\ a \end{pmatrix} \cdot \begin{pmatrix} c \\ d \end{pmatrix} = ad - bc \end{aligned}$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○●○○○○○○
○○○○○○○○○○○○

Determinant

3 × 3 Matrices

Number Theory

○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Determinant

3 × 3 Matrices

- The determinant of a 3 × 3 matrix is defined by

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = a \begin{vmatrix} e & f \\ h & i \end{vmatrix} - b \begin{vmatrix} d & f \\ g & i \end{vmatrix} + c \begin{vmatrix} d & e \\ g & h \end{vmatrix}$$
$$= a(ei - fh) - b(di - fg) + c(dh - eg)$$
$$= aei + bfg + cdh - ceg - bdi - afh$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○●○○○○○
○○○○○○○○○○○○

Determinant

3 × 3 Matrices

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○

Numerical Analysis

○○○○○○○

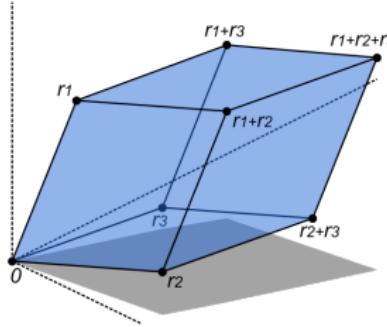
Determinant

3 × 3 Matrices

- The absolute value of the determinant of the matrix formed by the rows constructed from the vectors \vec{r}_1 , \vec{r}_2 and \vec{r}_3

$$\begin{pmatrix} r_{11} & r_{12} & r_{13} \\ r_{21} & r_{22} & r_{23} \\ r_{31} & r_{32} & r_{33} \end{pmatrix}$$

is the volume of the parallelepiped formed by \vec{r}_1 , \vec{r}_2 and \vec{r}_3 .



Linear Algebra

○○○○○○○○○○○○○○○○
○○○○●○○○○
○○○○○○○○○○○○

Determinant

$n \times n$ Matrices

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○

Determinant

$n \times n$ Matrices

- The determinant of an $n \times n$ matrix can be defined by the **Leibniz formula**.

$n \times n$ Matrices

- The determinant of an $n \times n$ matrix can be defined by the **Leibniz formula**.
- A permutation of the set $\{1, 2, \dots, n\}$ is denoted σ , and the value in the i -th position of the permutation σ is denoted σ_i .

$n \times n$ Matrices

- The determinant of an $n \times n$ matrix can be defined by the **Leibniz formula**.
- A permutation of the set $\{1, 2, \dots, n\}$ is denoted σ , and the value in the i -th position of the permutation σ is denoted σ_i .
- The set of all such permutations is denoted S_n .

$n \times n$ Matrices

- The determinant of an $n \times n$ matrix can be defined by the **Leibniz formula**.
- A permutation of the set $\{1, 2, \dots, n\}$ is denoted σ , and the value in the i -th position of the permutation σ is denoted σ_i .
- The set of all such permutations is denoted S_n .
- For each permutation σ , $s(\sigma)$ denotes the number of inversions of σ .

$n \times n$ Matrices

- The determinant of an $n \times n$ matrix can be defined by the **Leibniz formula**.
- A permutation of the set $\{1, 2, \dots, n\}$ is denoted σ , and the value in the i -th position of the permutation σ is denoted σ_i .
- The set of all such permutations is denoted S_n .
- For each permutation σ , $s(\sigma)$ denotes the number of inversions of σ .
- The Leibniz formula for the determinant of an $n \times n$ matrix A is

$$\det(A) = \sum_{\sigma \in S_n} (-1)^{s(\sigma)} \prod_{i=1}^n a_{i,\sigma_i}$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○●○○○
○○○○○○○○○○○○

Determinant

$n \times n$ Matrices

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○

Determinant

$n \times n$ Matrices

- The determinant of an $n \times n$ matrix has the following properties:
 - Swapping any pair of columns or of rows of a matrix multiplies its determinant by -1.
 - Multiplying a one column (row) by a scalar k multiplies the value of the determinant by k .
 - Adding a multiple of one column (row) to another column (row) does not change the value of the determinant.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○●○○
○○○○○○○○○○○

Determinant

$n \times n$ Matrices

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○●○○
○○○○○○○○○○

Determinant

$n \times n$ Matrices

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○

Linear Algebra

oooooooooooooooo
ooooooo●●oo
oooooooooooo

Determinant

Number Theory

oooooooo
oooooo
oooooooooooo
oooooooo
oooooooo
oooooooo

Numerical Analysis

oooooooo

$n \times n$ Matrices

- These properties are similar to the 3 types of the row operations.
- Hence, we can transform a matrix into a triangular matrix by Gaussian elimination.



$n \times n$ Matrices

- These properties are similar to the 3 types of the row operations.
- Hence, we can transform a matrix into a triangular matrix by Gaussian elimination.
- According to the definition, the determinant of a matrix in the row echelon form is the product of its entries on the main diagonal.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○●○
○○○○○○○○○○○

Determinant

Example

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○●○
○○○○○○○○○○

Determinant

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○

Numerical Analysis

○○○○○○○

Example

- For example, the determinant of

$$A = \begin{pmatrix} -2 & 2 & 3 \\ -1 & 1 & 3 \\ 2 & 0 & -1 \end{pmatrix}$$

can be computed using the following matrices:

$$B = \begin{pmatrix} -2 & 2 & \frac{3}{2} \\ 0 & 0 & \frac{9}{2} \\ 2 & 0 & -1 \end{pmatrix}, C = \begin{pmatrix} -2 & 2 & \frac{3}{2} \\ 0 & 0 & \frac{9}{2} \\ 0 & 2 & -4 \end{pmatrix}, D = \begin{pmatrix} -2 & 2 & 3 \\ 0 & 2 & -4 \\ 0 & 0 & \frac{9}{2} \end{pmatrix}$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○●○○○○○○
○○○○○○○○○○○○

Determinant

$n \times n$ Matrices

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○

Determinant

$n \times n$ Matrices

- Here, B is obtained from A by adding $-\frac{1}{2}$ times the first row to the second, so $\det(B) = \det(A)$.

Linear Algebra

oooooooooooooooooooo
oooooooooooo●
ooooooooooooooo

Determinant

Number Theory

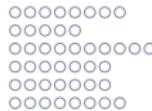
oooooooo
oooooo
oooooooooooo
oooooooooooo
oooooooooooo
oooooooooooo

Numerical Analysis

oooooooo

$n \times n$ Matrices

- Here, B is obtained from A by adding $-\frac{1}{2}$ times the first row to the second, so $\det(B) = \det(A)$.
- C is obtained from B by adding the first row to the third, so $\det(C) = \det(B)$.



Determinant

$n \times n$ Matrices

- Here, B is obtained from A by adding $-\frac{1}{2}$ times the first row to the second, so $\det(B) = \det(A)$.
- C is obtained from B by adding the first row to the third, so $\det(C) = \det(B)$.
- Finally, D is obtained from C by exchanging the second and third rows, so $\det(D) = -\det(C)$.



Determinant

$n \times n$ Matrices

- Here, B is obtained from A by adding $-\frac{1}{2}$ times the first row to the second, so $\det(B) = \det(A)$.
- C is obtained from B by adding the first row to the third, so $\det(C) = \det(B)$.
- Finally, D is obtained from C by exchanging the second and third rows, so $\det(D) = -\det(C)$.
- The determinant of the triangular matrix D is the product of its entries on the main diagonal

$$\det(D) = (-2) \cdot 2 \cdot \frac{9}{2} = -18$$

Determinant

$n \times n$ Matrices

- Here, B is obtained from A by adding $-\frac{1}{2}$ times the first row to the second, so $\det(B) = \det(A)$.
- C is obtained from B by adding the first row to the third, so $\det(C) = \det(B)$.
- Finally, D is obtained from C by exchanging the second and third rows, so $\det(D) = -\det(C)$.
- The determinant of the triangular matrix D is the product of its entries on the main diagonal

$$\det(D) = (-2) \cdot 2 \cdot \frac{9}{2} = -18$$

- Therefore, $\det(A) = -\det(D) = 18$.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
●○○○○○○○○○○

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○

Matrix Product

Matrix Product

Linear Algebra

oooooooooooooooo
oooooooooooo
●oooooooooooo

Number Theory

oooooooo
oooooo
oooooooooooo
oooooooo
oooooooo
oooooooo

Numerical Analysis

oooooooo

Matrix Product

Matrix Product

- If A is an $n \times m$ matrix and B is an $m \times p$ matrix,

$$A = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1m} \\ A_{21} & A_{22} & \cdots & A_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n2} & \cdots & A_{nm} \end{pmatrix}, B = \begin{pmatrix} B_{11} & B_{12} & \cdots & B_{1p} \\ B_{21} & B_{22} & \cdots & B_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ B_{m1} & B_{m2} & \cdots & B_{mp} \end{pmatrix}$$

the matrix product AB is defined to be an $n \times p$ matrix

$$AB = \begin{pmatrix} AB_{11} & AB_{12} & \cdots & AB_{1p} \\ AB_{21} & AB_{22} & \cdots & AB_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ AB_{n1} & AB_{n2} & \cdots & AB_{np} \end{pmatrix}$$

where $(AB)_{ij} = \sum_{k=1}^m A_{ik} B_{kj}$.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○●○○○○○○○○○○○○○○

Matrix Product

Number Theory

○○○○○○○○
○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○

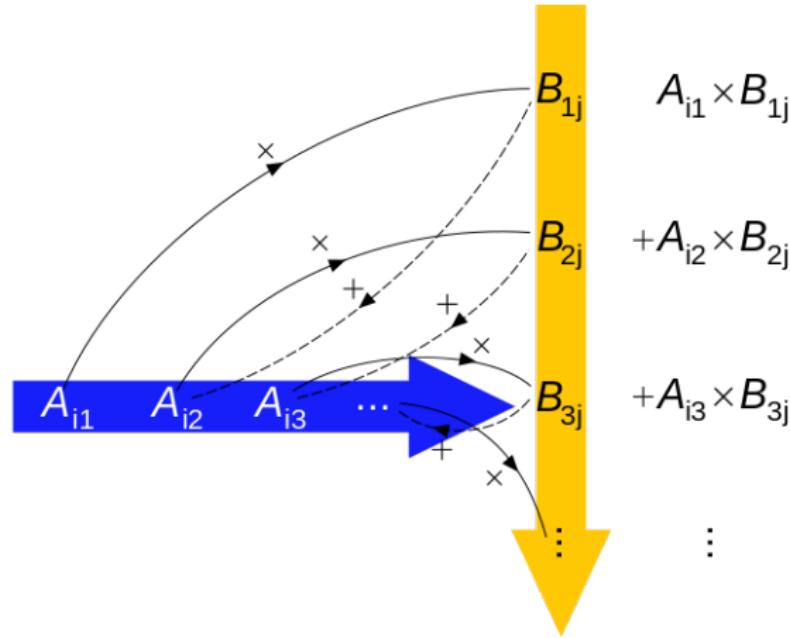
Numerical Analysis

○○○○○○○○

Illustration

Matrix Product

Illustration



Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○●○○○○○○○○○○

Matrix Product

Number Theory

○○○○○○○○
○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Illustration

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○●○○○○○○○○○○

Number Theory

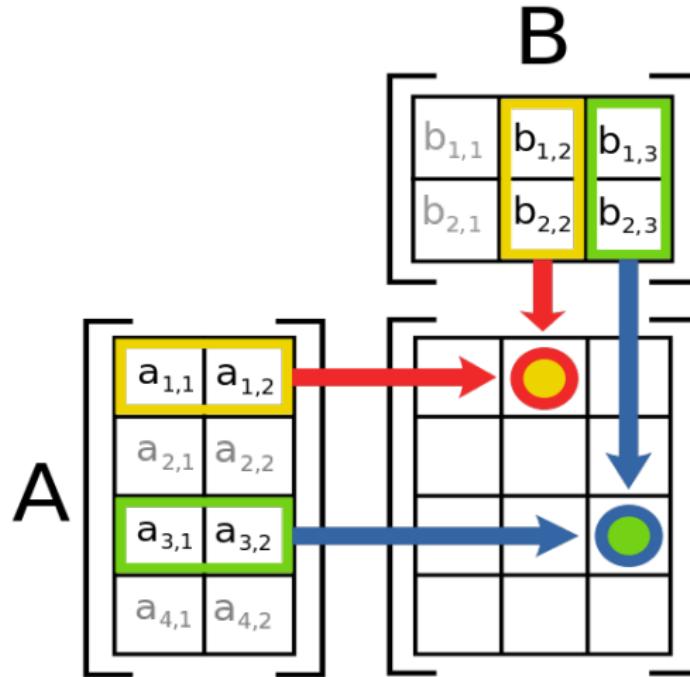
○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○

Matrix Product

Illustration



Linear Algebra

oooooooooooooooooooo
oooooooooooo
ooo●oooooooo

Matrix Product

Number Theory

oooooooo
ooooo
oooooooooooo
ooooooo
ooooooo
oooooooooooo

Numerical Analysis

ooooooo

Properties

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○●○○○○○○○○○○

Matrix Product

Number Theory

○○○○○○○○
○○○○○○○○
○○○○○○○○○○○○
○○○○○○○○
○○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Properties

- Not commutative:

$$BA \neq AB$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○
○○○●○○○○○○○○

Matrix Product

Number Theory

○○○○○○○○
○○○○○○○○
○○○○○○○○○○○○
○○○○○○○○
○○○○○○○○
○○○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Properties

- **Not** commutative:

$$BA \neq AB$$

- Distributive:

$$A(B + C) = AB + AC$$

$$(A + B)C = AC + BC$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○●○○○○○○○○

Matrix Product

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Properties

- **Not** commutative:

$$BA \neq AB$$

- Distributive:

$$A(B + C) = AB + AC$$

$$(A + B)C = AC + BC$$

- Scalar multiplication:

$$\lambda(AB) = (\lambda A)B = A(\lambda B)$$

Linear Algebra

oooooooooooooooooooo
oooooooooooo
oooo●oooooooooooo

Matrix Product

Number Theory

oooooooooooo
oooooooooooo
oooooooooooo
oooooooooooo
oooooooooooo
oooooooooooo

Numerical Analysis

oooooooooooo

Properties

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○●○○○○○○○

Matrix Product

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○

Numerical Analysis

○○○○○○○

Properties

- Associative:

$$ABC = (AB)C = A(BC)$$

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○●○○○○○○○

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○

○○○○○○○

Matrix Product

Properties

- Associative:

$$ABC = (AB)C = A(BC)$$

- Determinant:

$$\det \left(\prod_{i=1}^n A_i \right) = \prod_{i=1}^n \det(A_i)$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○●○○○○○○

Matrix Product

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○

Powers of Matrices

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○●○○○○○○○

Matrix Product

Number Theory

○○○○○○○
○○○○○○○
○○○○○○○○○○
○○○○○○○○
○○○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Powers of Matrices

- An $n \times n$ matrix A is raised to a positive integer k is defined as

$$A^k = \underbrace{AA \cdots A}_{k \text{ times}}$$

Matrix Product

Powers of Matrices

- An $n \times n$ matrix A is raised to a positive integer k is defined as

$$A^k = \underbrace{AA\cdots A}_{k \text{ times}}$$

- The zero power of A is defined as

$$A^0 = I_n = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○●○○○○○○

Matrix Product

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○

An Optimization for Recurrence

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○●○○○○○

Matrix Product

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

An Optimization for Recurrence

- The powers of matrices can be used to optimize the recurrence formula.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○●○○○○○○

Matrix Product

Number Theory

○○○○○○○
○○○○○○○
○○○○○○○○○○
○○○○○○○○
○○○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

An Optimization for Recurrence

- The powers of matrices can be used to optimize the recurrence formula.
- A k -dimensional status can be expressed as a k -dimensional row vector

$$\vec{x} = (x_1 \quad x_2 \quad \cdots \quad x_k)$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○●○○○○

Matrix Product

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○

An Optimization for Recurrence

An Optimization for Recurrence

- A **companion matrix** can be expressed a $k \times k$ matrix

$$A = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1k} \\ A_{21} & A_{22} & \cdots & A_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ A_{k1} & A_{k2} & \cdots & A_{kk} \end{pmatrix}$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○●○○○○

Matrix Product

Number Theory

○○○○○○○○
○○○○○○○○
○○○○○○○○○○○○
○○○○○○○○
○○○○○○○○
○○○○○○○○○○○○

Numerical Analysis

○○○○○○○○

An Optimization for Recurrence

oooooooooooooooooooo
oooooooooooo
oooooooo●oooo

oooooooo
oooooo
oooooooooooo
ooooooo
ooooooo
oooooooooooo

oooooooo

Matrix Product

An Optimization for Recurrence

- One transformation can be expressed as

$$\vec{x} \leftarrow \vec{x}A = (x_1 \quad x_2 \quad \cdots \quad x_k) \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1k} \\ A_{21} & A_{22} & \cdots & A_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ A_{k1} & A_{k2} & \cdots & A_{kk} \end{pmatrix}$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○●○○○

Number Theory

○○○○○○○○
○○○○○○○○
○○○○○○○○○○○○
○○○○○○○○
○○○○○○○○
○○○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Matrix Product

An optimization for Recurrence

oooooooooooooooooooo
oooooooooooo
oooooooooooo●oooo

oooooooo
oooooo
oooooooooooo
ooooooo
ooooooo
oooooooooooo

oooooooo

Matrix Product

An optimization for Recurrence

- Hence, n transformations can be expressed as

$$\vec{x} \leftarrow \vec{x}A = (x_1 \quad x_2 \quad \cdots \quad x_k) \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1k} \\ A_{21} & A_{22} & \cdots & A_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ A_{k1} & A_{k2} & \cdots & A_{kk} \end{pmatrix}^n$$

Matrix Product

An optimization for Recurrence

- Hence, n transformations can be expressed as

$$\vec{x} \leftarrow \vec{x}A = (x_1 \quad x_2 \quad \cdots \quad x_k) \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1k} \\ A_{21} & A_{22} & \cdots & A_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ A_{k1} & A_{k2} & \cdots & A_{kk} \end{pmatrix}^n$$

- Assuming that we can compute the exponentiation of matrices A^b in time $O(k^3 \log b)$ where A is a $k \times k$ matrix, the time complexity of n transformations is $O(k^3 \log n)$.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○●○○

Matrix Product

Number Theory

○○○○○○○○
○○○○○○○○
○○○○○○○○○○○○
○○○○○○○○
○○○○○○○○
○○○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Example

Matrix Product

Example

- The boundary condition of the Fibonacci sequence is

$$\begin{cases} f_1 = a \\ f_2 = b \end{cases}$$

and the recurrence formula of the Fibonacci sequence is

$$f_n = f_{n-1} + f_{n-2}$$

for $n \geq 3$.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○●○

Matrix Product

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Example

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○●○

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○

○○○○○○○

Matrix Product

Example

- Hence, the initial status is

$$\vec{x} = \begin{pmatrix} a & b \end{pmatrix}$$

and the companion matrix is

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○●

Matrix Product

Number Theory

○○○○○○○○
○○○○○○○○
○○○○○○○○○○○○
○○○○○○○○
○○○○○○○○
○○○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Example

Matrix Product

Example

- Hence, to obtain the n -th element of the Fibonacci sequence, we transform the status for $n - 1$ times and compute

$$\vec{x} A^{n-1} = \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{n-1}$$

Example

- Hence, to obtain the n -th element of the Fibonacci sequence, we transform the status for $n - 1$ times and compute

$$\vec{x} A^{n-1} = \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{n-1}$$

- Then, the first element of the obtained status is the n -th element of the Fibonacci sequence.

Linear Algebra

oooooooooooooooooooo
oooooooooooo
oooooooooooo

Number Theory

oooooooo
oooooo
oooooooooooo
ooooooo
ooooooo
oooooooo

Numerical Analysis

ooooooo

Outline

1 Linear Algebra

- Gaussian Elimination
- Determinant
- Matrix Product

2 Number Theory

- Divisibility
- Primes
- Congruence Relation
- Chinese Remainder Theorem
- Euler's Totient Function
- Modular Multiplicative Inverse

3 Numerical Analysis

- Lagrange Interpolation

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○

Divisibility

Divisibility

Number Theory

●○○○○○○○
○○○○○○○
○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Divisibility

Divisibility

- If $m > 0$ and the ratio $\frac{n}{m}$ is an integer, then we say n is divided by m .

Divisibility

Divisibility

- If $m > 0$ and the ratio $\frac{n}{m}$ is an integer, then we say n is divided by m .
- $m|n \Leftrightarrow m > 0$ and $n = mk$ for some integer k

Divisibility

Divisibility

- If $m > 0$ and the ratio $\frac{n}{m}$ is an integer, then we say n is divided by m .
- $m|n \Leftrightarrow m > 0$ and $n = mk$ for some integer k
- If n is not divided by m , then we say $m \nmid n$.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○

Divisibility

Number Theory

○●○○○○○○
○○○○○○
○○○○○○○○○○○
○○○○○○○○
○○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Greatest Common Divisor

Greatest Common Divisor

- The greatest common divisor of two integers m and n is the greatest integer divided by both m and n .

Greatest Common Divisor

- The greatest common divisor of two integers m and n is the greatest integer divided by both m and n .
-

$$\gcd(m, n) = \max\{k : k|m \text{ and } k|n\}$$

Greatest Common Divisor

- The greatest common divisor of two integers m and n is the greatest integer divided by both m and n .
-

$$\gcd(m, n) = \max\{k : k|m \text{ and } k|n\}$$

- For example, $\gcd(12, 18) = 6$.

Greatest Common Divisor

- The greatest common divisor of two integers m and n is the greatest integer divided by both m and n .
-

$$\gcd(m, n) = \max\{k : k|m \text{ and } k|n\}$$

- For example, $\gcd(12, 18) = 6$.
- If $n > 0$, then we have

$$\gcd(0, n) = n$$

since 0 is divided by any positive integer, and since n is the greatest divisor of itself.

Divisibility

Greatest Common Divisor

- The greatest common divisor of two integers m and n is the greatest integer divided by both m and n .
-

$$\gcd(m, n) = \max\{k : k|m \text{ and } k|n\}$$

- For example, $\gcd(12, 18) = 6$.
- If $n > 0$, then we have

$$\gcd(0, n) = n$$

since 0 is divided by any positive integer, and since n is the greatest divisor of itself.

- $\gcd(0, 0)$ is not defined.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○

Divisibility

Number Theory

○○●○○○○○
○○○○○○
○○○○○○○○○○
○○○○○○○○
○○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Least Common Multiple

Least Common Multiple

- Similarly,

$$\text{lcm}(m, n) = \min\{k : k > 0, m|k \text{ and } n|k\}$$

Divisibility

Least Common Multiple

- Similarly,

$$\text{lcm}(m, n) = \min\{k : k > 0, m|k \text{ and } n|k\}$$

- If $m \leq 0$ or $n \leq 0$, then $\text{lcm}(m, n)$ is not defined.

Divisibility

Least Common Multiple

- Similarly,

$$\text{lcm}(m, n) = \min\{k : k > 0, m|k \text{ and } n|k\}$$

- If $m \leq 0$ or $n \leq 0$, then $\text{lcm}(m, n)$ is not defined.
- Given $\text{gcd}(m, n)$, we have

$$\text{lcm}(m, n) = \frac{mn}{\text{gcd}(m, n)}$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○

Divisibility

Number Theory

○○○●○○○○
○○○○○○
○○○○○○○○○○
○○○○○○○○
○○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Euclidean Algorithm

Linear Algebra

oooooooooooooooooooo
oooooooooooo
oooooooooooo

Divisibility

Number Theory

oooo●oooo
oooooo
oooooooooooo
oooooooo
ooooooo
oooooooo

Numerical Analysis

ooooooo

Euclidean Algorithm

- The Euclidean algorithm is based on the recursive equation below:

Euclidean Algorithm

- The Euclidean algorithm is based on the recursive equation below:
-

$$\gcd(0, n) = n$$

$$\gcd(m, n) = \gcd(n \bmod m, m), m > 0$$

Euclidean Algorithm

- The Euclidean algorithm is based on the recursive equation below:
-

$$\gcd(0, n) = n$$

$$\gcd(m, n) = \gcd(n \bmod m, m), m > 0$$

- For example, $\gcd(12, 18) = \gcd(6, 12) = \gcd(0, 6) = 6$.

Euclidean Algorithm

- The Euclidean algorithm is based on the recursive equation below:
-

$$\gcd(0, n) = n$$

$$\gcd(m, n) = \gcd(n \bmod m, m), m > 0$$

- For example, $\gcd(12, 18) = \gcd(6, 12) = \gcd(0, 6) = 6$.
- Since $n \bmod m = n - \lfloor \frac{n}{m} \rfloor m$, then any common divisor of m and n must be a common divisor of m and $n \bmod m$.

Euclidean Algorithm

- The Euclidean algorithm is based on the recursive equation below:
-

$$\gcd(0, n) = n$$

$$\gcd(m, n) = \gcd(n \bmod m, m), m > 0$$

- For example, $\gcd(12, 18) = \gcd(6, 12) = \gcd(0, 6) = 6$.
- Since $n \bmod m = n - \lfloor \frac{n}{m} \rfloor m$, then any common divisor of m and n must be a common divisor of m and $n \bmod m$.
- The time complexity of the Euclidean algorithm is $O(\log \max\{a, b\})$.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○

Divisibility

Number Theory

○○○●○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Extended Euclidean Algorithm

Extended Euclidean Algorithm

- Extended Euclidean algorithm is used to calculate m' and n' that satisfy the equation

$$m'm + n'n = \gcd(m, n)$$

Extended Euclidean Algorithm

- Extended Euclidean algorithm is used to calculate m' and n' that satisfy the equation

$$m'm + n'n = \gcd(m, n)$$

- If $m = 0$, we have $m' = 0$ and $n' = 1$.

Extended Euclidean Algorithm

- Extended Euclidean algorithm is used to calculate m' and n' that satisfy the equation

$$m'm + n'n = \gcd(m, n)$$

- If $m = 0$, we have $m' = 0$ and $n' = 1$.
- Otherwise, let $r = n \bmod m$ and replace m and n by r and m .

Extended Euclidean Algorithm

- Extended Euclidean algorithm is used to calculate m' and n' that satisfy the equation

$$m'm + n'n = \gcd(m, n)$$

- If $m = 0$, we have $m' = 0$ and $n' = 1$.
- Otherwise, let $r = n \bmod m$ and replace m and n by r and m .
- Then, we calculate \bar{r} and \bar{m} such that

$$\bar{r}r + \bar{m}m = \gcd(r, m)$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○

Divisibility

Number Theory

○○○○●○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Extended Euclidean Algorithm

Divisibility

Extended Euclidean Algorithm

- Since $r = n - \lfloor \frac{n}{m} \rfloor m$ and $\gcd(r, m) = \gcd(m, n)$, then we have

$$\bar{r} \left(n - \lfloor \frac{n}{m} \rfloor m \right) + \bar{m}m = \gcd(m, n)$$

Divisibility

Extended Euclidean Algorithm

- Since $r = n - \lfloor \frac{n}{m} \rfloor m$ and $\gcd(r, m) = \gcd(m, n)$, then we have

$$\bar{r} \left(n - \lfloor \frac{n}{m} \rfloor m \right) + \bar{m}m = \gcd(m, n)$$

- Rewrite the equation, and we have

$$\left(\bar{m} - \lfloor \frac{n}{m} \rfloor \bar{r} \right) m + \bar{r}n = \gcd(m, n)$$

Divisibility

Extended Euclidean Algorithm

- Since $r = n - \lfloor \frac{n}{m} \rfloor m$ and $\gcd(r, m) = \gcd(m, n)$, then we have

$$\bar{r} \left(n - \lfloor \frac{n}{m} \rfloor m \right) + \bar{m}m = \gcd(m, n)$$

- Rewrite the equation, and we have

$$\left(\bar{m} - \lfloor \frac{n}{m} \rfloor \bar{r} \right) m + \bar{r}n = \gcd(m, n)$$

- Hence, $m' = \bar{m} - \lfloor \frac{n}{m} \rfloor \bar{r}$ and $n' = \bar{r}$.

Divisibility

Extended Euclidean Algorithm

- Since $r = n - \lfloor \frac{n}{m} \rfloor m$ and $\gcd(r, m) = \gcd(m, n)$, then we have

$$\bar{r} \left(n - \lfloor \frac{n}{m} \rfloor m \right) + \bar{m}m = \gcd(m, n)$$

- Rewrite the equation, and we have

$$\left(\bar{m} - \lfloor \frac{n}{m} \rfloor \bar{r} \right) m + \bar{r}n = \gcd(m, n)$$

- Hence, $m' = \bar{m} - \lfloor \frac{n}{m} \rfloor \bar{r}$ and $n' = \bar{r}$.
- For example, $m = 12$ and $n = 18$, and we have

$$6 = 0 \times 0 + 1 \times 6 = 1 \times 6 + 0 \times 12 = (-1) \times 12 + 1 \times 18.$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○

Divisibility

Number Theory

○○○○○●○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○

Numerical Analysis

○○○○○○○

Extended Euclidean Algorithm

Extended Euclidean Algorithm

- How to solve $ax + by = c$?

Extended Euclidean Algorithm

- How to solve $ax + by = c$?
- If $\gcd(a, b) \nmid c$, then the equation has no solution.

Divisibility

Extended Euclidean Algorithm

- How to solve $ax + by = c$?
- If $\gcd(a, b) \nmid c$, then the equation has no solution.
- Otherwise, supposing that (x, y) is a pair of integers such that $ax + by = \gcd(a, b)$, then

$$\left(\frac{cx}{\gcd(a, b)}, \frac{cy}{\gcd(a, b)} \right)$$

is a pair of integers that satisfies $ax + by = c$.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Divisibility

Number Theory

○○○○○●○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○

Numerical Analysis

○○○○○○○

- Supposing that (x, y) is a pair of integers such that $ax + by = c$, then

$$\left(x + \frac{bk}{\gcd(a, b)}, y - \frac{ak}{\gcd(a, b)} \right), k \in \mathbb{Z}$$

is also a pair of integers that satisfies the equation.

- Supposing that (x, y) is a pair of integers such that $ax + by = c$, then

$$\left(x + \frac{bk}{\gcd(a, b)}, y - \frac{ak}{\gcd(a, b)} \right), k \in \mathbb{Z}$$

is also a pair of integers that satisfies the equation.

- The time complexity of the extended Euclidean algorithm is $O(\log \max\{a, b\})$.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Primes

Primes

Number Theory

○○○○○○○
●○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Primes

- If a positive integer p has exactly two factors, i.e., 1 and p , then p is called a prime; otherwise, p is a composite.

Primes

- If a positive integer p has exactly two factors, i.e., 1 and p , then p is called a prime; otherwise, p is a composite.
- The first several primes are 2, 3, 5, 7, 11, 13, 17, 19, ⋯.

Primes

Primes

- If a positive integer p has exactly two factors, i.e., 1 and p , then p is called a prime; otherwise, p is a composite.
- The first several primes are 2, 3, 5, 7, 11, 13, 17, 19, \dots .
- Any positive integer n can be written as a product of primes.

Primes

Primes

- If a positive integer p has exactly two factors, i.e., 1 and p , then p is called a prime; otherwise, p is a composite.
- The first several primes are 2, 3, 5, 7, 11, 13, 17, 19, \dots .
- Any positive integer n can be written as a product of primes.
-

$$n = \prod_p p^{n_p}, n_p \geq 1$$

Primes

- If a positive integer p has exactly two factors, i.e., 1 and p , then p is called a prime; otherwise, p is a composite.
- The first several primes are 2, 3, 5, 7, 11, 13, 17, 19, ⋯.
- Any positive integer n can be written as a product of primes.



$$n = \prod_p p^{n_p}, n_p \geq 1$$

- Furthermore, the expansion equation above is unique.

Primes

- If a positive integer p has exactly two factors, i.e., 1 and p , then p is called a prime; otherwise, p is a composite.
- The first several primes are 2, 3, 5, 7, 11, 13, 17, 19, \dots .
- Any positive integer n can be written as a product of primes.

■

$$n = \prod_p p^{n_p}, n_p \geq 1$$

- Furthermore, the expansion equation above is unique.
- This proposition is called **Fundamental Theorem of Arithmetic**.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○

Primes

Number Theory

○○○○○○○
○●○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Sieve of Eratosthenes

Sieve of Eratosthenes

- The Sieve of Eratosthenes finds primes by iteratively marking the multiples of each prime as composites, starting with the multiples of 2.

Sieve of Eratosthenes

- The Sieve of Eratosthenes finds primes by iteratively marking the multiples of each prime as composites, starting with the multiples of 2.
- (1) Create a list of consecutive integers from 2 through n :
 $(2, 3, 4, \dots, n)$.

Sieve of Eratosthenes

- The Sieve of Eratosthenes finds primes by iteratively marking the multiples of each prime as composites, starting with the multiples of 2.
- (1) Create a list of consecutive integers from 2 through n :
 $(2, 3, 4, \dots, n)$.
- (2) Initially, let $p = 2$, the smallest prime number.

Sieve of Eratosthenes

- The Sieve of Eratosthenes finds primes by iteratively marking the multiples of each prime as composites, starting with the multiples of 2.
- (1) Create a list of consecutive integers from 2 through n :
 $(2, 3, 4, \dots, n)$.
- (2) Initially, let $p = 2$, the smallest prime number.
- (3) Enumerate the multiples of p by counting to n from $2p$ in increments of p , and mark them in the list.

Sieve of Eratosthenes

- The Sieve of Eratosthenes finds primes by iteratively marking the multiples of each prime as composites, starting with the multiples of 2.
- (1) Create a list of consecutive integers from 2 through n :
 $(2, 3, 4, \dots, n)$.
- (2) Initially, let $p = 2$, the smallest prime number.
- (3) Enumerate the multiples of p by counting to n from $2p$ in increments of p , and mark them in the list.
- (4) Find the first number greater than p in the list that is not marked. If there is no such number, stop; otherwise, let p equal this new number, and repeat from step (3).

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○

Primes

Number Theory

○○○○○○○
○○●○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Sieve of Eratosthenes

Sieve of Eratosthenes



$$T(n) = \sum_{i=1}^n \frac{n}{i} = n \sum_{i=1}^n \frac{1}{i}$$

Sieve of Eratosthenes



$$T(n) = \sum_{i=1}^n \frac{n}{i} = n \sum_{i=1}^n \frac{1}{i}$$

- According to the harmonic series,

$$\sum_{i=1}^n \frac{1}{i} = O(\log n)$$

Sieve of Eratosthenes



$$T(n) = \sum_{i=1}^n \frac{n}{i} = n \sum_{i=1}^n \frac{1}{i}$$

- According to the harmonic series,

$$\sum_{i=1}^n \frac{1}{i} = O(\log n)$$

- Hence,

$$T(n) = n * O(\log n) = O(n \log n)$$

i.e., the time complexity of the Sieve of Eratosthenes is $O(n \log n)$.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Primes

Linear Sieve

Number Theory

○○○○○○○○
○○○●○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Linear Sieve

- For $i \geq 2$, denote by $\ell p(i)$ the lowest prime which divides i evenly.

Linear Sieve

- For $i \geq 2$, denote by $\ell p(i)$ the lowest prime which divides i evenly.
- A non-prime x can be written uniquely as

Linear Sieve

- For $i \geq 2$, denote by $\ell p(i)$ the lowest prime which divides i evenly.
- A non-prime x can be written uniquely as
-

$$x = p^k \cdot q$$

Linear Sieve

- For $i \geq 2$, denote by $\ell p(i)$ the lowest prime which divides i evenly.
- A non-prime x can be written uniquely as
 - $$x = p^k \cdot q$$
- where (1) p is a prime, $p = \ell p(x)$;

Linear Sieve

- For $i \geq 2$, denote by $\ell p(i)$ the lowest prime which divides i evenly.
- A non-prime x can be written uniquely as
 - $$x = p^k \cdot q$$
- where (1) p is a prime, $p = \ell p(x)$;
- (2) $k \geq 1$;

Linear Sieve

- For $i \geq 2$, denote by $\ell p(i)$ the lowest prime which divides i evenly.

- A non-prime x can be written uniquely as



$$x = p^k \cdot q$$

- where (1) p is a prime, $p = \ell p(x)$;
- (2) $k \geq 1$;
- (3) $p = q$ or $p < \ell p(q)$.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Primes

Linear Sieve

Number Theory

○○○○○○○○
○○○●○○○○○○○○
○○○○○○○○○○○○
○○○○○○○○○○○○
○○○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Linear Sieve

- By the Fundamental Theorem of Arithmetic, x can be written uniquely as

$$x = \prod_{k=1}^m p_k^{n_k}$$

where $m > 1$, $p_i < p_{i+1}$ for $1 \leq i \leq m$,
and $m = 1$ implies $n_1 > 1$.

Linear Sieve

- By the Fundamental Theorem of Arithmetic, x can be written uniquely as

$$x = \prod_{k=1}^m p_k^{n_k}$$

where $m > 1$, $p_i < p_{i+1}$ for $1 \leq i \leq m$,
and $m = 1$ implies $n_1 > 1$.

- If $m = 1$, let $p = p_1$, $q = p_1$ and $k = n_1 - 1$;

Linear Sieve

- By the Fundamental Theorem of Arithmetic, x can be written uniquely as

$$x = \prod_{k=1}^m p_k^{n_k}$$

where $m > 1$, $p_i < p_{i+1}$ for $1 \leq i \leq m$,
and $m = 1$ implies $n_1 > 1$.

- If $m = 1$, let $p = p_1$, $q = p_1$ and $k = n_1 - 1$;
- if $m > 1$, let $p = p_1$, $q = \prod_{k=2}^m p_k^{n_k}$ and $k = n_1$.

Linear Sieve

- By the Fundamental Theorem of Arithmetic, x can be written uniquely as

$$x = \prod_{k=1}^m p_k^{n_k}$$

where $m > 1$, $p_i < p_{i+1}$ for $1 \leq i \leq m$,
and $m = 1$ implies $n_1 > 1$.

- If $m = 1$, let $p = p_1$, $q = p_1$ and $k = n_1 - 1$;
- if $m > 1$, let $p = p_1$, $q = \prod_{k=2}^m p_k^{n_k}$ and $k = n_1$.
- Hence, for every integer i and for every $j \leq \ell p(i)$ where j is a prime, mark the product of i and j as a composite.

Linear Sieve

- By the Fundamental Theorem of Arithmetic, x can be written uniquely as

$$x = \prod_{k=1}^m p_k^{n_k}$$

where $m > 1$, $p_i < p_{i+1}$ for $1 \leq i \leq m$,
and $m = 1$ implies $n_1 > 1$.

- If $m = 1$, let $p = p_1$, $q = p_1$ and $k = n_1 - 1$;
- if $m > 1$, let $p = p_1$, $q = \prod_{k=2}^m p_k^{n_k}$ and $k = n_1$.
- Hence, for every integer i and for every $j \leq \ell p(i)$ where j is a prime, mark the product of i and j as a composite.
- Since each composite x is only marked by $\ell p(x)$ once, then the time complexity of the linear sieve is $O(n)$.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○

Congruence Relation

Number Theory

○○○○○○○○
○○○○○○
●○○○○○○○○○○
○○○○○○○○
○○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Congruence Relation

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○

Congruence Relation

Number Theory

○○○○○○○
○○○○○
●○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○

Numerical Analysis

○○○○○○○

Congruence Relation



$$a \equiv b \pmod{m} \Leftrightarrow a \text{ mod } m = b \text{ mod } m$$

Congruence Relation



$$a \equiv b \pmod{m} \Leftrightarrow a \text{ mod } m = b \text{ mod } m$$

- For example, $9 \equiv -16 \pmod{5}$, since
 $9 \text{ mod } 5 = (-16) \text{ mod } 5$.

Congruence Relation



$$a \equiv b \pmod{m} \Leftrightarrow a \text{ mod } m = b \text{ mod } m$$

- For example, $9 \equiv -16 \pmod{5}$, since
 $9 \text{ mod } 5 = (-16) \text{ mod } 5$.
- Alternatively, $a \equiv b \pmod{m} \Leftrightarrow (a - b) \text{ is a multiple of } m$.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Congruence Relation

Number Theory

○○○○○○○○
○○○○○○
○●○○○○○○○○
○○○○○○○○
○○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Congruence Relation

Congruence Relation

- If $a \text{ mod } m = b \text{ mod } m$, then, for some integer k and l , we have

$$a - b = (a \text{ mod } m + km) - (b \text{ mod } m + lm) = (k - l)m$$

Congruence Relation

- If $a \text{ mod } m = b \text{ mod } m$, then, for some integer k and l , we have

$$a - b = (a \text{ mod } m + km) - (b \text{ mod } m + lm) = (k - l)m$$

- Conversely, given that $a - b = km$, then $a = b$ when $m = 0$; otherwise,

$$a \text{ mod } m = a - \left\lfloor \frac{a}{m} \right\rfloor m$$

$$= (b + km) - \left\lfloor \frac{b + km}{m} \right\rfloor m = b - \left\lfloor \frac{b}{m} \right\rfloor m = b \text{ mod } m$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Congruence Relation

Number Theory

○○○○○○○
○○○○○
○○●○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○

Numerical Analysis

○○○○○○○

Equivalence Relation

Equivalence Relation

- The congruence relation is an equivalence relation; i.e., for all a, b and $c \in \mathbb{Z}$:

Equivalence Relation

- The congruence relation is an equivalence relation; i.e., for all a, b and $c \in \mathbb{Z}$:
- $a \equiv a$ (Reflexivity)

Equivalence Relation

- The congruence relation is an equivalence relation; i.e., for all a, b and $c \in \mathbb{Z}$:
 - $a \equiv a$ (Reflexivity)
 - $a \equiv b \Rightarrow b \equiv a$ (Symmetry)

Equivalence Relation

- The congruence relation is an equivalence relation; i.e., for all a, b and $c \in \mathbb{Z}$:
 - $a \equiv a$ (Reflexivity)
 - $a \equiv b \Rightarrow b \equiv a$ (Symmetry)
 - $a \equiv b \equiv c \Rightarrow a \equiv c$ (Transitivity)

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○

Congruence Relation

Number Theory

○○○○○○○
○○○○○
○○●○○○○○
○○○○○○
○○○○○○
○○○○○○○

Numerical Analysis

○○○○○○○

Addition, Subtraction and Multiplication

Linear Algebra

oooooooooooooooooooo
oooooooooooo
oooooooooooo

Congruence Relation

Number Theory

oooooooooooo
oooooooooooo
oooooooooooo
oooooooooooo
oooooooooooo
oooooooooooo

Numerical Analysis

oooooooooooo

Addition, Subtraction and Multiplication

- The congruence relation is compatible with addition, subtraction and multiplication on the integers.

Addition, Subtraction and Multiplication

- The congruence relation is compatible with addition, subtraction and multiplication on the integers.
- If

$$a \equiv b \text{ and } c \equiv d \pmod{m}$$

then

$$a \pm c \equiv b \pm d \pmod{m}$$

$$ac \equiv bd \pmod{m}$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Congruence Relation

Number Theory

○○○○○○○
○○○○○
○○○●○○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Division

Division

- Note that the congruence relation is not compatible with division; i.e., if $ad \equiv bd$, we cannot assert that $a \equiv b$.

Division

- Note that the congruence relation is not compatible with division; i.e., if $ad \equiv bd \pmod{m}$, we cannot assert that $a \equiv b \pmod{m}$.
- For example, $3 \times 2 \equiv 5 \times 2 \pmod{4}$, but $3 \not\equiv 5 \pmod{4}$.

Division

- Note that the congruence relation is not compatible with division; i.e., if $ad \equiv bd \pmod{m}$, we cannot assert that $a \equiv b \pmod{m}$.
- For example, $3 \times 2 \equiv 5 \times 2 \pmod{4}$, but $3 \not\equiv 5 \pmod{4}$.
- However, if d and m are coprime, we have

$$ad \equiv bd \Leftrightarrow a \equiv b \pmod{m}, \quad a, b, d, m \in \mathbb{Z}, \quad \gcd(d, m) = 1$$

Division

- Note that the congruence relation is not compatible with division; i.e., if $ad \equiv bd \pmod{m}$, we cannot assert that $a \equiv b \pmod{m}$.
- For example, $3 \times 2 \equiv 5 \times 2 \pmod{4}$, but $3 \not\equiv 5 \pmod{4}$.
- However, if d and m are coprime, we have

$$ad \equiv bd \Leftrightarrow a \equiv b \pmod{m}, \quad a, b, d, m \in \mathbb{Z}, \quad \gcd(d, m) = 1$$

- For example, if m is not a multiple of 5, then $15 \equiv 35 \pmod{m} \Rightarrow 3 \equiv 7 \pmod{m}$.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Congruence Relation

Number Theory

○○○○○○○
○○○○○
○○○○●○○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Modular Multiplicative Inverse

Modular Multiplicative Inverse

- To prove this property, we are to find d' and m' such that $d'd + m'm = 1$.

Modular Multiplicative Inverse

- To prove this property, we are to find d' and m' such that $d'd + m'm = 1$.
- Hence, if $ad \equiv bd$, then we have $add' \equiv bdd'$.

Linear Algebra

○○○○○○○○○○○○○○
○○○○○○○○
○○○○○○○○○○

Congruence Relation

Number Theory

○○○○○○○
○○○○○
○○○○●○○○
○○○○○○
○○○○○○
○○○○○○○

Numerical Analysis

○○○○○○○

Modular Multiplicative Inverse

- To prove this property, we are to find d' and m' such that $d'd + m'm = 1$.
- Hence, if $ad \equiv bd$, then we have $add' \equiv bdd'$.
- Since $dd' \equiv 1$, then we have $add' \equiv a$ and $bdd' \equiv b$, and therefore $a \equiv b$.

Modular Multiplicative Inverse

- To prove this property, we are to find d' and m' such that $d'd + m'm = 1$.
- Hence, if $ad \equiv bd$, then we have $add' \equiv bdd'$.
- Since $dd' \equiv 1$, then we have $add' \equiv a$ and $bdd' \equiv b$, and therefore $a \equiv b$.
- When considering congruence expression regarding $(mod\ m)$, d' serves like $\frac{1}{d}$, and hence we call it "the modular inverse of a modulo m ".

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○

Congruence Relation

Number Theory

○○○○○○○
○○○○○
○○○○●○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Division

Division

- Furthermore, we have

$$ad \equiv bd \pmod{md} \Leftrightarrow a \equiv b \pmod{m}, d \neq 0$$

since $a \pmod{m} = b \pmod{m} \Leftrightarrow (a \pmod{m})d = (b \pmod{m})d \Leftrightarrow ad \pmod{md} = bd \pmod{md}$.

Division

- Furthermore, we have

$$ad \equiv bd \pmod{md} \Leftrightarrow a \equiv b \pmod{m}, d \neq 0$$

since $a \pmod{m} = b \pmod{m} \Leftrightarrow (a \pmod{m})d = (b \pmod{m})d \Leftrightarrow ad \pmod{md} = bd \pmod{md}$.

- For example, $3 \times 2 \equiv 5 \times 2 \pmod{4} \Rightarrow 3 \equiv 5 \pmod{2}$.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Congruence Relation

Number Theory

○○○○○○○
○○○○○
○○○○○●○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Division

Division

- More generally, we have

$$ad \equiv bd \pmod{m} \Leftrightarrow a \equiv b \pmod{\frac{m}{\gcd(d, m)}}$$

where $a, b, d, m \in \mathbb{Z}$.

Division

- More generally, we have

$$ad \equiv bd \pmod{m} \Leftrightarrow a \equiv b \pmod{\frac{m}{\gcd(d, m)}}$$

where $a, b, d, m \in \mathbb{Z}$.

- We can multiply $ad \equiv bd$ by d' where $d'd + m'm = \gcd(d, m)$, which gives

$$a \cdot \gcd(d, m) \equiv b \cdot \gcd(d, m) \pmod{m}$$

and divide it by $\gcd(d, m)$.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Congruence Relation

Number Theory

○○○○○○○○
○○○○○○
○○○○○○●○
○○○○○○○○
○○○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○○

Module

Module

- Moreover, we have

$$a \equiv b \pmod{md} \Rightarrow a \equiv b \pmod{m}, d \in \mathbb{Z}$$

since any multiple of md must be a multiple of m .

Module

- Moreover, we have

$$a \equiv b \pmod{md} \Rightarrow a \equiv b \pmod{m}, d \in \mathbb{Z}$$

since any multiple of md must be a multiple of m .

- Conversely,

$$a \equiv b \pmod{m} \text{ and } a \equiv b \pmod{n} \Leftrightarrow a \equiv b \pmod{\text{lcm}(m, n)}$$

where $m, n \in \mathbb{Z}, m, n > 0$,

since if $a - b$ is a common multiple of m and n , then it must be a multiple of $\text{lcm}(m, n)$.

Congruence Relation

Module

- Moreover, we have

$$a \equiv b \pmod{md} \Rightarrow a \equiv b \pmod{m}, d \in \mathbb{Z}$$

since any multiple of md must be a multiple of m .

- Conversely,

$$a \equiv b \pmod{m} \text{ and } a \equiv b \pmod{n} \Leftrightarrow a \equiv b \pmod{\text{lcm}(m, n)}$$

where $m, n \in \mathbb{Z}, m, n > 0$,

since if $a - b$ is a common multiple of m and n , then it must be a multiple of $\text{lcm}(m, n)$.

- For example, if we know that $a \equiv b \pmod{12}$ and $a \equiv b \pmod{18}$, then we have $a \equiv b \pmod{36}$.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Congruence Relation

Number Theory

○○○○○○○○
○○○○○○
○○○○○○○●
○○○○○○○○
○○○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○○

Module

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○

Congruence Relation

Number Theory

○○○○○○○○
○○○○○○○○
○○○○○○○○●
○○○○○○○○
○○○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○○

Module

- The module m can be decomposed into factors that are pairwise coprime.

Module

- The module m can be decomposed into factors that are pairwise coprime.
- If $m = \prod_p p^{m_p}$, then we have

$$a \equiv b \pmod{m} \Leftrightarrow a \equiv b \pmod{p^{m_p}}$$

for each p .

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○

Number Theory

○○○○○○○○
○○○○○○
○○○○○○○○○○
●○○○○○○
○○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Chinese Remainder Theorem

Chinese Remainder Theorem

Chinese Remainder Theorem

Chinese Remainder Theorem

- Let m_1, m_2, \dots, m_k be integers greater than 1, and

$$M = \prod_{i=1}^k m_i.$$

Chinese Remainder Theorem

Chinese Remainder Theorem

- Let m_1, m_2, \dots, m_k be integers greater than 1, and $M = \prod_{i=1}^k m_i$.
- The Chinese remainder theorem asserts that if the m_i are pairwise coprime, and if a_1, a_2, \dots, a_k are any integers, then there exist integers x such that

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

and any two such x are congruent modulo M ; i.e., there is exactly one such x in the range $0 \leq x < M$.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○●○○○○○
○○○○○○○
○○○○○○○○○

Numerical Analysis

○○○○○○○

Chinese Remainder Theorem

Solution

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○

Number Theory

○○○○○○○○
○○○○○○○○
○○○○○○○○○○○○
○●○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Chinese Remainder Theorem

Solution

- Let $M_i = \frac{M}{m_i}$ and $t_i = M_i^{-1} \pmod{m_i}$.

Chinese Remainder Theorem

Solution

- Let $M_i = \frac{M}{m_i}$ and $t_i = M_i^{-1} \pmod{m_i}$.
- Since $M_i = \frac{M}{m_i} = \frac{m_1 m_2 \cdots m_k}{m_i}$, we have

$$M_i \equiv 0 \pmod{m_j}, i \neq j$$

Chinese Remainder Theorem

Solution

- Let $M_i = \frac{M}{m_i}$ and $t_i = M_i^{-1} \pmod{m_i}$.
- Since $M_i = \frac{M}{m_i} = \frac{m_1 m_2 \cdots m_k}{m_i}$, we have

$$M_i \equiv 0 \pmod{m_j}, i \neq j$$

- Since $t_i = M_i^{-1} \pmod{m_i}$ and since M_i and m_i are coprime, we have

$$a_i t_i M_i \equiv a_i \pmod{m_i}$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○

Chinese Remainder Theorem

Number Theory

○○○○○○○○
○○○○○○○○
○○○○○○○○○○○○
○○●○○○○○
○○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Solution

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Number Theory

○○○○○○○○
○○○○○○
○○○○○○○○○○
○○●○○○○
○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Chinese Remainder Theorem

Solution

- Let $X \equiv \sum_{i=1}^k a_i t_i M_i \pmod{M}$.

Chinese Remainder Theorem

Solution

- Let $X \equiv \sum_{i=1}^k a_i t_i M_i \pmod{M}$.
- Since $m_i|M$, we have

$$X \equiv \sum_{i=1}^k a_i t_i M_i \equiv a_i \pmod{m_i}$$

for each i such that $1 \leq i \leq k$.

Chinese Remainder Theorem

Solution

- Let $X \equiv \sum_{i=1}^k a_i t_i M_i \pmod{M}$.
- Since $m_i|M$, we have

$$X \equiv \sum_{i=1}^k a_i t_i M_i \equiv a_i \pmod{m_i}$$

for each i such that $1 \leq i \leq k$.

- Hence, X is a solution to the system of congruent equations above.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○

Number Theory

○○○○○○○○
○○○○○○
○○○○○○○○○○○○
○○○●○○○○
○○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Chinese Remainder Theorem

Non-Coprime Chinese Remainder Theorem: Method 1

Chinese Remainder Theorem

Non-Coprime Chinese Remainder Theorem: Method 1

- What if the m_i are not coprime?

Chinese Remainder Theorem

Non-Coprime Chinese Remainder Theorem: Method 1

- What if the m_i are not coprime?
- Consider 2 equations:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

Chinese Remainder Theorem

Non-Coprime Chinese Remainder Theorem: Method 1

- What if the m_i are not coprime?
- Consider 2 equations:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

- Considering combining the 2 equations, we have

$$a_1 + m_1 x_1 = a_2 + m_2 x_2$$

Chinese Remainder Theorem

Non-Coprime Chinese Remainder Theorem: Method 1

- What if the m_i are not coprime?
- Consider 2 equations:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

- Considering combining the 2 equations, we have

$$a_1 + m_1 x_1 = a_2 + m_2 x_2$$

- Rearranging gives

$$m_1 x_1 - m_2 x_2 = a_2 - a_1$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○

Number Theory

○○○○○○○○
○○○○○○
○○○○○○○○○○
○○○○●○○
○○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Chinese Remainder Theorem

Non-Coprime Chinese Remainder Theorem: Method 1

Non-Coprime Chinese Remainder Theorem: Method 1

- That $\gcd(m_1, m_2) \nmid (a_2 - a_1)$ indicates that the system of congruent equations has no solution.

Chinese Remainder Theorem

Non-Coprime Chinese Remainder Theorem: Method 1

- That $\gcd(m_1, m_2) \nmid (a_2 - a_1)$ indicates that the system of congruent equations has no solution.
- Otherwise, the extended Euclidean algorithm gives the minimal positive value of x_1 and hence $x = a_1 + m_1x_1$.

Chinese Remainder Theorem

Non-Coprime Chinese Remainder Theorem: Method 1

- That $\gcd(m_1, m_2) \nmid (a_2 - a_1)$ indicates that the system of congruent equations has no solution.
- Otherwise, the extended Euclidean algorithm gives the minimal positive value of x_1 and hence $x = a_1 + m_1 x_1$.
- The result of combining the 2 equations is

$$x \bmod \text{lcm}(m_1, m_2)$$

Chinese Remainder Theorem

Non-Coprime Chinese Remainder Theorem: Method 1

- That $\gcd(m_1, m_2) \nmid (a_2 - a_1)$ indicates that the system of congruent equations has no solution.
- Otherwise, the extended Euclidean algorithm gives the minimal positive value of x_1 and hence $x = a_1 + m_1 x_1$.
- The result of combining the 2 equations is

$$x \bmod \text{lcm}(m_1, m_2)$$

- Combine 2 equations at a time, and eventually we obtain the solution to the system of congruent equations.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○

Number Theory

○○○○○○○○
○○○○○○
○○○○○○○○○○○○
○○○○●○
○○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○○○○

Chinese Remainder Theorem

Non-Coprime Chinese Remainder Theorem: Method 2

[Chinese Remainder Theorem](#)

Non-Coprime Chinese Remainder Theorem: Method 2

- For each prime factor $p|M$, find the maximum power of p in all the m_i , and set a new system of congruent equations using the maximum power of each p as moduli:

$$\begin{cases} x \equiv a'_1 \pmod{p_1^{n_1}} \\ x \equiv a'_2 \pmod{p_2^{n_2}} \\ \dots \\ x \equiv a'_{k'} \pmod{p_{k'}^{n_{k'}}} \end{cases}$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○

Chinese Remainder Theorem

Number Theory

○○○○○○○○
○○○○○○
○○○○○○○○○○
○○○○○●○
○○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○○

Non-Coprime Chinese Remainder Theorem: Method 2

Non-Coprime Chinese Remainder Theorem: Method 2

- Use the Chinese remainder theorem to solve the new system of congruent equations.

Non-Coprime Chinese Remainder Theorem: Method 2

- Use the Chinese remainder theorem to solve the new system of congruent equations.
- Since we only consider the maximum power of each prime factor p , a check on the validity of the answer over the original system of congruent equations is required.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
●○○○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Euler's Totient Function

Euler's Totient Function

Euler's Totient Function

Euler's Totient Function

- Euler's Totient Function, or Euler's Phi Function, written as $\varphi(n)$, counts the positive integers up to n that are relatively prime to n ; i.e., it is defined as the number of integer k in the range $1 \leq k \leq n$ for which $\gcd(n, k) = 1$.

Euler's Totient Function

Euler's Totient Function

- Euler's Totient Function, or Euler's Phi Function, written as $\varphi(n)$, counts the positive integers up to n that are relatively prime to n ; i.e., it is defined as the number of integer k in the range $1 \leq k \leq n$ for which $\gcd(n, k) = 1$.
- For example, $\varphi(9) = 6$, since the 6 numbers 1, 2, 4, 5, 7 and 8 are all relatively prime to 9, but the other 3 numbers in the range, 3, 6 and 9, are not, because $\gcd(9, 3) = \gcd(9, 6) = 3$ and $\gcd(9, 9) = 9$.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○●○○○○○
○○○○○○○○○

Numerical Analysis

○○○○○○○

Euler's Totient Function

Multiplicative Function

Euler's Totient Function

Multiplicative Function

- Euler's Totient Function is a multiplicative function, meaning that if m and n are relatively prime, then

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Euler's Totient Function

Multiplicative Function

- Euler's Totient Function is a multiplicative function, meaning that if m and n are relatively prime, then

$$\varphi(mn) = \varphi(m)\varphi(n)$$

- For example, $\varphi(12) = \varphi(3)\varphi(4) = 2 \times 2 = 4$.

Euler's Totient Function

Multiplicative Function

- Euler's Totient Function is a multiplicative function, meaning that if m and n are relatively prime, then

$$\varphi(mn) = \varphi(m)\varphi(n)$$

- For example, $\varphi(12) = \varphi(3)\varphi(4) = 2 \times 2 = 4$.
- Since $\varphi(n)$ is multiplicative, it can be computed along with the linear sieve.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○○
○○●○○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Euler's Totient Function

Euler's Totient Function

Euler's Totient Function

Euler's Totient Function

- If p is a prime and $k \geq 1$, then

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1) = p^k \left(1 - \frac{1}{p}\right)$$

Euler's Totient Function

Euler's Totient Function

- If p is a prime and $k \geq 1$, then

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1) = p^k \left(1 - \frac{1}{p}\right)$$

- Since p is a prime, the only possible values of $\gcd(p^k, m)$ are $1, p, p^2, \dots, p^k$, and the only way for $\gcd(p^k, m)$ to not equal 1 is for m to be a multiple of p , i.e.,
 $p, 2p, 3p, \dots, p^{k-1}p = p^k$.

Euler's Totient Function

Euler's Totient Function

- If p is a prime and $k \geq 1$, then

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1) = p^k \left(1 - \frac{1}{p}\right)$$

- Since p is a prime, the only possible values of $\gcd(p^k, m)$ are $1, p, p^2, \dots, p^k$, and the only way for $\gcd(p^k, m)$ to not equal 1 is for m to be a multiple of p , i.e.,
 $p, 2p, 3p, \dots, p^{k-1}p = p^k$.
- Hence, the other $(p^k - p^{k-1})$ numbers are all relatively prime to p^k .

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○●○○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Euler's Totient Function

Euler's Product Formula

Euler's Totient Function

Euler's Product Formula

- The fundamental theorem of arithmetic states that if $n > 1$, there is a unique expression of n ,

$$n = \prod_{k=1}^m p_k^{n_k}$$

where $p_1 < p_2 < \dots < p_m$ are prime numbers and each $n_i \geq 1$.

Euler's Totient Function

Euler's Product Formula

- The fundamental theorem of arithmetic states that if $n > 1$, there is a unique expression of n ,

$$n = \prod_{k=1}^m p_k^{n_k}$$

where $p_1 < p_2 < \dots < p_m$ are prime numbers and each $n_i \geq 1$.

- The multiplicative property gives

$$\varphi(n) = \varphi(p_1^{n_1}) \varphi(p_2^{n_2}) \cdots \varphi(p_m^{n_m})$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○●○○
○○○○○○○○

Numerical Analysis

○○○○○○○

Euler's Totient Function

Euler's Product Formula

Euler's Totient Function

Euler's Product Formula

- The formula for $\varphi(p^k)$ gives

$$\varphi(n) = p_1^{n_1} \left(1 - \frac{1}{p_1}\right) p_2^{n_2} \left(1 - \frac{1}{p_2}\right) \cdots p_m^{n_m} \left(1 - \frac{1}{p_m}\right)$$

Euler's Totient Function

Euler's Product Formula

- The formula for $\varphi(p^k)$ gives

$$\varphi(n) = p_1^{n_1} \left(1 - \frac{1}{p_1}\right) p_2^{n_2} \left(1 - \frac{1}{p_2}\right) \cdots p_m^{n_m} \left(1 - \frac{1}{p_m}\right)$$

- Rearranging gives

$$\varphi(n) = p_1^{n_1} p_2^{n_2} \cdots p_m^{n_m} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right)$$

Euler's Totient Function

Euler's Product Formula

- The formula for $\varphi(p^k)$ gives

$$\varphi(n) = p_1^{n_1} \left(1 - \frac{1}{p_1}\right) p_2^{n_2} \left(1 - \frac{1}{p_2}\right) \cdots p_m^{n_m} \left(1 - \frac{1}{p_m}\right)$$

- Rearranging gives

$$\varphi(n) = p_1^{n_1} p_2^{n_2} \cdots p_m^{n_m} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right)$$

- That is,

$$\varphi(n) = n \prod_{k=1}^m \left(1 - \frac{1}{p_k}\right)$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○●○
○○○○○○○○

Numerical Analysis

○○○○○○○

Euler's Totient Function

Euler's Product Formula

Euler's Totient Function

Euler's Product Formula

- For example,

$$\varphi(36) = \varphi(2^23^2) = 36 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 36 \cdot \frac{1}{2} \cdot \frac{2}{3} = 12.$$

Euler's Totient Function

Euler's Product Formula

- For example,
$$\varphi(36) = \varphi(2^23^2) = 36 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 36 \cdot \frac{1}{2} \cdot \frac{2}{3} = 12.$$
- Indeed, there are 12 positive integers coprime with 36 and lower than 36: 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35.

Linear Algebra

oooooooooooooooooooo
oooooooooooo
oooooooooooo

Euler's Totient Function

Number Theory

oooooooooooo
oooooooooooo
oooooooooooo
oooooooooooo
oooooooo●
oooooooooooo

Numerical Analysis

oooooooooooo

Euler's Theorem

Euler's Totient Function

Euler's Theorem

- If a and n are relatively prime, then

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Euler's Totient Function

Euler's Theorem

- If a and n are relatively prime, then

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

- The special case where n is prime is known as **Fermat's Little Theorem**:

$$a^p \equiv a \pmod{p}, p \text{ is prime}$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
●○○○○○○○

Numerical Analysis

○○○○○○○

Modular Multiplicative Inverse

Modular Multiplicative Inverse

Modular Multiplicative Inverse

Modular Multiplicative Inverse

- In modular arithmetic, the modular multiplicative inverse of an integer a modulo m is an integer x such that

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

Modular Multiplicative Inverse

Modular Multiplicative Inverse

- In modular arithmetic, the modular multiplicative inverse of an integer a modulo m is an integer x such that

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

- The modular multiplicative inverse of a modulo m exists iff. a and m are coprime, i.e., iff. $\gcd(a, m) = 1$.

Modular Multiplicative Inverse

Modular Multiplicative Inverse

- In modular arithmetic, the modular multiplicative inverse of an integer a modulo m is an integer x such that

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

- The modular multiplicative inverse of a modulo m exists iff. a and m are coprime, i.e., iff. $\gcd(a, m) = 1$.
- If the modular multiplicative inverse of a modulo m exists, the operation of division by a modulo m can be defined as multiplying by the inverse of a , i.e., a^{-1} .

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Modular Multiplicative Inverse

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○○
○○○○○○○
○●○○○○○○

Numerical Analysis

○○○○○○○

Example

Modular Multiplicative Inverse

Example

- Suppose we wish to find the modular multiplicative inverse of 3 modulo 11.

Modular Multiplicative Inverse

Example

- Suppose we wish to find the modular multiplicative inverse of 3 modulo 11.
-

$$x \equiv 3^{-1} \pmod{11}$$

Example

- Suppose we wish to find the modular multiplicative inverse of 3 modulo 11.



$$x \equiv 3^{-1} \pmod{11}$$

- This is the same as find x such that

$$3x \equiv 1 \pmod{11}$$

Modular Multiplicative Inverse

Example

- Suppose we wish to find the modular multiplicative inverse of 3 modulo 11.
-

$$x \equiv 3^{-1} \pmod{11}$$

- This is the same as find x such that

$$3x \equiv 1 \pmod{11}$$

- Working in \mathbb{Z}_{11} we find that $3 \cdot 4 = 12 \equiv 1 \pmod{11}$, and there are no other values of x in \mathbb{Z}_{11} that also satisfy the congruence.

Modular Multiplicative Inverse

Example

- Suppose we wish to find the modular multiplicative inverse of 3 modulo 11.
-

$$x \equiv 3^{-1} \pmod{11}$$

- This is the same as find x such that

$$3x \equiv 1 \pmod{11}$$

- Working in \mathbb{Z}_{11} we find that $3 \cdot 4 = 12 \equiv 1 \pmod{11}$, and there are no other values of x in \mathbb{Z}_{11} that also satisfy the congruence.
- Hence, the modular multiplicative inverse of 3 modulo 11 is 4.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○○
○○○○○○○
○○●○○○○○

Numerical Analysis

○○○○○○○

Modular Multiplicative Inverse

Extended Euclidean Algorithm

Extended Euclidean Algorithm

- The modular multiplicative inverse is the solution to

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

Modular Multiplicative Inverse

Extended Euclidean Algorithm

- The modular multiplicative inverse is the solution to

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

- That is,

$$ax - 1 = qm$$

Modular Multiplicative Inverse

Extended Euclidean Algorithm

- The modular multiplicative inverse is the solution to

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

- That is,

$$ax - 1 = qm$$



$$ax - qm = 1$$

Modular Multiplicative Inverse

Extended Euclidean Algorithm

- The modular multiplicative inverse is the solution to

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

- That is,

$$ax - 1 = qm$$



$$ax - qm = 1$$

- This is the exact form that the extended Euclidean algorithm solves, assuming that $\gcd(a, m) = 1$.

Modular Multiplicative Inverse

Extended Euclidean Algorithm

- The modular multiplicative inverse is the solution to

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

- That is,

$$ax - 1 = qm$$



$$ax - qm = 1$$

- This is the exact form that the extended Euclidean algorithm solves, assuming that $\gcd(a, m) = 1$.
- The algorithm runs in time $O(\log m)$.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Modular Multiplicative Inverse

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○●○○○○

Numerical Analysis

○○○○○○○

Euler's Theorem

Modular Multiplicative Inverse

Euler's Theorem

- According to Euler's theorem, if a is coprime to m , i.e., $\gcd(a, m) = 1$, then

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

where $\varphi(m)$ is Euler's totient function.

Modular Multiplicative Inverse

Euler's Theorem

- According to Euler's theorem, if a is coprime to m , i.e., $\gcd(a, m) = 1$, then

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

where $\varphi(m)$ is Euler's totient function.

- Hence, the modular multiplicative inverse can be found directly:

$$a^{\varphi(m)-1} \equiv a^{-1} \pmod{m}$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Modular Multiplicative Inverse

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○●○○○

Numerical Analysis

○○○○○○○

Euler's Theorem

Modular Multiplicative Inverse

Euler's Theorem

- When m is a prime, the modular inverse is given by

$$a^{-1} \equiv a^{m-2} \pmod{m}$$

Modular Multiplicative Inverse

Euler's Theorem

- When m is a prime, the modular inverse is given by

$$a^{-1} \equiv a^{m-2} \pmod{m}$$

- Assuming that the value $\varphi(m)$ is known and that we can compute the exponentiation a^b in time $O(\log b)$, the time complexity of calculating the modular inverse is $O(\log m)$.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○

Modular Multiplicative Inverse

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○
○○○○○○
○○○○○●○○

Numerical Analysis

○○○○○○○

Inverse of Factorials

Modular Multiplicative Inverse

Inverse of Factorials

- According to the definition of the modular multiplicative inverse, we have

$$(n!)^{-1} \equiv \frac{1}{n!} \equiv \frac{n+1}{(n+1)!}$$

Modular Multiplicative Inverse

Inverse of Factorials

- According to the definition of the modular multiplicative inverse, we have

$$(n!)^{-1} \equiv \frac{1}{n!} \equiv \frac{n+1}{(n+1)!}$$

- Hence, given $((n+1)!)^{-1}$, we can compute $(n!)^{-1}$ by

$$(n!)^{-1} \equiv (n+1)((n+1))^{-1}$$

Modular Multiplicative Inverse

Inverse of Factorials

- According to the definition of the modular multiplicative inverse, we have

$$(n!)^{-1} \equiv \frac{1}{n!} \equiv \frac{n+1}{(n+1)!}$$

- Hence, given $((n+1)!)^{-1}$, we can compute $(n!)^{-1}$ by

$$(n!)^{-1} \equiv (n+1)((n+1))^{-1}$$

- Therefore, we can compute $(i!)^{-1}$ for each i in the range $0 \leq i \leq n$ in time $O(n)$.

Linear Algebra

oooooooooooooooooooo
oooooooooooo
oooooooooooo

Modular Multiplicative Inverse

Number Theory

oooooooooooo
oooooooooooo
oooooooooooo
oooooooooooo
oooooooooooo
oooooooooooo
oooooooooooo●○

Numerical Analysis

oooooooooooo

Inverse of 1 through n

Modular Multiplicative Inverse

Inverse of 1 through n

- Suppose that $a = \lfloor \frac{y}{x} \rfloor$ and $b = y \bmod x$ where y is prime and $1 < x < y$.

Modular Multiplicative Inverse

Inverse of 1 through n

- Suppose that $a = \lfloor \frac{y}{x} \rfloor$ and $b = y \bmod x$ where y is prime and $1 < x < y$.
- Hence, we have

$$ax + b \equiv 0 \pmod{y}$$

Modular Multiplicative Inverse

Inverse of 1 through n

- Suppose that $a = \lfloor \frac{y}{x} \rfloor$ and $b = y \bmod x$ where y is prime and $1 < x < y$.
- Hence, we have

$$ax + b \equiv 0 \pmod{y}$$

- Multiply the equation by $x^{-1}b^{-1}$, and we have

$$ab^{-1} + x^{-1} \equiv 0 \pmod{y}$$

and hence

$$x^{-1} \equiv -ab^{-1} \pmod{y}$$

Linear Algebra

oooooooooooooooooooo
oooooooooooo
oooooooooooo

Modular Multiplicative Inverse

Number Theory

oooooooooooo
oooooooooooo
oooooooooooo
oooooooooooo
oooooooooooo
oooooooooooo
oooooooooooo●

Numerical Analysis

oooooooooooo

Inverse of 1 through n

Modular Multiplicative Inverse

Inverse of 1 through n

- Replace a and b by $\lfloor \frac{y}{x} \rfloor$ and $y \bmod x$ respectively, and we have

$$x^{-1} \equiv -\lfloor \frac{y}{x} \rfloor \cdot (y \bmod x)^{-1} \pmod{y}$$

Inverse of 1 through n

- Replace a and b by $\lfloor \frac{y}{x} \rfloor$ and $y \bmod x$ respectively, and we have

$$x^{-1} \equiv -\lfloor \frac{y}{x} \rfloor \cdot (y \bmod x)^{-1} \pmod{y}$$

- Given 1^{-1} through $(x-1)^{-1}$, we can compute x^{-1} in time $O(1)$.

Inverse of 1 through n

- Replace a and b by $\lfloor \frac{y}{x} \rfloor$ and $y \bmod x$ respectively, and we have

$$x^{-1} \equiv -\lfloor \frac{y}{x} \rfloor \cdot (y \bmod x)^{-1} \pmod{y}$$

- Given 1^{-1} through $(x-1)^{-1}$, we can compute x^{-1} in time $O(1)$.
- Therefore, we can compute 1^{-1} through n^{-1} in time $O(n)$.

Linear Algebra

oooooooooooooooooooo
oooooooooooo
oooooooooooo

Number Theory

oooooooo
oooooo
oooooooooooo
ooooooo
ooooooo
oooooooooooo

Numerical Analysis

oooooooo

Outline

1 Linear Algebra

- Gaussian Elimination
- Determinant
- Matrix Product

2 Number Theory

- Divisibility
- Primes
- Congruence Relation
- Chinese Remainder Theorem
- Euler's Totient Function
- Modular Multiplicative Inverse

3 Numerical Analysis

- Lagrange Interpolation

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Lagrange Interpolation

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○
○○○○○○
○○○○○○○○

Numerical Analysis

●○○○○○○○

Polynomial Interpolation

Polynomial Interpolation

- Given a set of $n + 1$ data points (x_i, y_i) , where no two x_i are the same, the polynomial interpolation problem is to find a polynomial p of degree at most n such that

$$p(x_i) = y_i, i = 0, 1, \dots, n$$

Polynomial Interpolation

- Given a set of $n + 1$ data points (x_i, y_i) , where no two x_i are the same, the polynomial interpolation problem is to find a polynomial p of degree at most n such that

$$p(x_i) = y_i, i = 0, 1, \dots, n$$

- It can be proved that such a polynomial p exists and is unique.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Lagrange Interpolation

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○○

Numerical Analysis

○●○○○○○

Lagrange Interpolation

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○

Numerical Analysis

○●○○○○○

Lagrange Interpolation

Lagrange Interpolation

- The **interpolation polynomial in the Lagrange form** is a linear combination

$$L(x) = \sum_{j=0}^n y_j l_j(x)$$

Lagrange Interpolation

Lagrange Interpolation

- The **interpolation polynomial in the Lagrange form** is a linear combination

$$L(x) = \sum_{j=0}^n y_j l_j(x)$$

- The **Lagrange basis polynomials** are

$$\begin{aligned} l_j(x) &= \prod_{\substack{0 \leq m \leq n \\ m \neq j}} \frac{x - x_m}{x_j - x_m} \\ &= \frac{(x - x_0)}{(x_j - x_0)} \cdots \frac{(x - x_{j-1})}{(x_j - x_{j-1})} \frac{(x - x_{j+1})}{(x_j - x_{j+1})} \cdots \frac{(x - x_n)}{(x_j - x_n)} \end{aligned}$$

where $0 \leq j \leq n$.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Lagrange Interpolation

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○●○○○○○

Lagrange Interpolation

Lagrange Interpolation

Lagrange Interpolation

- For all $i \neq j$, $l_j(x)$ includes the term $(x - x_i)$ in the numerator, so the whole product will be 0 at $x = x_i$:

$$\begin{aligned} l_{j \neq i}(x_i) &= \prod_{m \neq j} \frac{x_i - x_m}{x_j - x_m} \\ &= \frac{(x_i - x_0)}{(x_j - x_0)} \cdots \frac{(x_i - x_i)}{(x_j - x_i)} \cdots \frac{(x_i - x_n)}{(x_j - x_n)} = 0 \end{aligned}$$

Lagrange Interpolation

Lagrange Interpolation

- For all $i \neq j$, $l_j(x)$ includes the term $(x - x_i)$ in the numerator, so the whole product will be 0 at $x = x_i$:

$$\begin{aligned} l_{j \neq i}(x_i) &= \prod_{m \neq j} \frac{x_i - x_m}{x_j - x_m} \\ &= \frac{(x_i - x_0)}{(x_j - x_0)} \cdots \frac{(x_i - x_i)}{(x_j - x_i)} \cdots \frac{(x_i - x_n)}{(x_j - x_n)} = 0 \end{aligned}$$

- On the other hand,

$$l_i(x_i) = \prod_{m \neq i} \frac{x_i - x_m}{x_i - x_m} = 1$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Lagrange Interpolation

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○●○○○○

Lagrange Interpolation

Lagrange Interpolation

Lagrange Interpolation

- It follows that

$$\begin{cases} y_i l_i(x_i) = y_i \\ y_j l_j(x_i) = 0, j \neq i \end{cases}$$

Lagrange Interpolation

Lagrange Interpolation

- It follows that

$$\begin{cases} y_i l_i(x_i) = y_i \\ y_j l_j(x_i) = 0, j \neq i \end{cases}$$

- Hence, at each point x_i ,

$$L(x_i) = y_i + 0 + 0 + \cdots + 0 = y_i$$

showing that L interpolates the function exactly.

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Lagrange Interpolation

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○●○○○

Example 1

Lagrange Interpolation

Example 1

- We wish to interpolate $f(x) = x^2$ over the range $1 \leq x \leq 3$, given these three points:

$$x_0 = 1 \quad f(x_0) = 1$$

$$x_1 = 2 \quad f(x_1) = 4$$

$$x_2 = 3 \quad f(x_2) = 9$$

Lagrange Interpolation

Example 1

- We wish to interpolate $f(x) = x^2$ over the range $1 \leq x \leq 3$, given these three points:

$$x_0 = 1 \quad f(x_0) = 1$$

$$x_1 = 2 \quad f(x_1) = 4$$

$$x_2 = 3 \quad f(x_2) = 9$$

- The interpolating polynomial is

$$\begin{aligned} L(x) &= 1 \cdot \frac{x - 2}{1 - 2} \cdot \frac{x - 3}{1 - 3} + 4 \cdot \frac{x - 1}{2 - 1} \cdot \frac{x - 3}{2 - 3} + 9 \cdot \frac{x - 1}{3 - 1} \cdot \frac{x - 2}{3 - 2} \\ &= x^2 \end{aligned}$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Lagrange Interpolation

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○●○○

Example 2

Lagrange Interpolation

Example 2

- We wish to interpolate $f(x) = x^3$ over the range $1 \leq x \leq 3$, given these three points:

$$x_0 = 1 \quad f(x_0) = 1$$

$$x_1 = 2 \quad f(x_1) = 8$$

$$x_2 = 3 \quad f(x_2) = 27$$

Lagrange Interpolation

Example 2

- We wish to interpolate $f(x) = x^3$ over the range $1 \leq x \leq 3$, given these three points:

$$x_0 = 1 \quad f(x_0) = 1$$

$$x_1 = 2 \quad f(x_1) = 8$$

$$x_2 = 3 \quad f(x_2) = 27$$

- The interpolating polynomial is

$$\begin{aligned} L(x) &= 1 \cdot \frac{x - 2}{1 - 2} \cdot \frac{x - 3}{1 - 3} + 8 \cdot \frac{x - 1}{2 - 1} \cdot \frac{x - 3}{2 - 3} + 27 \cdot \frac{x - 1}{3 - 1} \cdot \frac{x - 2}{3 - 2} \\ &= 6x^2 - 11x + 6 \end{aligned}$$

Linear Algebra

○○○○○○○○○○○○○○○○
○○○○○○○○○○
○○○○○○○○○○○○

Number Theory

○○○○○○○
○○○○○
○○○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○○○○

Numerical Analysis

○○○○○●○

Lagrange Interpolation

Time Complexity and a Special Case

Linear Algebra

oooooooooooooooooooo
oooooooooooo
oooooooooooo

Number Theory

oooooooo
oooooo
oooooooooooo
ooooooo
ooooooo
ooooooo

Numerical Analysis

ooooooo●○

Lagrange Interpolation

Time Complexity and a Special Case

- The Lagrange Interpolation runs in time $O(n^2)$.

Lagrange Interpolation

Time Complexity and a Special Case

- The Lagrange Interpolation runs in time $O(n^2)$.
- Given that the polynomial interpolation problem is computed in the residue system modulo p , where p is prime, and that $x_i = i$, the original Lagrange polynomial

$$L(x) = \sum_{j=0}^n y_j l_j(x) = \sum_{j=0}^n y_j \prod_{m \neq j} \frac{x - x_m}{x_j - x_m}$$

can be converted to

$$L(x) = \sum_{j=0}^n y_j \prod_{m \neq j} \frac{x - m}{j - m}$$

Linear Algebra

oooooooooooooooooooo
oooooooooooo
oooooooooooo

Number Theory

oooooooo
oooooo
oooooooooooo
ooooooo
ooooooo
oooooooooooo

Numerical Analysis

ooooooo●

Lagrange Interpolation

Time Complexity and a Special Case

Lagrange Interpolation

Time Complexity and a Special Case

- Rewrite the expression above, and we have

$$L(x) = \sum_{j=0}^n y_j \frac{\prod_{i=x-k}^{x-j-1} i \prod_{i=x-j+1}^x i}{(-1)^{n-j} j! (n-j)!}$$

Lagrange Interpolation

Time Complexity and a Special Case

- Rewrite the expression above, and we have

$$L(x) = \sum_{j=0}^n y_j \frac{\prod_{i=x-k}^{x-j-1} i \prod_{i=x-j+1}^x i}{(-1)^{n-j} j! (n-j)!}$$

- Assuming that we have preprocessed prefix products, suffix products, factorials and modular multiplicative inverses, the Lagrange interpolation can run in time $O(n)$.

Linear Algebra

oooooooooooooooooooo
oooooooooooo
oooooooooooo

Number Theory

oooooooo
oooooo
oooooooooooo
ooooooo
ooooooo
oooooooooooo

Numerical Analysis

ooooooo

Thank you!