MATH1172 Vector Calculus and Number Theory

A Review of Topics in Pure Mathematics[1]

Kayvan Nejabati Zenouz[2]

University of Greenwich

April 27, 2020

"Thus it is left to the reader to put it all together by himself, if he so pleases, but nothing is done for a reader's comfort"

Stages on Life's Way, Søren Kierkegaard 1813 - 1855

[1] Use these notes in conjunction with R demos accessible on https://kayvannejabati.shinyapps.io/MATH1172Demo/.

[2] Office: QM315, Email: K.NejabatiZenouz@greenwich.ac.uk,
Student Drop-in Hours: MONDAYS 12:00-13:00 (MATHS ARCADE) AND TUESDAYS 15:00-16:00 (QM315)

Contents

1. Introduction
   - Module Aims and Assessment
   - Topics to be Covered
   - Reading List and References
2. Topic 1: Vector Algebra and Real-Valued Functions
   - Introduction
   - Vectors Algebra
   - Euclidean Space
   - Dot and Cross Products
   - Real-Valued Functions
3. Topic 2: Differentiation, Gradient, Divergence, Curl
   - Continuity of Multivariate Functions
   - Differentiation of Multivariate Functions
   - Gradient of a Scalar field
   - Divergence of a Vector Field
   - Curl of a Vector Field
   - Mixed Partial Derivative and Laplacian
4. Topic 3: Line, Surface, and Volume Integrals
   - Line Integrals
   - Surface Integrals
   - Volume Integrals
5. Topic 4: Integrals Theorems and Applications
   - Gauss's (Divergence) Theorem
   - Stokes' Theorem
6. Topic 1: Integers and Divisibility
   - Methods of Number Theory
   - Well-Ordering Principle and Archimedes Property
   - Polygonal Numbers
   - The Division Algorithm
   - Greatest Common Divisor
   - The Euclidean Algorithm
   - The Diophantine Equation $ax + by = c$
7. Topic 2: Primes and Their Distribution
   - Prime Numbers
   - Fundamental Theorem of Arithmetic
   - Distribution of Primes
   - Goldbach's Conjecture
   - Primes in Arithmetic Progression
8. Topic 3: The Theory of Congruences
   - Basic Properties of Congruences
   - Cancellation Rule
   - Representations of Integers
   - Linear Congruences
   - Chinese Remainder Theorem
9. Topic 4: Fermat's, Wilson's Theorems, and Number Theoretic Functions
   - Fermat's Little Theorem and Pseudoprimes
   - Wilson's Theorem
   - Number Theoretic Functions
   - Applications to RSA Cryptosystem

Lecture Contents

1. Introduction
   - Module Aims and Assessment
   - Topics to be Covered
   - Reading List and References
2. Topic 1: Vector Algebra and Real-Valued Functions
   - Introduction
   - Vectors Algebra
   - Euclidean Space
   - Dot and Cross Products
   - Real-Valued Functions
3. Topic 2: Differentiation, Gradient, Divergence, Curl
   - Continuity of Multivariate Functions
   - Differentiation of Multivariate Functions
   - Gradient of a Scalar field
   - Divergence of a Vector Field
   - Curl of a Vector Field
   - Mixed Partial Derivative and Laplacian
4. Topic 3: Line, Surface, and Volume Integrals
   - Line Integrals
   - Surface Integrals
   - Volume Integrals
5. Topic 4: Integrals Theorems and Applications
   - Gauss's (Divergence) Theorem
   - Stokes' Theorem
6. Topic 1: Integers and Divisibility
   - Methods of Number Theory
   - Well-Ordering Principle and Archimedes Property
   - Polygonal Numbers
   - The Division Algorithm
   - Greatest Common Divisor
   - The Euclidean Algorithm
   - The Diophantine Equation $ax + by = c$
7. Topic 2: Primes and Their Distribution
   - Prime Numbers
   - Fundamental Theorem of Arithmetic
   - Distribution of Primes
   - Goldbach's Conjecture
   - Primes in Arithmetic Progression
8. Topic 3: The Theory of Congruences
   - Basic Properties of Congruences
   - Cancellation Rule
   - Representations of Integers
   - Linear Congruences
   - Chinese Remainder Theorem
9. Topic 4: Fermat's, Wilson's Theorems, and Number Theoretic Functions
   - Fermat's Little Theorem and Pseudoprimes
   - Wilson's Theorem
   - Number Theoretic Functions
   - Applications to RSA Cryptosystem

Aims

Main aim of this module is to develop an understanding of vector calculus in science and engineering as well classical techniques and results in number theory. In particular, by the end of this part you will be able to...

1. Understand and manipulate real-valued functions.
2. Evaluate multiple integrals including line, surface, and volume integrals.
3. Apply concepts of vector calculus to study problems in applied mathematics and theoretical physics.
4. Learn the properties of integers and primes numbers.
5. Analysis congruences and understand key theorems relating to properties of natural numbers.
6. Know about number theoretic functions and apply your knowledge to learn about cryptosystems.

Topics to be Covered...

Vector Calculus:

1. Vector Algebra and Real-Valued Functions
2. Differentiation, Gradient, Divergence, Curl
3. Line, Surface, and Volume Integrals
4. Integral Theorems and Applications

Number Theory:

1. Integers and Divisibility
2. Primes and Their Distributions
3. The Theory of Congruences
4. Fermat's, Wilson's Theorems, and Number Theoretic Functions

Assessment

Assessment

- Vector Calculus Assignment, weight 50%, due 19/03/2020.
- Closed Book Examination, weight 50%, May 2020.

Guidance for Success

- Attend Lectures,
- Engage with Tutorials,
- Ask Questions, Read Books,
- Use Online Resources (Google, YouTube, etc...),
- Keep Your Work Organised,
- Always Ask for Help.

Useful Software

You may consider using the packages offered by **GeoGebra** www.geogebra.org for graphics and geometric manipulations.

Reading List and References

For reading list see Matthews (2012); Company (2012); Burton (2011); Kraft and Washington (2018).

Burton, D.
2011. *Elementary Number Theory*. Mcgraw-Hill.

Company, W.
2012. *Vector Calculus, 6th Ed, Marsden & Tromba, 2012: Vector Calculus*, Vector Calculus. Bukupedia.

Kraft, J. and L. Washington
2018. *An Introduction to Number Theory with Cryptography*, Textbooks in Mathematics. CRC Press.

Matthews, P.
2012. *Vector Calculus*, Springer Undergraduate Mathematics Series. Springer London.

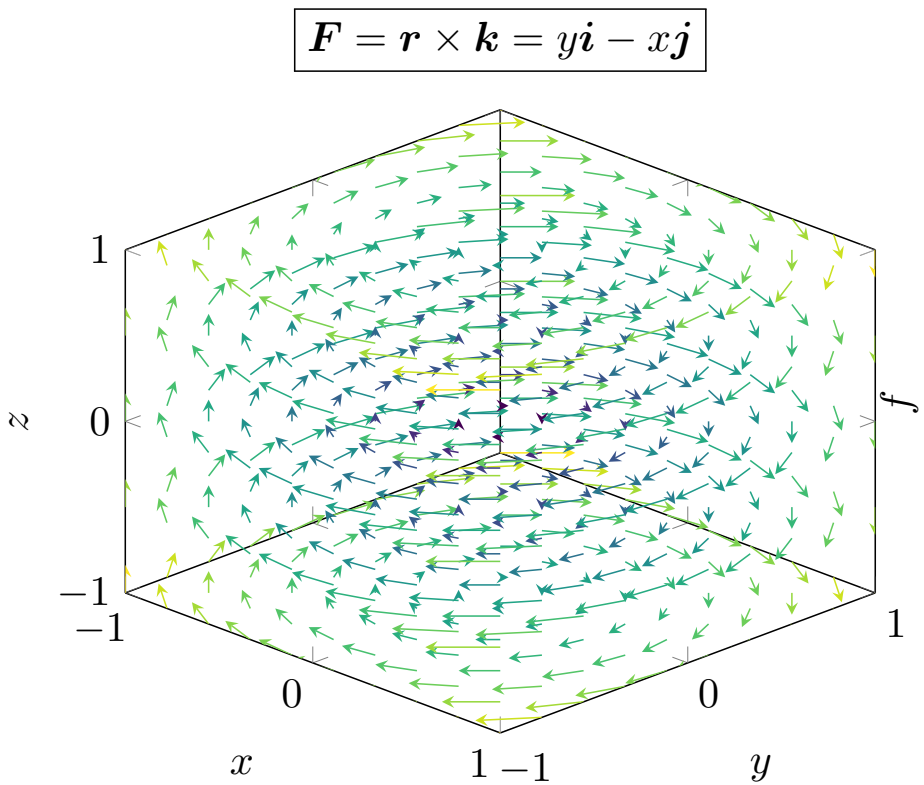
Class Activity with www.menti.com

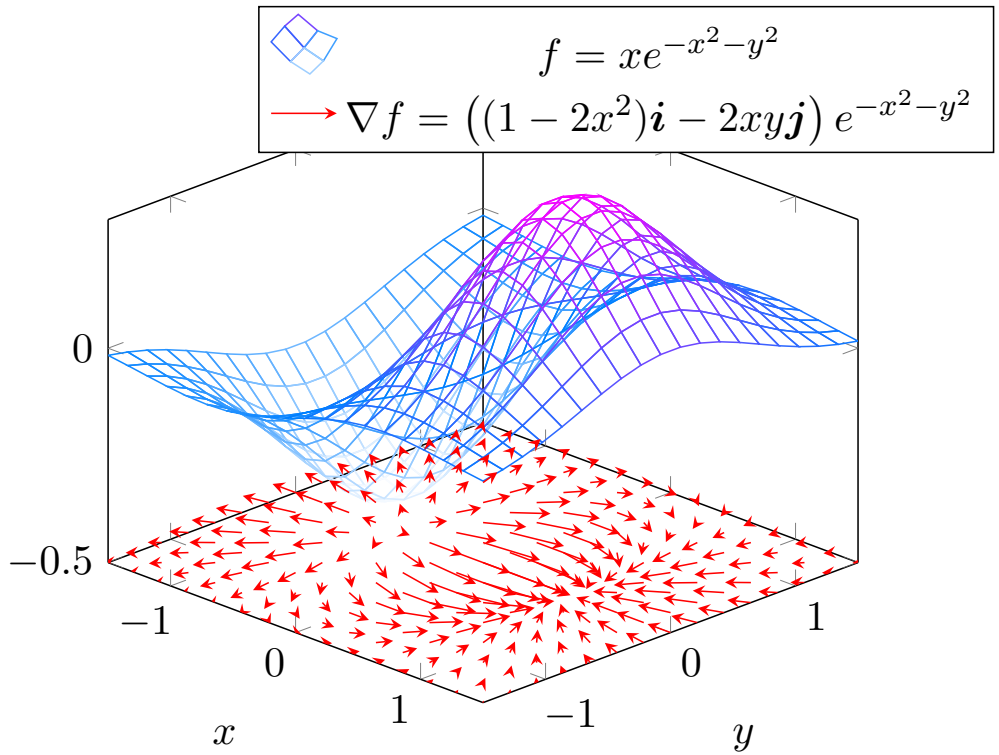
Please **scan** the barcode with your **phone** in order to take part in the class activity.

https://www.menti.com/hdk487qe1b

Alternatively, go to www.menti.com on your electronic devices and enter the access code **86 18 89**.

Topic 1
Vector Algebra and Real-Valued Functions





Lecture Contents

1. Introduction
   - Module Aims and Assessment
   - Topics to be Covered
   - Reading List and References
2. Topic 1: Vector Algebra and Real-Valued Functions
   - Introduction
   - Vectors Algebra
   - Euclidean Space
   - Dot and Cross Products
   - Real-Valued Functions
3. Topic 2: Differentiation, Gradient, Divergence, Curl
   - Continuity of Multivariate Functions
   - Differentiation of Multivariate Functions
   - Gradient of a Scalar field
   - Divergence of a Vector Field
   - Curl of a Vector Field
   - Mixed Partial Derivative and Laplacian
4. Topic 3: Line, Surface, and Volume Integrals
   - Line Integrals
   - Surface Integrals
   - Volume Integrals
5. Topic 4: Integrals Theorems and Applications
   - Gauss's (Divergence) Theorem
   - Stokes' Theorem
6. Topic 1: Integers and Divisibility
   - Methods of Number Theory
   - Well-Ordering Principle and Archimedes Property
   - Polygonal Numbers
   - The Division Algorithm
   - Greatest Common Divisor
   - The Euclidean Algorithm
   - The Diophantine Equation $ax + by = c$
7. Topic 2: Primes and Their Distribution
   - Prime Numbers
   - Fundamental Theorem of Arithmetic
   - Distribution of Primes
   - Goldbach's Conjecture
   - Primes in Arithmetic Progression
8. Topic 3: The Theory of Congruences
   - Basic Properties of Congruences
   - Cancellation Rule
   - Representations of Integers
   - Linear Congruences
   - Chinese Remainder Theorem
9. Topic 4: Fermat's, Wilson's Theorems, and Number Theoretic Functions
   - Fermat's Little Theorem and Pseudoprimes
   - Wilson's Theorem
   - Number Theoretic Functions
   - Applications to RSA Cryptosystem

Intended Learning Outcomes

By the end of this session you will be able to...

1. Understand the main objectives in studying vector calculus.
2. Review the basics of vectors, vector spaces, linear maps.
3. Calculate dot and cross products of vectors.
4. Find length of vectors and angles between two vectors.
5. Learn about real-valued functions and produce graphs and level sets of functions.

Vector calculus

Properties and partial **differentiation** of scalar and vector **quantities** in two or three dimensions.

It studies

- **Scalar functions** of position and time the form $f(\boldsymbol{x}, t)$; e.g.,

$$f(\boldsymbol{x}, t) = f(x, y, z, t) = x^2 + y^2 + z^2 - t.$$

- **Vector functions** of position and time $\boldsymbol{u}(\boldsymbol{x}, t)$; e.g.,

$$\boldsymbol{u}(\boldsymbol{x}, t) = (u_1(\boldsymbol{x}, t), u_2(\boldsymbol{x}, t), u_3(\boldsymbol{x}, t)) .$$

Applications

It is the **fundamental** language of mathematical **physics** and used in topics such as **Heat Transfer**, **Fluid Mechanics**, **Electromagnetism**, **Relativity**, and **Quantum Mechanics**.

History

- **Plato 429 B.C.**

  Explain the motion of the heavenly bodies by some geometrical theory.

  World is rational and can be rationally understood. It has mathematical design.

- **Euclid 300 B.C.** in 11 volumes of *Elements* **geometry** is born.
- **Muhammad ibn Musa al-Khwarizmi 800 A.D** in *The Compendious Book on Calculation by Completion and Balancing* **algebra** is born.
- **René Descartes 1637** in *La Géométrie* invented coordinate system, **analytic geometry** born.
- **Johannes Kepler** calculated planetary orbits.
- **Vectors** were conceptualised by **Newton 1687**, and formalised by **Hamilton**.
- **Calculus** was invented by **Newton** and **Leibniz**.

Applications of Vector Calculus: Governing Equations

Heat Transfer

For solid with temperature $T(\boldsymbol{x}, t)$, thermal conductivity K, density ρ, time t, and c specific heat we have

$$c\rho\frac{\partial T}{\partial t} = \nabla \cdot (K\nabla T)\,.$$

Fluid Mechanics

For flow velocity $\boldsymbol{u}(\boldsymbol{x}, t)$, density ρ, pressure P, time t, fluid viscosity μ, and $\boldsymbol{g}$ gravity we have

$$\rho\left(\frac{\partial \boldsymbol{u}}{\partial t} + \boldsymbol{u}\cdot\nabla\boldsymbol{u}\right) = \rho\boldsymbol{g} - \nabla P + \mu\nabla^2\boldsymbol{u}, \text{ and } \nabla\cdot\boldsymbol{u} = 0.$$

Electromagnetism

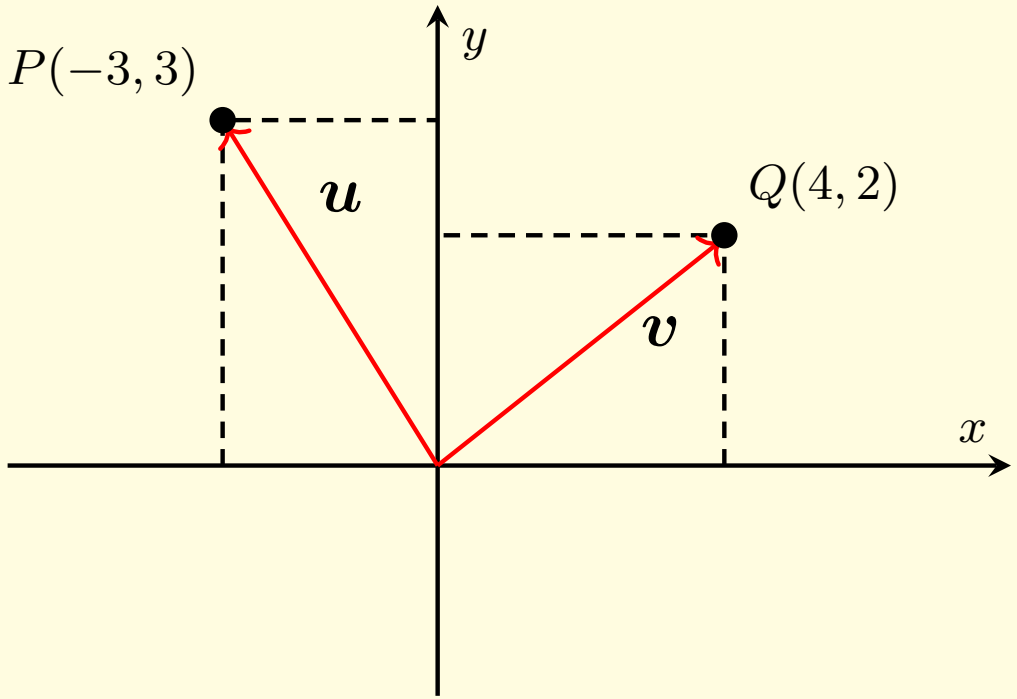
For the electric field $\boldsymbol{E}(\boldsymbol{x}, t)$, magnetic field $\boldsymbol{B}(\boldsymbol{x}, t)$, charge density ρ, current density $\boldsymbol{J}$, constants ϵ_0, μ_0 we have

$$\nabla\cdot\boldsymbol{E} = \frac{\rho}{\epsilon_0},\ \nabla\cdot\boldsymbol{B} = 0,\ \nabla\times\boldsymbol{E} = -\frac{\partial \boldsymbol{B}}{\partial t},\ \nabla\times\boldsymbol{B} = \mu_0\left(\boldsymbol{J} + \epsilon_0\frac{\partial \boldsymbol{E}}{\partial t}\right).$$

We review concepts relating to vectors.

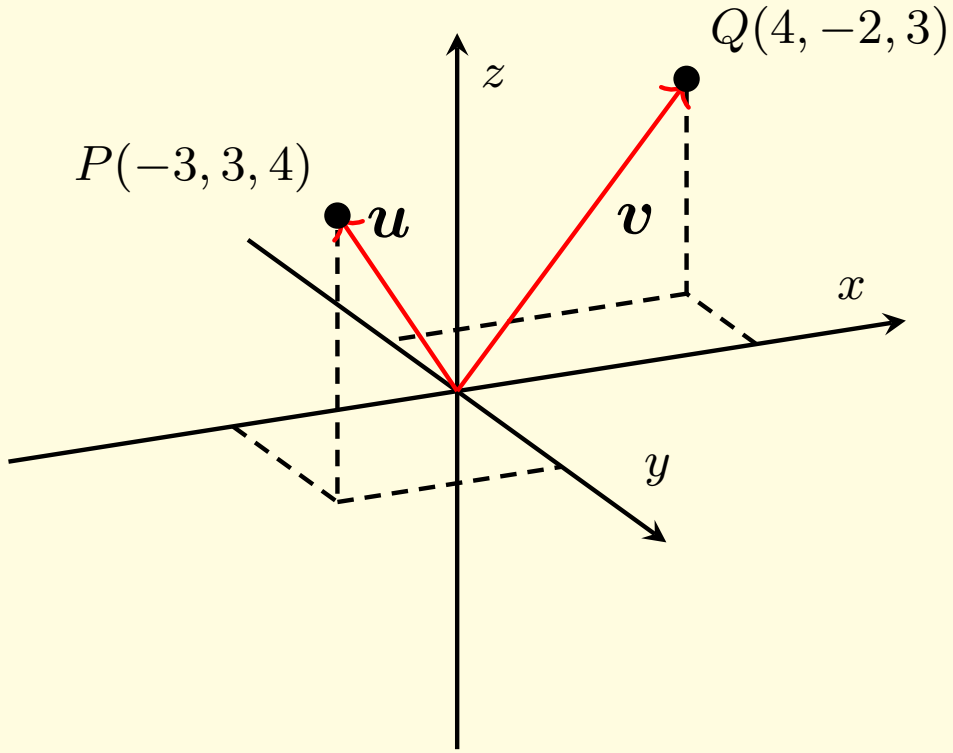
What is a vector?

Think about the 2-dimensional space $\mathbb{R}^2$



What is a vector?

Think about the 3-dimensional space $\mathbb{R}^3$



Geometry: Intuition

- Many physical quantities, such as mass, temperature, pressure, and speed, possess only **magnitude**, they are called **scalars**.
- **Vectors** have **magnitude** and **direction**. For example, velocity, force, and electric field.
- Vectors are represented by tuples, for example,

$$\boldsymbol{u} = \begin{pmatrix} -3 \\ 2 \\ 4 \end{pmatrix}, \ \boldsymbol{v} = \begin{pmatrix} 4 \\ -2 \\ 3 \end{pmatrix}.$$

- We denote vectors by bold letters $\boldsymbol{u}$ or $\underline{u}$.

Vector Addition

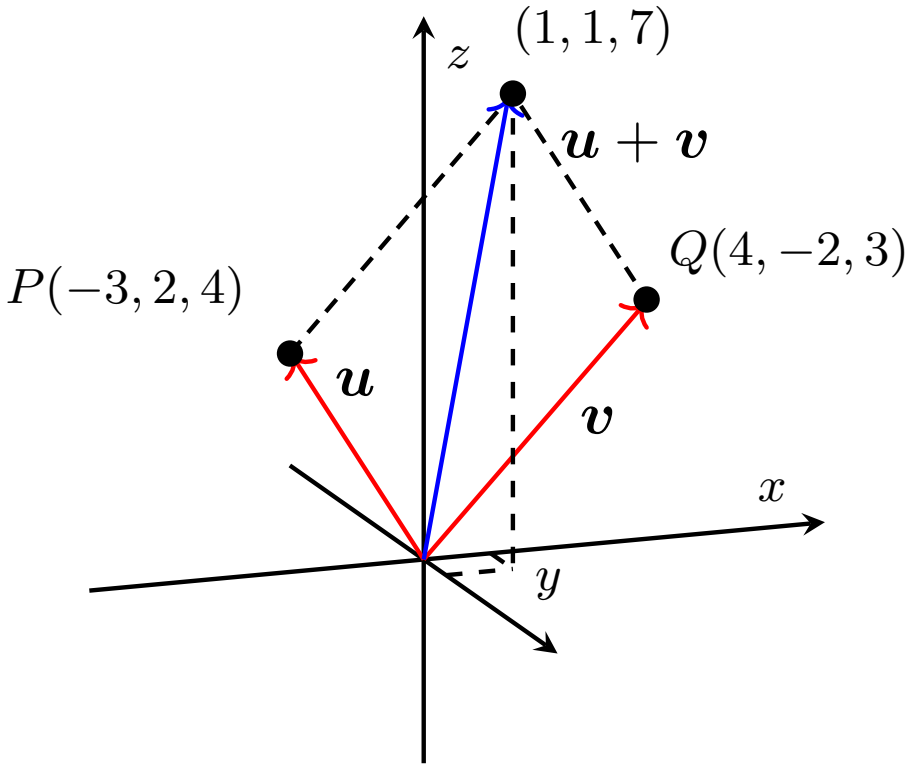
Algebraically the result of adding two vectors is **component-wise addition**. For example,

if

$$\boldsymbol{a} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}, \quad \boldsymbol{b} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix},$$

then

$$\boldsymbol{a} + \boldsymbol{b} = \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ a_3 + b_3 \end{pmatrix}.$$



Geometrically the result of adding two vectors is obtained by the **parallelogram law**.

Scalar Multiplication

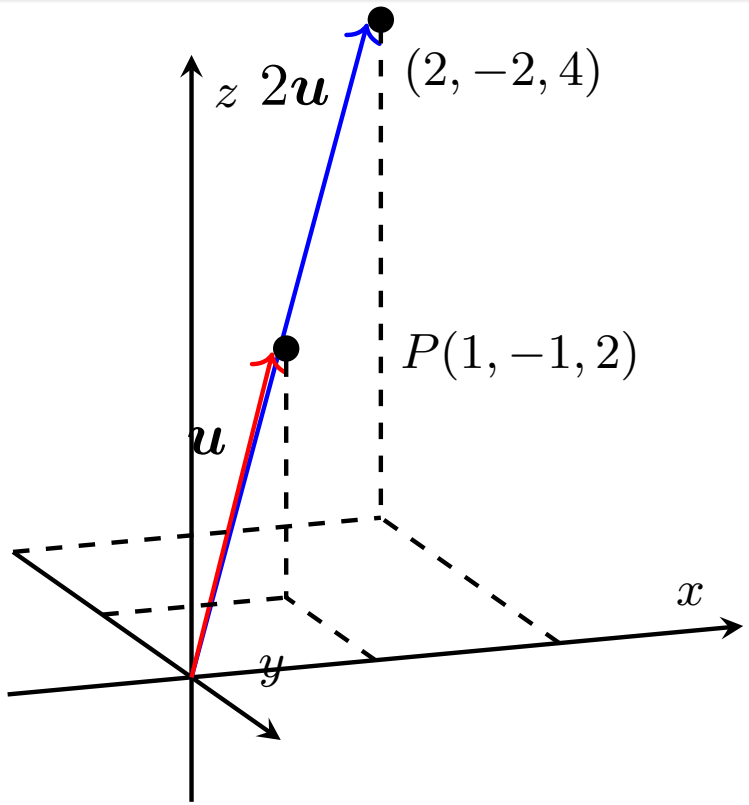
Algebraically the result of multiplying a vector by a scalar λ is **component-wise**. For example,

if

$$\boldsymbol{a} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix},$$

then

$$\lambda\boldsymbol{a} = \begin{pmatrix} \lambda a_1 \\ \lambda a_2 \\ \lambda a_3 \end{pmatrix}.$$



Geometrically the result of adding two vectors is obtained by **scaling the vector**, changing direction if $\lambda < 0$.

Example $\mathbb{R}^n$

The n-dimensional Real Euclidean Space

For a natural number n let $\mathcal{V} = \mathbb{R}^n$ with addition and scalar multiplication

$$(u_1, u_2, ..., u_n) + (v_1, v_2, ..., v_n) = (u_1 + v_1, u_2 + v_2, ..., u_n + v_n)$$
$$\lambda(u_1, u_2, ..., u_n) = (\lambda u_1, \lambda u_2, ..., \lambda u_n),$$
$$\mathbf{0} = (0, 0, ..., 0).$$

In such case for $\boldsymbol{u} = (u_1, u_2, ..., u_n)$ the vector $\widetilde{\boldsymbol{u}}$ such that $\boldsymbol{u} + \widetilde{\boldsymbol{u}} = \mathbf{0}$ is give by

$$-\boldsymbol{u} = (-u_1, -u_2, ..., -u_n).$$

Remark 1:

In **this course** we will be concerned with $\mathbb{R}^n$ particularly for $n = 2, 3$ i.e., $\mathbb{R}^2$ and $\mathbb{R}^3$.

Exercise 1:

Let $\boldsymbol{u} = (2, 4, -5, 1)$ and $\boldsymbol{v} = (1, 2, 3, 4)$. Find

$$\boldsymbol{u} + \boldsymbol{v},\ 3\boldsymbol{v},\ -\boldsymbol{v},\ 2\boldsymbol{u} - 3\boldsymbol{v}.$$

Properties of Vectors in $\mathbb{R}^n$

Vectors is $\mathbb{R}^n$ form a set $\mathcal{V}$, with elements $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}, ...$, together with addition $+$ and a scalar multiplication so that

$$\boldsymbol{u} + \boldsymbol{v} \in \mathcal{V} \text{ and } \lambda \boldsymbol{u} \in \mathcal{V} \text{ for all } \boldsymbol{u}, \boldsymbol{v} \in \mathcal{V}, \ \lambda \in \mathbb{R}.$$

In addition, for any $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in \mathcal{V}$ and $\lambda, \mu \in \mathbb{R}$ the following **axioms** are satisfied.

Group Axioms	1.	$\boldsymbol{u} + \boldsymbol{v} = \boldsymbol{v} + \boldsymbol{u}$
	2.	$(\boldsymbol{u} + \boldsymbol{v}) + \boldsymbol{w} = \boldsymbol{u} + (\boldsymbol{v} + \boldsymbol{w})$
	3.	There exists $\mathbf{0} \in \mathcal{V}$ such that $\boldsymbol{u} + \mathbf{0} = \boldsymbol{u}$
	4.	There exists $\widetilde{\boldsymbol{u}} \in \mathcal{V}$ such that $\boldsymbol{u} + \widetilde{\boldsymbol{u}} = \mathbf{0}$
		$\widetilde{\boldsymbol{u}}$ is denoted by $-\boldsymbol{u}$
Scalar Axioms	5.	$\lambda(\boldsymbol{u} + \boldsymbol{v}) = \lambda \boldsymbol{u} + \lambda \boldsymbol{v}$
	6.	$(\lambda + \mu)\boldsymbol{u} = \lambda \boldsymbol{u} + \mu \boldsymbol{u}$
	7.	$\lambda(\mu \boldsymbol{u}) = (\lambda \mu)\boldsymbol{u}$
	8.	$1\boldsymbol{u} = \boldsymbol{u}$

In particular, we call $\mathcal{V}$ a **vector space** over $\mathbb{R}$.

Standard Basic Vectors in $\mathbb{R}^3$

The **standard unite** vectors $\boldsymbol{i} = (1, 0, 0)$, $\boldsymbol{j} = (0, 1, 0)$, $\boldsymbol{k} = (0, 0, 1)$ are sometimes used to write vectors in $\mathbb{R}^3$, so if $\boldsymbol{a} = (a_1, a_2, a_3)$, then we can also write

$$\boldsymbol{a} = a_1\boldsymbol{i} + a_2\boldsymbol{j} + a_3\boldsymbol{k}.$$

Exercise 2: Vector Spaces

1. Two vectors $u = (u_1, u_2, ..., u_n)$ and $v = (v_1, v_2, ..., v_n)$ are **equal** if $u_i = v_i$ for every $i = 1, ..., n$. Find x, y, z so that
$$(x - y, x + z, z - 1) = (1, 2, 3).$$

2. **Function Spaces**. Let X be a set and $\mathrm{M}(X, \mathbb{R})$ the set of all functions $f : X \longrightarrow \mathbb{R}$ with addition and scalar multiplication
$$(f + g)(x) = f(x) + g(x)$$
$$(\lambda f)(x) = \lambda f(x).$$

Show $\mathrm{M}(X, \mathbb{R})$ satisfies the 8 axioms on slide 22.

Remark 2: Maps Between Vector Spaces

Give two vector spaces $\mathcal{U}$ and $\mathcal{V}$ a **linear map**, or a homomorphism, between $\mathcal{U}$ and $\mathcal{V}$ is a **function**

$$\begin{aligned} A : \mathcal{U} &\longrightarrow \mathcal{V} \\ u &\longmapsto Au \end{aligned}$$

which **respects** the vector addition and scalar multiplications, so

$$A(u+v) = Au + Av \text{ and } A(\lambda u) = \lambda Au.$$

For example, all 3×3 matrices

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

are linear maps from $\mathbb{R}^3$ to $\mathbb{R}^3$.

Vectors Joining Points

If you have two points $P = (x_1, ..., x_n)$ and $Q = (y_1, ..., y_n)$, the vector starting from P to Q has components

$$\overrightarrow{PQ} = (y_1 - x_1, ..., y_n - x_n).$$

For example, the vector joining $P = (0, 0, 0)$ and $Q = (1, 1, 1)$ is

$$\overrightarrow{PQ} = \boldsymbol{i} + \boldsymbol{j} + \boldsymbol{k}.$$

Equation of a Line

The parametric equation of a line through the tip of a vector $\boldsymbol{a}$ and in the direction of $\boldsymbol{v}$ is

$$\boldsymbol{l}(t) = \boldsymbol{a} + \boldsymbol{v}t.$$

Example

The line through the tip of $\boldsymbol{j} + 2\boldsymbol{k}$ in the direction of $2\boldsymbol{i} + 4\boldsymbol{k}$ is

$$\boldsymbol{l}(t) = 3t\boldsymbol{i} + \boldsymbol{j} + (2 + 4t)\,\boldsymbol{k}.$$

Alternatively, the **algebraic equation** for the line is given by the intersection fo the two plan

$$y = 1 \text{ and } \frac{x}{3} = \frac{z-2}{4}.$$

Equation of a Plane

Two nonparallel vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ span a plane

$$\boldsymbol{v}(s,t) = s\boldsymbol{a} + t\boldsymbol{b}.$$

Exercise 3: Planes

Find parametric and algebraic equation of the plane spanned by $\boldsymbol{i}$ and $\boldsymbol{j}$.

Dot Product

Definition (Inner or Dot Product)

Given two vectors $\boldsymbol{a} = (a_1, ..., a_n)$ and $\boldsymbol{b} = (b_1, ..., b_n)$ the dot product of $\boldsymbol{a}$ and $\boldsymbol{b}$ is given by

$$\boldsymbol{a} \cdot \boldsymbol{b} = \sum_{i=1}^{n} a_i b_i = a_1 b_1 + \cdots + a_n b_n.$$

Example

The dot product of $\boldsymbol{a} = 3\boldsymbol{i} + 2\boldsymbol{j} - \boldsymbol{k}$ and $\boldsymbol{b} = \boldsymbol{i} - \boldsymbol{j} - \boldsymbol{k}$ is

$$\boldsymbol{a} \cdot \boldsymbol{b} = 3 \times 1 - 2 \times 1 + 1 \times 1 = 2.$$

Exercise 4: Dot Product

Find the following dot products.

$$\boldsymbol{i} \cdot \boldsymbol{i},\ \boldsymbol{j} \cdot \boldsymbol{j},\ \boldsymbol{k} \cdot \boldsymbol{k},\ \boldsymbol{i} \cdot \boldsymbol{j},\ \boldsymbol{j} \cdot \boldsymbol{k},\ \boldsymbol{i} \cdot (a_1 \boldsymbol{i} + a_2 \boldsymbol{j} + a_3 \boldsymbol{k}).$$

Remark 3: Properties of Dot Product

Given vectors $\boldsymbol{a}$, $\boldsymbol{b}$, and $\boldsymbol{c}$, in $\mathbb{R}^n$ and real numbers α and β, then following holds.

1. $\boldsymbol{a} \cdot \boldsymbol{a} \geq 0$; and $\boldsymbol{a} \cdot \boldsymbol{a} = 0$ if and only if $\boldsymbol{a} = \boldsymbol{0}$.
2. $(\alpha \boldsymbol{a}) \cdot \boldsymbol{b} = \alpha\,(\boldsymbol{a} \cdot \boldsymbol{b})$ and $\boldsymbol{a} \cdot (\beta \boldsymbol{b}) = \beta\,(\boldsymbol{a} \cdot \boldsymbol{b})$.
3. $\boldsymbol{a} \cdot (\boldsymbol{b} + \boldsymbol{c}) = \boldsymbol{a} \cdot \boldsymbol{b} + \boldsymbol{a} \cdot \boldsymbol{c}$ and $(\boldsymbol{a} + \boldsymbol{b}) \cdot \boldsymbol{c} = \boldsymbol{a} \cdot \boldsymbol{c} + \boldsymbol{b} \cdot \boldsymbol{c}$
4. $\boldsymbol{a} \cdot \boldsymbol{b} = \boldsymbol{b} \cdot \boldsymbol{a}$

Exercise 5: Properties

Construct a proof for each of the properties above.

Length of a Vector and Unit Vectors

Definition (Length of a Vector)

The **norm** of a vector $\boldsymbol{a}$ denoted by $\|\boldsymbol{a}\|$ is given by

$$\|\boldsymbol{a}\| = \sqrt{\boldsymbol{a} \cdot \boldsymbol{a}},$$

so if $\boldsymbol{a} = a_1\boldsymbol{i} + a_2\boldsymbol{j} + a_3\boldsymbol{k}$, then we have

$$\|\boldsymbol{a}\| = \sqrt{a_1^2 + a_2^2 + a_3^2}.$$

It follows from Pythagorean Theorem that the norm of $\boldsymbol{a}$ coincides with the length of $\boldsymbol{a}$.

Exercise 6: Unit Vectors

Prove that for a vector $\boldsymbol{a}$, the vector

$$\widehat{\boldsymbol{a}} = \frac{\boldsymbol{a}}{\|\boldsymbol{a}\|}$$

has length 1, it is called the **normalised** vector.

Distance Between Points

Let $\boldsymbol{a}$ and $\boldsymbol{b}$ be vectors with tips P and Q respectively, then the distance between P and Q is

$$\left\|\overrightarrow{PQ}\right\| = \|\boldsymbol{b} - \boldsymbol{a}\|.$$

Theorem (Angles Between Vectors)

Let $\boldsymbol{a}$ and $\boldsymbol{b}$ be vectors in $\mathbb{R}^3$ and let $0 \leq \theta \leq \pi$ be the angle between them. Then we have

$$\boldsymbol{a} \cdot \boldsymbol{b} = \|\boldsymbol{a}\| \, \|\boldsymbol{b}\| \cos\theta.$$

Proof.

Exercise. Hint: use the cosine rule from trigonometry. □

Example

Let $\boldsymbol{a} = \boldsymbol{i} + \boldsymbol{j}$ and $\boldsymbol{b} = 2\boldsymbol{j}$, then we have

$$\boldsymbol{a} \cdot \boldsymbol{b} = 2,\ \boldsymbol{a} \cdot \boldsymbol{a} = 2,\ \boldsymbol{b} \cdot \boldsymbol{b} = 4,\ \text{so}$$
$$2 = \sqrt{2} \times \sqrt{4} \cos\theta$$

which implies that

$$\cos\theta = \frac{\sqrt{2}}{2},\ \text{so}\ \theta = \frac{\pi}{4}.$$

Corollary (Cauchy-Schwartz Inequality)

Let $\boldsymbol{a}$ and $\boldsymbol{b}$ be vectors in $\mathbb{R}^3$. Then we have

$$|\boldsymbol{a} \cdot \boldsymbol{b}| \leq \|\boldsymbol{a}\| \, \|\boldsymbol{b}\| .$$

Orthogonal Projection

Given two vectors $\boldsymbol{a}$ and $\boldsymbol{v}$ the orthogonal projection of $\boldsymbol{v}$ on $\boldsymbol{a}$ is given by

$$\boldsymbol{p} = \frac{\boldsymbol{a} \cdot \boldsymbol{v}}{\|\boldsymbol{a}\|^2} \boldsymbol{a}.$$

Theorem (Triangle Inequality)

For vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ we have

$$\|\boldsymbol{b} + \boldsymbol{a}\| \leq \|\boldsymbol{a}\| + \|\boldsymbol{b}\| .$$

Proof.

Exercise. Hint: expand $\|\boldsymbol{b} + \boldsymbol{a}\|^2$ and use the Cauchy-Schwartz Inequality. □

Displacement and Velocity

If an object has a constant velocity $\boldsymbol{v}$ and travels for t seconds, then the displacement is a function of time (in fact a line), given by

$$\boldsymbol{d} = \boldsymbol{v}t.$$

Work Done Against a Force

If a constant force $\boldsymbol{F}$ acts on a body and is displaced by $\boldsymbol{d}$, then the work done against the force is give by

$$-\boldsymbol{F} \cdot \boldsymbol{d}.$$

Equation of a Plane

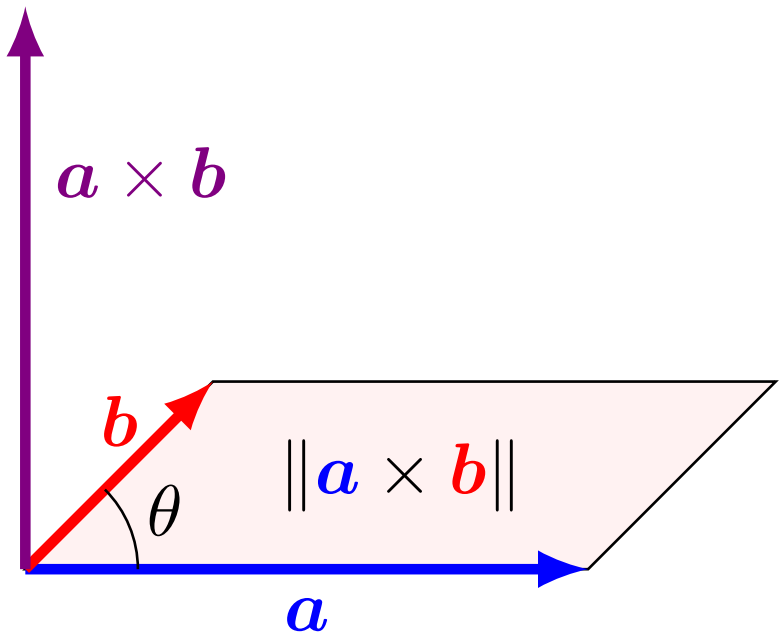
Let $\boldsymbol{r} = x\boldsymbol{i} + y\boldsymbol{j} + z\boldsymbol{k}$, and $\boldsymbol{a} \neq \boldsymbol{0}$ be a fixed vector. Then the equation of a plane perpendicular to $\boldsymbol{a}$ is

$$\boldsymbol{r} \cdot \boldsymbol{a} = xa_1 + ya_2 + za_3 = c \text{ for some } c \in \mathbb{R}.$$

Cross Product Introduction

The cross product of two vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ written as $\boldsymbol{a} \times \boldsymbol{b}$ is a vector perpendicular to both $\boldsymbol{a}$ and $\boldsymbol{b}$ whose magnitude is

$$\|\boldsymbol{a}\| \, \|\boldsymbol{b}\| \sin\theta.$$



The upward direction of $\boldsymbol{a} \times \boldsymbol{b}$ is know as the **right-handed** rule.

Definition (Cross Product)

Given two vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ the cross product is defined as the determinant of a certain matrix formed by $\boldsymbol{a}$ and $\boldsymbol{b}$,

$$\boldsymbol{a} \times \boldsymbol{b} = \begin{vmatrix} \boldsymbol{i} & \boldsymbol{j} & \boldsymbol{k} \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix} = \begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix} \boldsymbol{i} - \begin{vmatrix} a_1 & a_3 \\ b_1 & b_3 \end{vmatrix} \boldsymbol{j} + \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} \boldsymbol{k}.$$

Example

The cross product of $\boldsymbol{a} = 3\boldsymbol{i} + 2\boldsymbol{j} - \boldsymbol{k}$ and $\boldsymbol{b} = \boldsymbol{i} - \boldsymbol{j} - \boldsymbol{k}$ is

$$\begin{aligned} \boldsymbol{a} \times \boldsymbol{b} &= \begin{vmatrix} \boldsymbol{i} & \boldsymbol{j} & \boldsymbol{k} \\ 3 & 2 & -1 \\ 1 & -1 & -1 \end{vmatrix} \\ &= (2 \times -1 - -1 \times -1)\,\boldsymbol{i} - (3 \times -1 - -1 \times 1)\,\boldsymbol{j} \\ &\quad + (3 \times -1 - -1 \times 1)\,\boldsymbol{k} = -3\boldsymbol{i} + 2\boldsymbol{j} - 2\boldsymbol{k}. \end{aligned}$$

Remark 4: Properties of Cross Product

Given vectors $\boldsymbol{a}$, $\boldsymbol{b}$, and $\boldsymbol{c}$, in $\mathbb{R}^3$ and real numbers α and β, the following holds.

1. $\boldsymbol{a} \times \boldsymbol{b} = -\boldsymbol{b} \times \boldsymbol{a}$; thus $\boldsymbol{a} \times \boldsymbol{a} = 0$.
2. $(\alpha \boldsymbol{a}) \times \boldsymbol{b} = \alpha\,(\boldsymbol{a} \times \boldsymbol{b})$ and $\boldsymbol{a} \times (\beta \boldsymbol{b}) = \beta\,(\boldsymbol{a} \times \boldsymbol{b})$.
3. $\boldsymbol{a} \times (\boldsymbol{b} + \boldsymbol{c}) = \boldsymbol{a} \times \boldsymbol{b} + \boldsymbol{a} \times \boldsymbol{c}$ and $(\boldsymbol{a} + \boldsymbol{b}) \times \boldsymbol{c} = \boldsymbol{a} \times \boldsymbol{c} + \boldsymbol{b} \times \boldsymbol{c}$

Exercise 7: Cross Product

- Find the following cross products.

  $\boldsymbol{i} \times \boldsymbol{i},\ \boldsymbol{j} \times \boldsymbol{j},\ \boldsymbol{k} \times \boldsymbol{k},\ \boldsymbol{i} \times \boldsymbol{j},\ \boldsymbol{j} \times \boldsymbol{k},\ \boldsymbol{i} \times \boldsymbol{k},\ \boldsymbol{i} \times (a_1 \boldsymbol{i} + a_2 \boldsymbol{j} + a_3 \boldsymbol{k})\,.$

- Prove the properties in Remark 4.

Scalar Triple Product

- The scalar **triple product** of three vectors $\boldsymbol{a}$, $\boldsymbol{b}$, and $\boldsymbol{c}$, in $\mathbb{R}^3$ is defined **determinant** of the matrix with rows $\boldsymbol{a}$, $\boldsymbol{b}$, and $\boldsymbol{c}$, so

$$[\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}] = \boldsymbol{a} \cdot \boldsymbol{b} \times \boldsymbol{c} = \begin{vmatrix} b_2 & b_3 \\ c_2 & c_3 \end{vmatrix} a_1 - \begin{vmatrix} b_1 & b_3 \\ c_1 & c_3 \end{vmatrix} a_2 + \begin{vmatrix} b_1 & b_2 \\ c_1 & c_2 \end{vmatrix} a_3.$$

- Geometrically its magnitude is the **volume** of parallelepiped formed by the three vectors.
- The scalar product has the following properties.
  1. $\boldsymbol{a} \cdot \boldsymbol{b} \times \boldsymbol{c} = \boldsymbol{a} \times \boldsymbol{b} \cdot \boldsymbol{c}$
  2. $\boldsymbol{a} \cdot \boldsymbol{b} \times \boldsymbol{c} = \boldsymbol{b} \cdot \boldsymbol{c} \times \boldsymbol{a} = \boldsymbol{c} \cdot \boldsymbol{a} \times \boldsymbol{b}$
  3. The triple product is zero if any of the two vectors are parallel.

Solid Body Rotation

Let $\boldsymbol{r} = x\boldsymbol{i} + y\boldsymbol{j} + z\boldsymbol{k}$, and $\boldsymbol{\Omega} = \Omega\boldsymbol{k}$ for some fixed Ω. Then the vector

$$\boldsymbol{r} \times \boldsymbol{\Omega} = \Omega y\boldsymbol{i} - \Omega x\boldsymbol{j}$$

is the rotation of $\boldsymbol{r}$ around the z-axis with angular velocity Ω.

Exercise 8: Triple Product

A particle with mass m and electric charge q moves in a uniform magnetic field $\boldsymbol{B}$. Given that the force $\boldsymbol{F}$ on the particle is $\boldsymbol{F} = q\boldsymbol{v} \times \boldsymbol{B}$, with $\boldsymbol{v}$ the velocity of the particle, show that the particle has constant speed.

Let f be a function whose domain is a subset $U \subset \mathbb{R}^n$ range contained in $\mathbb{R}^m$, so

$$f : U \subseteq \mathbb{R}^n \longrightarrow \mathbb{R}^m$$
$$\boldsymbol{x} = (x_1, x_2, ..., x_n) \longmapsto f(\boldsymbol{x}) = (f_1(\boldsymbol{x}), ..., f_m(\boldsymbol{x})).$$

If $m = 1$, then f is called an scalar-valued function, or a **scalar field**, for example

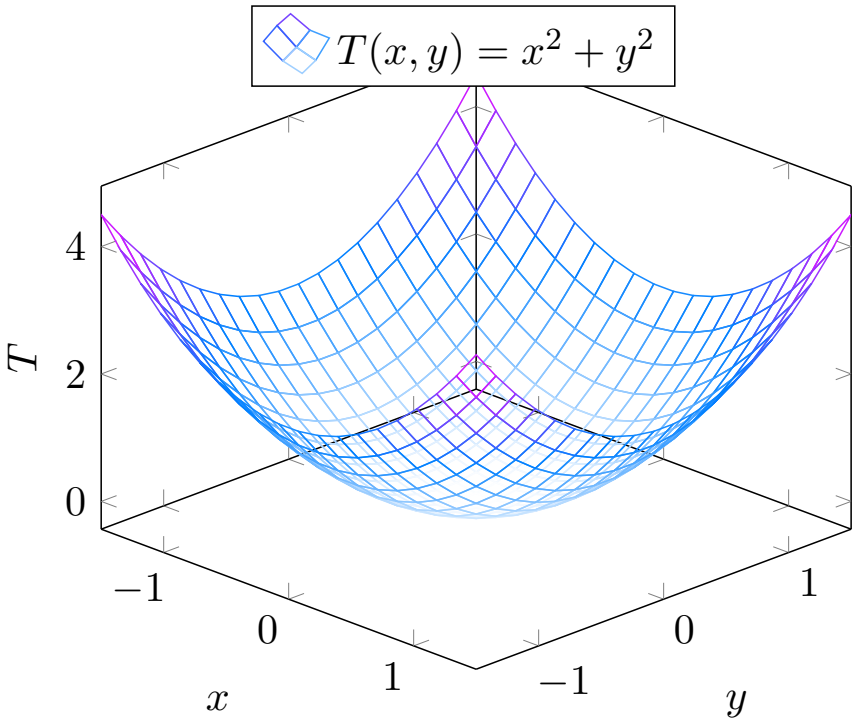
$$f(x, y, z) = \sqrt{x^2 + y^2 + z^2}.$$

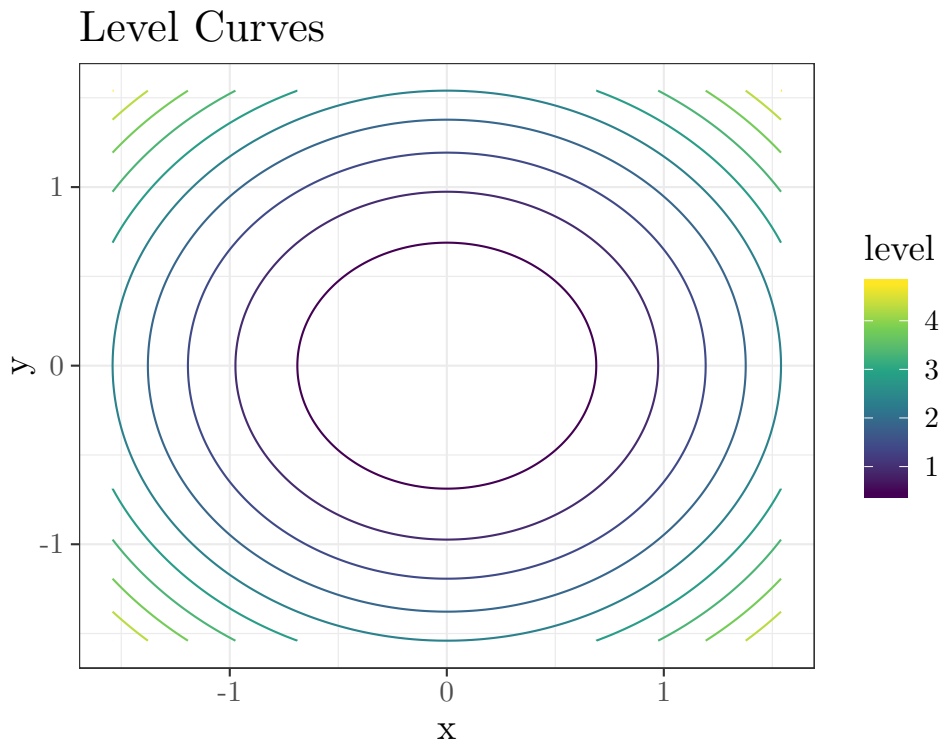
If $m > 1$, then f is called an vector-valued function, or a **vector field**, for example

$$\boldsymbol{F}(x, y, z) = \left(\sqrt{x^2 + y^2 + z^2}, \frac{y}{\sqrt{x^2 + y^2 + z^2}} \right).$$

Scalar Field

Scalar fields produce a **single value** for each position. Temperature of a square plate is a scalar field, so for each position we have a value $T(x, y)$.

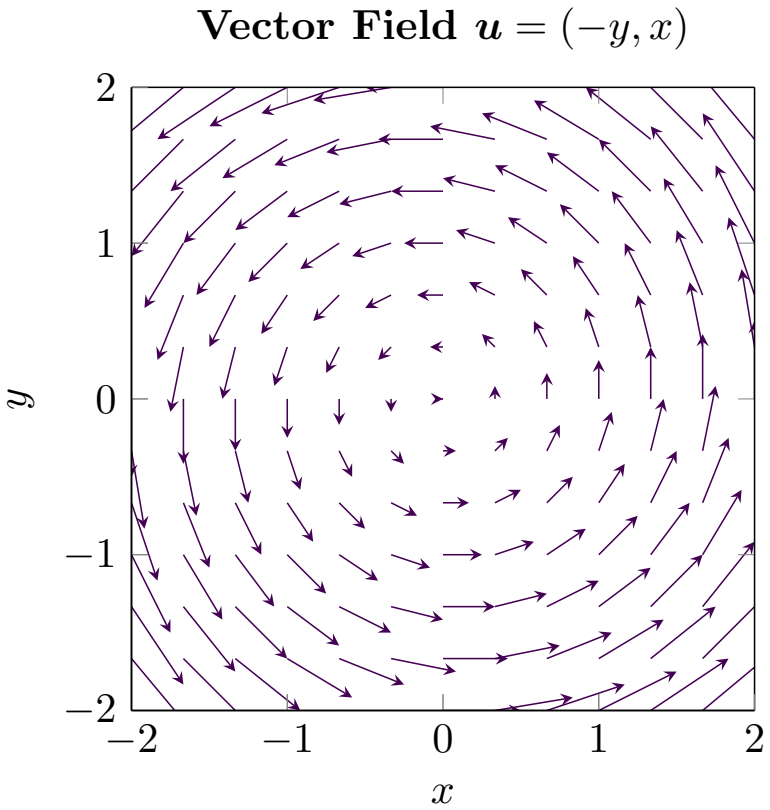


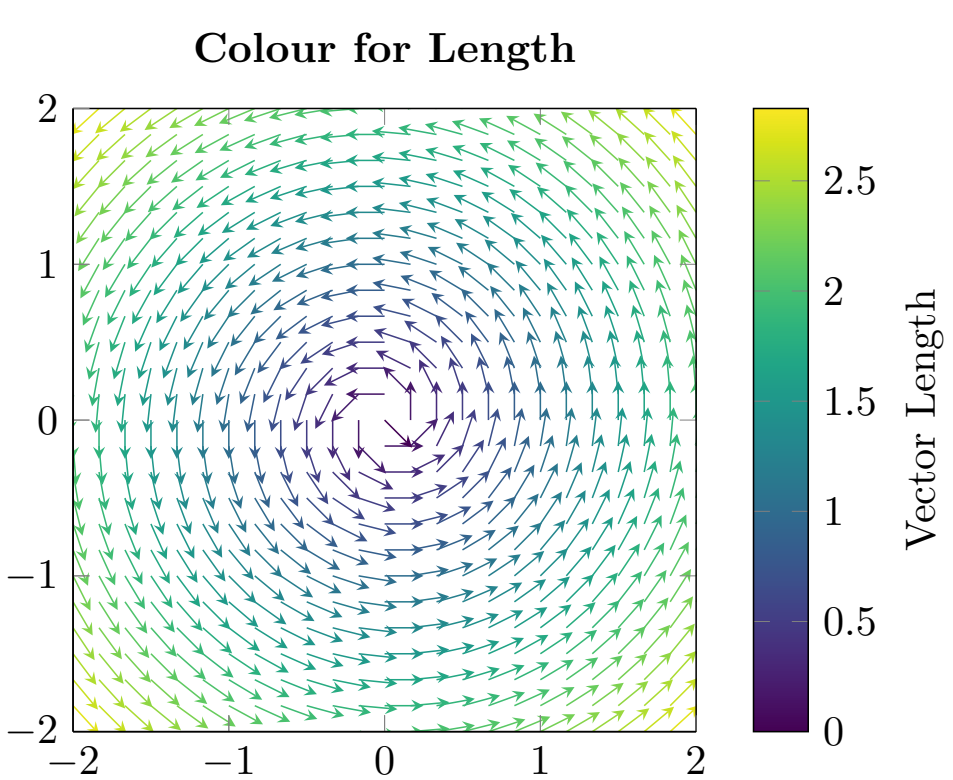


Level curves are given by $x^2 + y^2 = c$ for different values of $c > 0$.

Vector Fields

Vector Fields assign a **vector** to each position, e.g., consider velocity of a fluid on a square plate $\boldsymbol{u}(x, y)$





Definition (Graph of a Function)

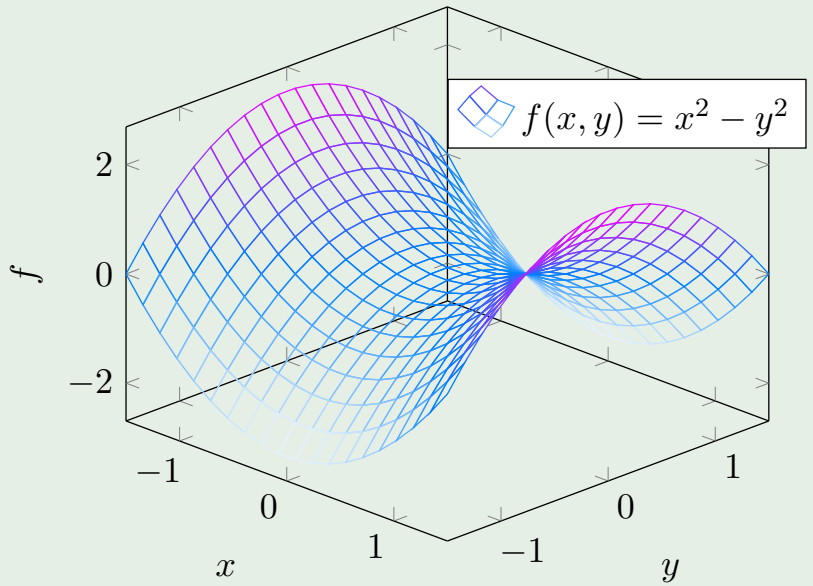
Let $\boldsymbol{f} : U \subset \mathbb{R}^n \longrightarrow \mathbb{R}^m$ be a function. Then the graph of f is a subset of $\mathbb{R}^{n+m}$ defined as

$$\text{graph } \boldsymbol{f} = \{(x_1, ..., x_n, f_1(\boldsymbol{x}), ..., , f_m(\boldsymbol{x})) \mid \boldsymbol{x} = (x_1, ..., x_n) \in U\}.$$

Example

The graph of $f : \mathbb{R}^2 \longrightarrow \mathbb{R}$ given by $f(x, y) = x^2 - y^2$ is

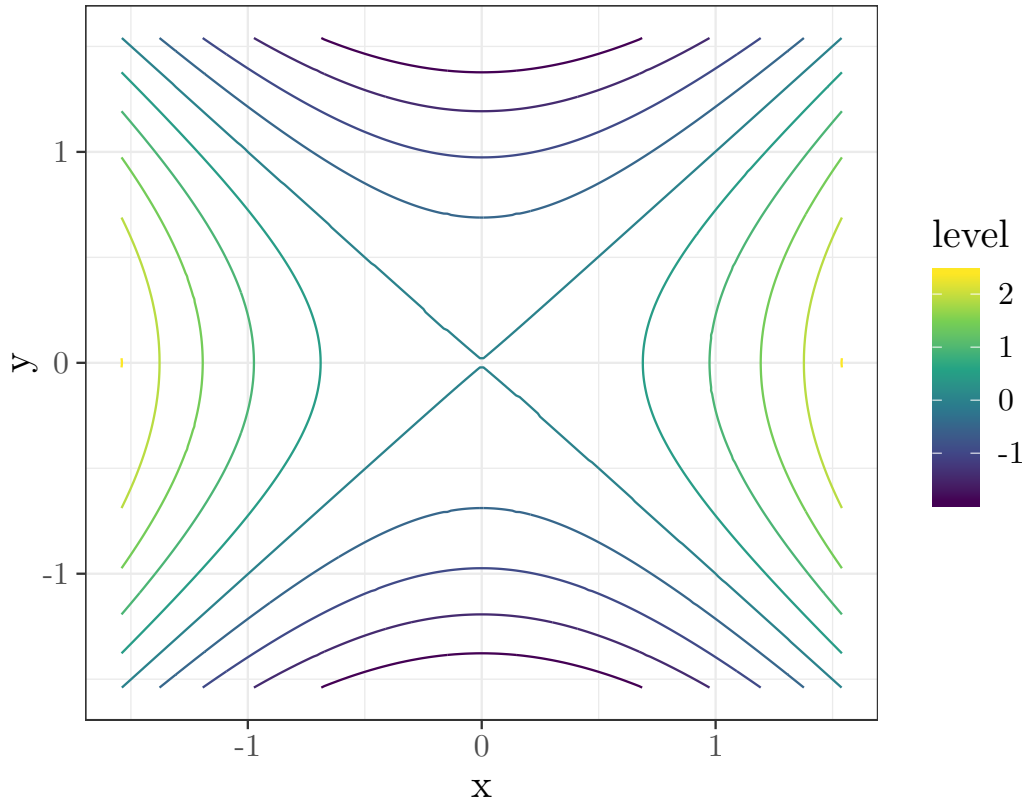
$$\text{graph } f = \left\{\left(x, y, x^2 - y^2\right) \mid \boldsymbol{x} = (x, y) \in \mathbb{R}^2\right\}.$$



Definition (Level Curves and Surfaces)

Let $\boldsymbol{f} : U \subset \mathbb{R}^n \longrightarrow \mathbb{R}$ be a function and $c \in \mathbb{R}$. Then level set of value c for f is the set of point $\boldsymbol{x} \in U$ such that $f(\boldsymbol{x}) = c$. If $n = 2$, we have curves, and for $n = 3$ we have surfaces.

The level curves of $f : \mathbb{R}^2 \longrightarrow \mathbb{R}$ given by $f(x, y) = x^2 - y^2$ are



Exercise 8: Scalar and Vector Fields

- Produce graph$f$ and level curves of f for $f(x, y) = x^2 + y$.
- For $\boldsymbol{F}(x, y) = (-x, -y)$ plot the vector field.

Summary

What we did today...

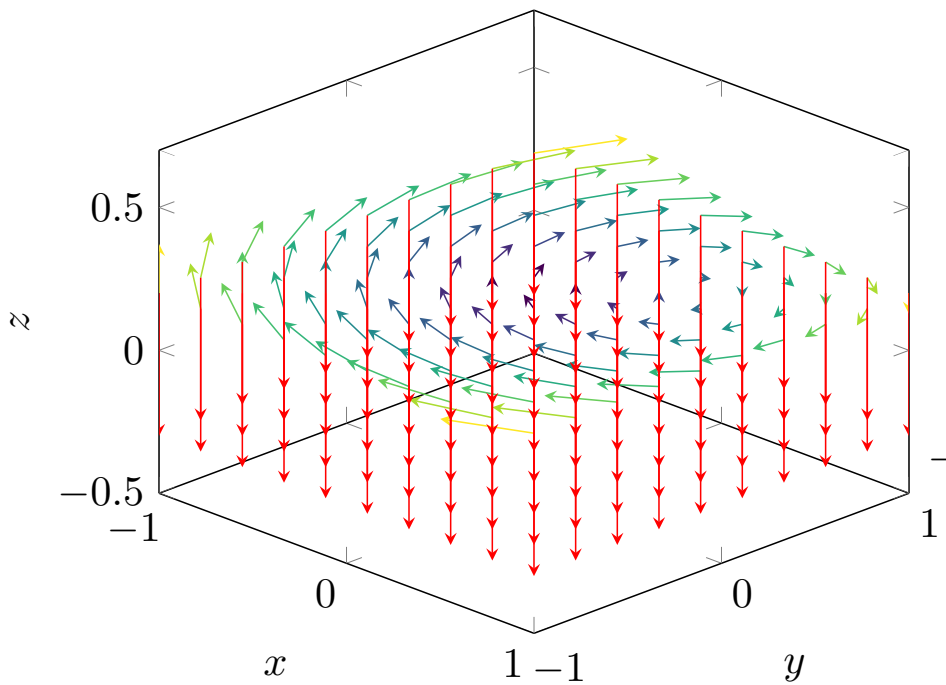
Vector Algebra	Vectors, Spaces, Linear Maps
Dot and Cross Product	Lengths, Angles, Inequalities
Real-Valued Functions	Scalar, Vector Fields
Visualisations	Graphs, Level Surfaces
Next Time	Differentation, grad, div, curl

"In these days the angel of topology and the devil of abstract algebra fight for the soul of every individual discipline of mathematics."

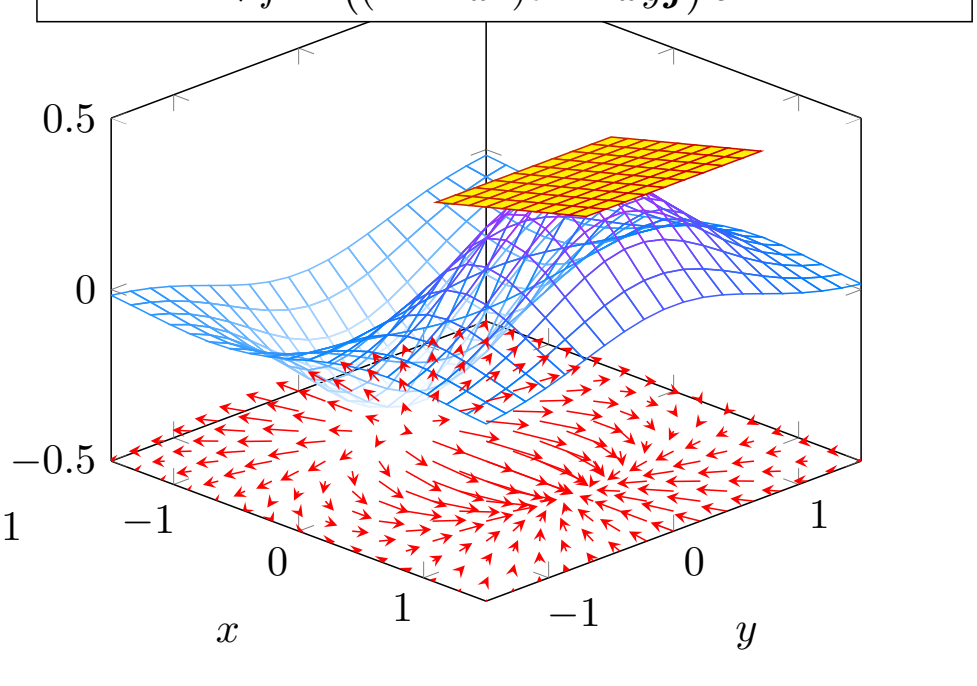
Hermann Weyl 1885-1955, Mathematician and Philosopher

Topic 2
Differentiation, Gradient, Divergence, Curl

$$\boldsymbol{F} = \boldsymbol{r} \times \boldsymbol{k} + z\boldsymbol{k} = y\boldsymbol{i} - x\boldsymbol{j} + z\boldsymbol{k}$$
$$\nabla \cdot \boldsymbol{F} = 1, \quad \nabla \times \boldsymbol{F} = -2\boldsymbol{k}$$



$$f = xe^{-x^2-y^2}$$
$$z = 0.65e^{-0.65^2} + (1 - 2 \times 0.65^2)e^{-0.65^2}(x - 0.65)$$
$$\nabla f = \left((1 - 2x^2)\boldsymbol{i} - 2xy\boldsymbol{j}\right) e^{-x^2-y^2}$$



Lecture Contents

1. Introduction
   - Module Aims and Assessment
   - Topics to be Covered
   - Reading List and References
2. Topic 1: Vector Algebra and Real-Valued Functions
   - Introduction
   - Vectors Algebra
   - Euclidean Space
   - Dot and Cross Products
   - Real-Valued Functions
3. Topic 2: Differentiation, Gradient, Divergence, Curl
   - Continuity of Multivariate Functions
   - Differentiation of Multivariate Functions
   - Gradient of a Scalar field
   - Divergence of a Vector Field
   - Curl of a Vector Field
   - Mixed Partial Derivative and Laplacian
4. Topic 3: Line, Surface, and Volume Integrals
   - Line Integrals
   - Surface Integrals
   - Volume Integrals
5. Topic 4: Integrals Theorems and Applications
   - Gauss's (Divergence) Theorem
   - Stokes' Theorem
6. Topic 1: Integers and Divisibility
   - Methods of Number Theory
   - Well-Ordering Principle and Archimedes Property
   - Polygonal Numbers
   - The Division Algorithm
   - Greatest Common Divisor
   - The Euclidean Algorithm
   - The Diophantine Equation $ax + by = c$
7. Topic 2: Primes and Their Distribution
   - Prime Numbers
   - Fundamental Theorem of Arithmetic
   - Distribution of Primes
   - Goldbach's Conjecture
   - Primes in Arithmetic Progression
8. Topic 3: The Theory of Congruences
   - Basic Properties of Congruences
   - Cancellation Rule
   - Representations of Integers
   - Linear Congruences
   - Chinese Remainder Theorem
9. Topic 4: Fermat's, Wilson's Theorems, and Number Theoretic Functions
   - Fermat's Little Theorem and Pseudoprimes
   - Wilson's Theorem
   - Number Theoretic Functions
   - Applications to RSA Cryptosystem

Intended Learning Outcomes

By the end of this session you will be able to...

1. Understand continuity and differentiation of multivariate functions.
2. Calculate partial derivatives of multivariate functions.
3. Compute the gradient and Laplacian of scalar fields.
4. Calculate the divergence and curl of vector fields.

Multivariate Functions

Let f be a function whose domain is a subset $U \subset \mathbb{R}^n$ range contained in $\mathbb{R}^m$, so

$$f : U \subseteq \mathbb{R}^n \longrightarrow \mathbb{R}^m$$
$$\boldsymbol{x} = (x_1, x_2, ..., x_n) \longmapsto f(\boldsymbol{x}) = (f_1(\boldsymbol{x}), ..., f_m(\boldsymbol{x})).$$

Recall: if $m = 1$, then f is a **scalar field**, for example,

$$f(x, y) = x + y,\ g(x, y) = x^2 + y^2,\ h(x, y) = xy.$$

If $m > 1$, then f is a **vector field**, for example,

$$\boldsymbol{F}(x, y) = (x, 0)\,,\ \boldsymbol{F}(x, y) = (x, y)\,,\ \boldsymbol{F}(x, y) = (y, 0)\,.$$

If $n = 1$, then f is called a **path** for example,

$$f(x) = (x, x^2, x^3),\ f(x) = (\cos x, \sin x, x).$$

We will be interested in the properties of these functions involving continuity and differentiability.

Continuity of Multivariate Functions

Let

$$f : U \subseteq \mathbb{R}^n \longrightarrow \mathbb{R}^m$$

be a real-valued function, $\boldsymbol{x}_0 \in U$, and $\boldsymbol{b} = f(\boldsymbol{x}_0)$.

- The **continuity** of f is concerned with the behaviour of f on the points in the neighbourhood of $\boldsymbol{x}$.
- If f **well-behaved** around $\boldsymbol{x}_0$, we say f is continuous at $\boldsymbol{x}_0$
- In general we say $f(\boldsymbol{x})$ **approaches** $\boldsymbol{b}$ as $\boldsymbol{x}$ approaches $\boldsymbol{x}_0$ and write

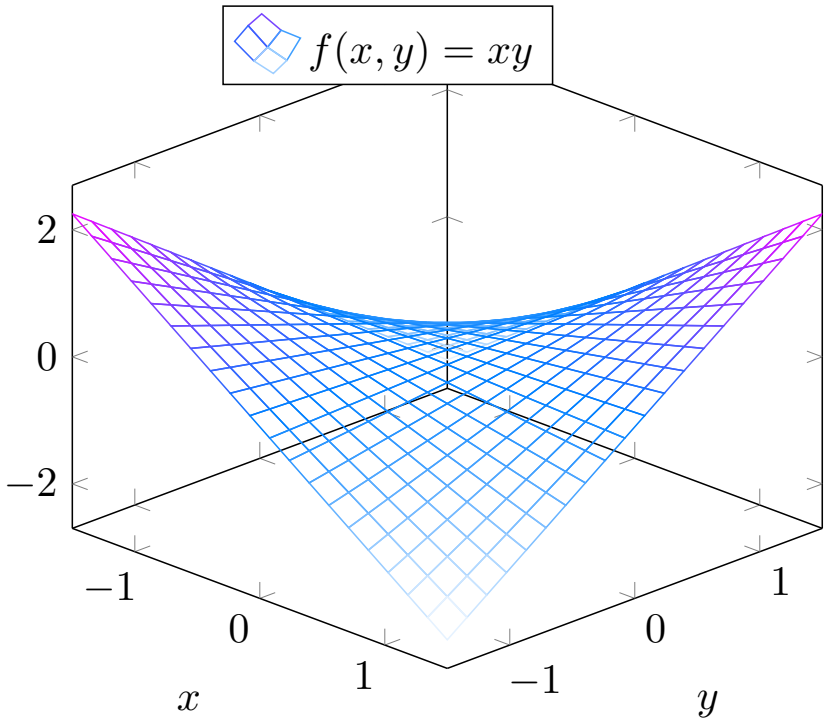
$$\lim_{\boldsymbol{x} \to \boldsymbol{x}_0} f(\boldsymbol{x}) = \boldsymbol{b}.$$

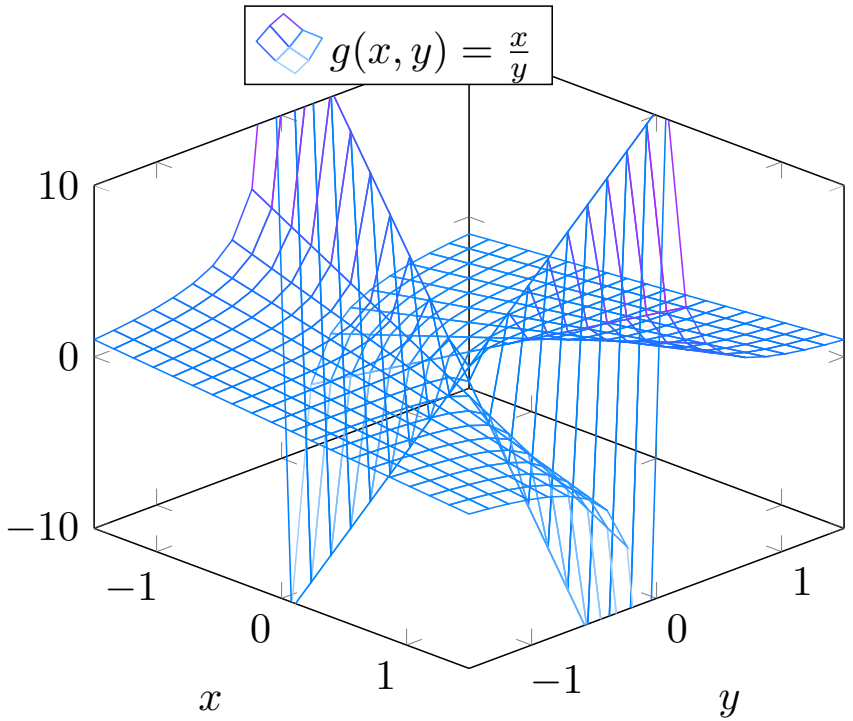
Definition (Continuity)

Let $f : U \subseteq \mathbb{R}^n \longrightarrow \mathbb{R}^m$ and $\boldsymbol{x}_0 \in U$, then we say f is **continuous** at $\boldsymbol{x}_0$ if for every number $\epsilon > 0$ there exists a number $\delta > 0$ such that for every $\boldsymbol{x} \in U$ with $\|\boldsymbol{x} - \boldsymbol{x}_0\| < \delta$ implies that $\|f(\boldsymbol{x}) - f(\boldsymbol{x}_0)\| < \epsilon$.

Examples of Continuity

The function $f(x, y) = xy$ is everywhere continuous on $\mathbb{R}^2$.





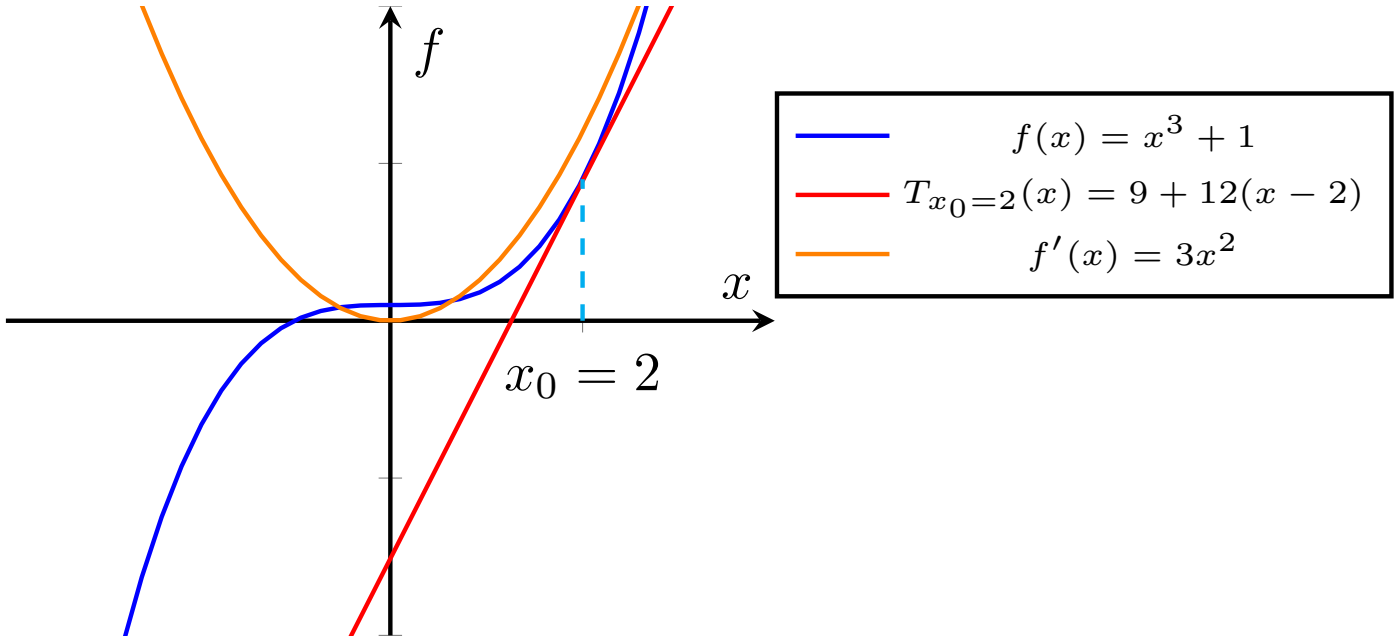
The function $g(x, y) = \dfrac{x}{y}$ is not continuous on all point of the line $y = 0$ and continuous everywhere else. Continuity really means that there are no **"breaks"** in the graph of the function. We will be working with continuous functions.

Differentiation of Multivariate Functions

- Differentiation is concerned with **approximation** of function with **linear** functions.
- Recall is the case $f : \mathbb{R} \longrightarrow \mathbb{R}$ the value $f'(x_0)$ denotes the slope of the tangent line at x_0, and we had

$$f'(x_0) = \frac{\mathrm{d}f}{\mathrm{d}x} = \lim_{x \to x_0} \frac{f(x) - f(x_0)}{x - x_0}.$$

- For example,



Partial Derivatives I

- In the case of multivariate functions say

$$f : U \subseteq \mathbb{R}^n \longrightarrow \mathbb{R}^m$$
$$\boldsymbol{x} = (x_1, x_2, ..., x_n) \longmapsto f(\boldsymbol{x}) = (f_1(\boldsymbol{x}), ..., f_m(\boldsymbol{x})).$$

- We can calculate the derivative of the function f in the direction of a vector $\boldsymbol{v}$, using

$$\mathrm{d}f_{\boldsymbol{v}} = \lim_{h \to 0} \frac{f(\boldsymbol{x} + h\boldsymbol{v}) - f(\boldsymbol{x})}{h}.$$

- We can have the derivative of the function f in the direction of a vector **unit vectors** $\boldsymbol{i}$, $\boldsymbol{j}$, $\boldsymbol{k}$.

Definition (Partial Derivative)

Let $f : U \subseteq \mathbb{R}^3 \longrightarrow \mathbb{R}$ be a real-valued function. Then $\dfrac{\partial f}{\partial x}, \dfrac{\partial f}{\partial y}, \dfrac{\partial f}{\partial z}$ the **partial derivatives** of f with respect to x, y, z are real-values functions defined by

$$\frac{\partial f}{\partial x} = \lim_{h\to 0} \frac{f(\boldsymbol{x} + h\boldsymbol{i}) - f(\boldsymbol{x})}{h} = \lim_{h\to 0} \frac{f(x+h, y, z) - f(x, y, z)}{h}$$
$$\frac{\partial f}{\partial y} = \lim_{h\to 0} \frac{f(\boldsymbol{x} + h\boldsymbol{j}) - f(\boldsymbol{x})}{h} = \lim_{h\to 0} \frac{f(x, y+h, z) - f(x, y, z)}{h}$$
$$\frac{\partial f}{\partial z} = \lim_{h\to 0} \frac{f(\boldsymbol{x} + h\boldsymbol{k}) - f(\boldsymbol{x})}{h} = \lim_{h\to 0} \frac{f(x, y, z+h) - f(x, y, z)}{h}$$

For example, $\dfrac{\partial f}{\partial x}$ is the derivative of f with respect to x assuming y and z are kept constant.

Example

If $f(x, y, z) = x^2y + y^3 + \sin z$, find $\dfrac{\partial f}{\partial x}$, $\dfrac{\partial f}{\partial y}$, and $\dfrac{\partial f}{\partial z}$.

Solution: To find $\dfrac{\partial f}{\partial x}$ assume y and z are constant, so

$$\frac{\partial f}{\partial x} = 2xy,$$

similarly

$$\frac{\partial f}{\partial y} = x^2 + 3y^2 \text{ and } \frac{\partial f}{\partial z} = \cos z.$$

Exercise 1: Partial Derivative

Find the all partial derivatives of the function

$$f(x, y) = x^2 + y^2 + xy,\ g(x, y) = xe^{-x^2-y^2},\ h(x, y, z) = \sin xyz.$$

Tangent Spaces

- Partial derivatives can be used to **approximate** functions using linear spaces.
- Given a function say $f : U \subseteq \mathbb{R}^2 \longrightarrow \mathbb{R}$, and $\boldsymbol{x}_0 = (x_0, y_0) \in U$ we can write the equation of tangent plane to the graph$f$ at $(x_0, y_0, f(\boldsymbol{x}_0))$ by

$$z = f(\boldsymbol{x}_0) + \frac{\partial f}{\partial x}(\boldsymbol{x}_0)(x - x_0) + \frac{\partial f}{\partial y}(\boldsymbol{x}_0)(y - y_0).$$

- If we had $f : U \subseteq \mathbb{R}^3 \longrightarrow \mathbb{R}$, then we would have the equation of tangent space would be

$$t = f(\boldsymbol{x}_0) + \frac{\partial f}{\partial x}(\boldsymbol{x}_0)(x - x_0) + \frac{\partial f}{\partial y}(\boldsymbol{x}_0)(y - y_0) + \frac{\partial f}{\partial z}(\boldsymbol{x}_0)(z - z_0).$$

Exercise 2: Tangent Spaces

Find the tangent plane to the graph of $g(x, y) = xe^{-x^2-y^2}$ at $\boldsymbol{x}_0 = \left(\frac{\sqrt{2}}{2}, 0\right)$.

Matrix of Partial Derivatives

In the general case of functions

$$f : U \subseteq \mathbb{R}^n \longrightarrow \mathbb{R}^m$$
$$\boldsymbol{x} = (x_1, x_2, ..., x_n) \longmapsto f(\boldsymbol{x}) = (f_1(\boldsymbol{x}), ..., f_m(\boldsymbol{x})),$$

we can calculate an $m \times n$ matrix of partial derivatives

$$\boldsymbol{T} = \boldsymbol{D}f(\boldsymbol{x_0}) = \begin{pmatrix} \dfrac{\partial f_1}{\partial x_1} & \dfrac{\partial f_1}{\partial x_2} & \cdots & \dfrac{\partial f_1}{\partial x_n} \\ \vdots & \vdots & \vdots & \\ \dfrac{\partial f_m}{\partial x_1} & \dfrac{\partial f_m}{\partial x_2} & \cdots & \dfrac{\partial f_m}{\partial x_n} \end{pmatrix}.$$

where $\partial f_i / \partial x_j$ is evaluated at $\boldsymbol{x_0}$. For example, if $n = m = 3$,

$$\boldsymbol{D}f(\boldsymbol{x_0}) = \begin{pmatrix} \dfrac{\partial f_1}{\partial x} & \dfrac{\partial f_1}{\partial y} & \dfrac{\partial f_1}{\partial z} \\ \dfrac{\partial f_2}{\partial x} & \dfrac{\partial f_2}{\partial y} & \dfrac{\partial f_2}{\partial z} \\ \dfrac{\partial f_3}{\partial x} & \dfrac{\partial f_3}{\partial y} & \dfrac{\partial f_3}{\partial z} \end{pmatrix}.$$

Definition (Differentiable or C^1 Function)

Let $f : U \subseteq \mathbb{R}^n \longrightarrow \mathbb{R}^m$ be a function, we can f is **differentiable** at $\boldsymbol{x_0} \in U$ if the partial derivatives of f exist at $\boldsymbol{x_0}$ and if

$$\lim_{\boldsymbol{x} \to \boldsymbol{x_0}} \frac{\|f(\boldsymbol{x}) - f(\boldsymbol{x}_0) - \boldsymbol{T}(\boldsymbol{x} - \boldsymbol{x}_0)\|}{\|\boldsymbol{x} - \boldsymbol{x}_0\|} = 0,$$

where $\boldsymbol{T}(\boldsymbol{x} - \boldsymbol{x}_0)$ is the matrix multiplication of $\boldsymbol{T}$ with $\boldsymbol{x} - \boldsymbol{x}_0$.

Exercise 3: Matrix of Derivatives

Find the matrix of partial derivatives of $f(x, y, z) = (y, -x, z)$.

Remark 1: Properties of Derivative

Let $f, g : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ and $h : \mathbb{R}^m \longrightarrow \mathbb{R}^p$, and $\boldsymbol{c} \in \mathbb{R}$. We may write $\boldsymbol{D}f$ for $\boldsymbol{D}f(\boldsymbol{x}_0)$ etc... Then following holds.

1. **Constant Multiple Rule:**

$$\boldsymbol{D}\left(cf\right) = c\boldsymbol{D}f$$

2. **Sum Rule:**

$$\boldsymbol{D}\left(f+g\right) = \boldsymbol{D}f + \boldsymbol{D}g$$

3. **Product Rule:**

$$\boldsymbol{D}\left(fg\right) = g\boldsymbol{D}f + f\boldsymbol{D}g$$

4. **Chain Rule:**

$$\boldsymbol{D}\left(h \circ f\right) = \boldsymbol{D}h\boldsymbol{D}f$$

Definition (Gradient)

Let $f : U \subseteq \mathbb{R}^n \longrightarrow \mathbb{R}$ be a scalar field, then the row vector of derivatives

$$\boldsymbol{D}f(\boldsymbol{x_0}) = \left(\frac{\partial f}{\partial x_1}, \quad \frac{\partial f}{\partial x_2}, \quad \cdots, \quad \frac{\partial f}{\partial x_n} \right).$$

is called the **gradient** of f denoted by ∇f of grad$f$.

Example

If $f : U \subseteq \mathbb{R}^3 \longrightarrow \mathbb{R}$, then $\nabla f = \dfrac{\partial f}{\partial x}\boldsymbol{i} + \dfrac{\partial f}{\partial y}\boldsymbol{j} + \dfrac{\partial f}{\partial z}\boldsymbol{k}$. For example, for $f(x, y, z) = xe^y + z$, we have

$$\nabla f = e^y \boldsymbol{i} + xe^y \boldsymbol{j} + \boldsymbol{k}.$$

Exercise 4: Gradient

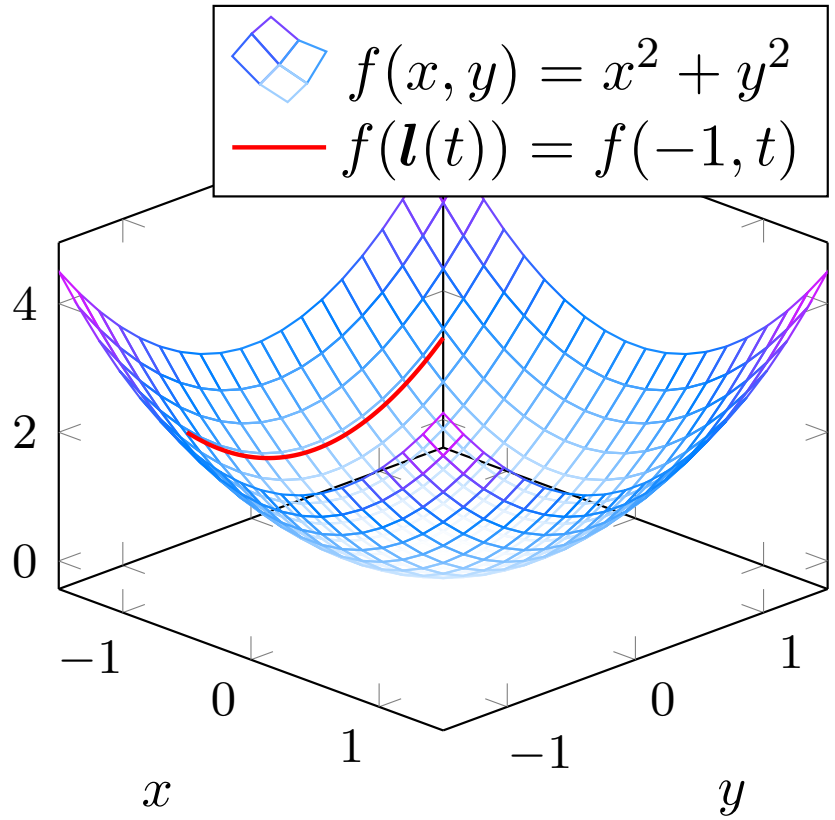
Find the gradient of $f(x, y) = xe^{-x^2-y^2}$.

Gradient and Directional Derivative

Let $f : U \subseteq \mathbb{R}^3 \longrightarrow \mathbb{R}$ be a scalar filed. Consider the line starting at a point $\boldsymbol{x}$ in the direction of $\boldsymbol{v}$ inside U, i.e.,

$$\boldsymbol{l}(t) = \boldsymbol{x} + t\boldsymbol{v}, \text{ for } t \in \mathbb{R}.$$

We may ask how fast is f changing along $\boldsymbol{l}$.



Definition (Directional Derivative)

If $f : \mathbb{R}^3 \longrightarrow \mathbb{R}$, the **directional derivative** of f at $\boldsymbol{x}$ along $\boldsymbol{v}$, which is normally a unit vector, is given by

$$\frac{\mathrm{d}}{\mathrm{d}t} f(\boldsymbol{x} + t\boldsymbol{v}) \Big|_{t=0} \quad \text{if it exists.}$$

Theorem

*If $f : \mathbb{R}^3 \longrightarrow \mathbb{R}$ is differentiable, the **directional derivative** of f at $\boldsymbol{x}$ along $\boldsymbol{v}$ exists and we*

$$\frac{\mathrm{d}}{\mathrm{d}t} f(\boldsymbol{x} + t\boldsymbol{v}) \Big|_{t=0} = \nabla f \cdot \boldsymbol{v} = v_1 \frac{\partial f}{\partial x} + v_2 \frac{\partial f}{\partial y} + v_3 \frac{\partial f}{\partial z}.$$

Exercise 4: Gradient

Compute the rate of change of $f(x, y) = xe^{-x^2-y^2}$ along $\boldsymbol{v} = \boldsymbol{i}$ at the point $(0, 0)$.

Theorem (Direction of Fastest Increase)

If $f : \mathbb{R}^3 \longrightarrow \mathbb{R}$ and $\nabla f \neq 0$, then ∇f points in the direction along which f increases fastest.

Proof.

Let $\boldsymbol{n}$ be a unit vector, then the rate of increase of f in the direction of $\boldsymbol{n}$ is $\nabla f \cdot \boldsymbol{n} = \|\nabla f\| \cos\theta$, where θ is the angle between ∇f and $\boldsymbol{n}$, maximum increase happens when $\theta = 0$. □

Theorem (Gradient Normal to Level Surfaces)

If $f : \mathbb{R}^3 \longrightarrow \mathbb{R}$ and $\boldsymbol{x}_0$ is a point in the level surface S given by $f(x, y, z) = k$, for some k, then $\nabla f(\boldsymbol{x}_0)$ is normal to the level surface. That is if $\boldsymbol{v}$ is a tangent vector at $t = 0$ to a path $\boldsymbol{c}(t)$ in S with $\boldsymbol{c}(0) = \boldsymbol{x}_0$, the $\nabla f(\boldsymbol{x}_0) \cdot \boldsymbol{v} = 0$.

Remark 2: Vector Property of Gradient

If $f : \mathbb{R}^3 \longrightarrow \mathbb{R}$, then the gradient

$$\nabla f = \frac{\partial f}{\partial x}\boldsymbol{i} + \frac{\partial f}{\partial y}\boldsymbol{j} + \frac{\partial f}{\partial z}\boldsymbol{k}$$

can be considered as a vector field, so

$$\nabla f : \mathbb{R}^3 \longrightarrow \mathbb{R}^3.$$

- If p denotes the pressure of a gas, then there is a force $\boldsymbol{F}$ acting on a volume δV due to the pressure gradient given by

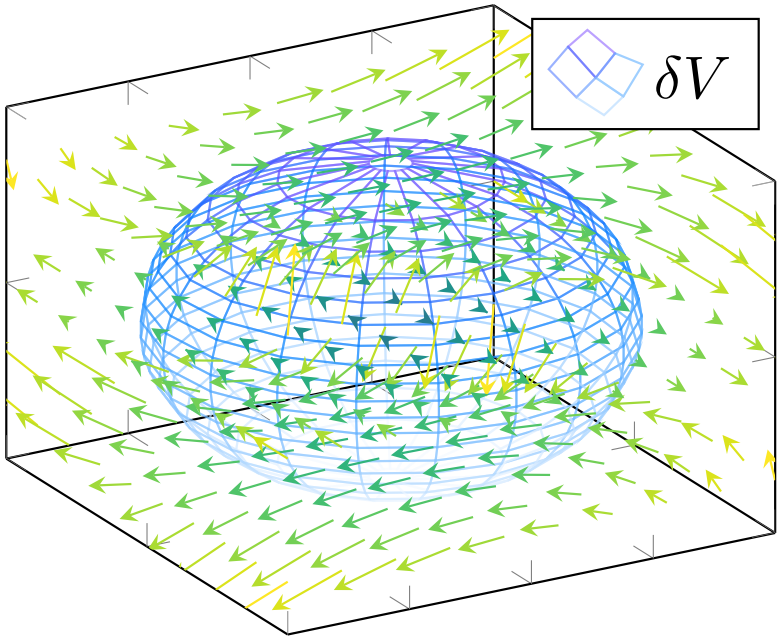
$$\boldsymbol{F} = \nabla p \delta V.$$

- A material has constant thermal conductivity K and variable temperature $T(\boldsymbol{r})$. Because of temperature variation heat flow from the hot to the clod regions. The heat flux $\boldsymbol{q}$ is given by

Divergence of a Vector Field

Lets consider vector fields, which are functions of the form

$$\boldsymbol{F} : U \subseteq \mathbb{R}^3 \longrightarrow \mathbb{R}^3$$
$$\boldsymbol{x} = (x, y, z) \longmapsto \boldsymbol{F}(\boldsymbol{x}) = (F_1(\boldsymbol{x}), F_2(\boldsymbol{x}), F_3(\boldsymbol{x})).$$



Divergence of a vector field is a scalar field, roughly corresponds to the amount of flux of $\boldsymbol{F}$ out of a small volume δV divided by volume of δV.

Definition (Divergence)

If $\boldsymbol{F} = F_1\boldsymbol{i} + F_2\boldsymbol{j} + F_3\boldsymbol{k}$ is a vector field, the **divergence** of $\boldsymbol{F}$ is a scalar field given by

$$\operatorname{div}\boldsymbol{F} = \nabla \cdot \boldsymbol{F} = \frac{\partial F_1}{\partial x} + \frac{\partial F_2}{\partial y} + \frac{\partial F_3}{\partial z}.$$

Example

If $\boldsymbol{F} = y\boldsymbol{i} - x\boldsymbol{j} + z\boldsymbol{k}$, then

$$\nabla \cdot \boldsymbol{F} = 1.$$

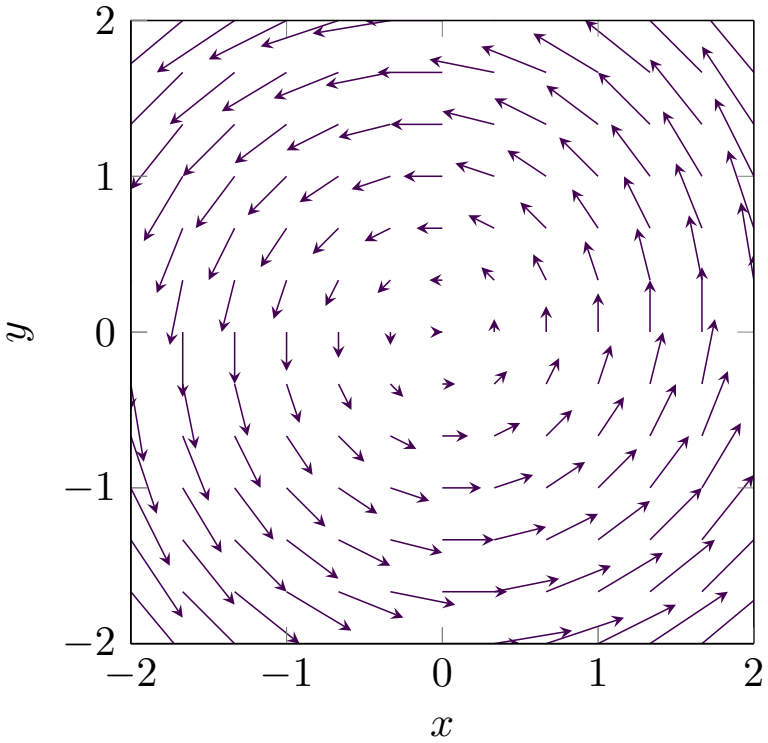
Exercise 5: Divergence

Let $\boldsymbol{F} = x^2y\boldsymbol{i} + z\boldsymbol{j} - xyz\boldsymbol{k}$. Compute

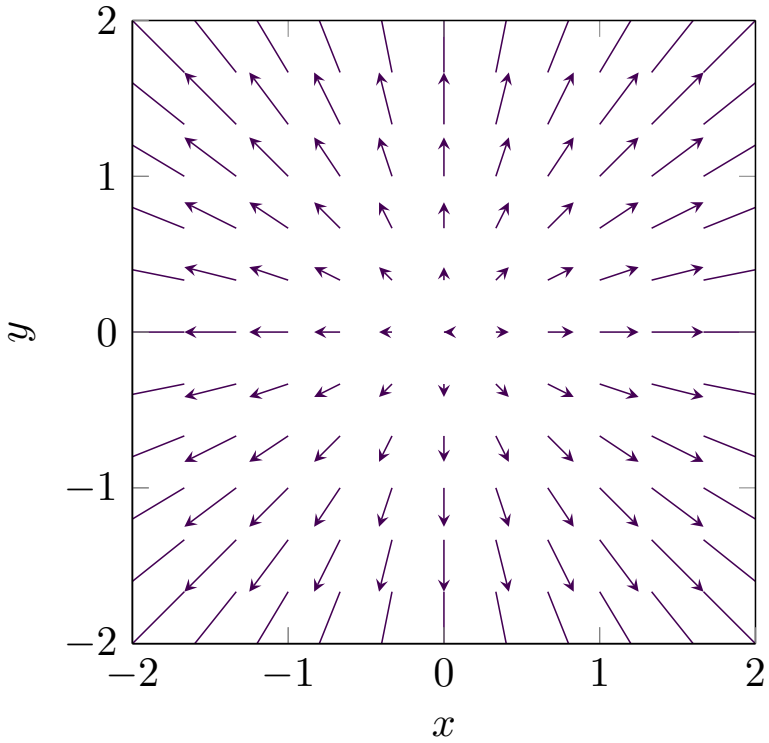
$$\nabla \cdot \boldsymbol{F}.$$

Divergence is related to sources and sinks.

$\boldsymbol{u} = (-y, x), \quad \nabla \cdot \boldsymbol{u} = 0$

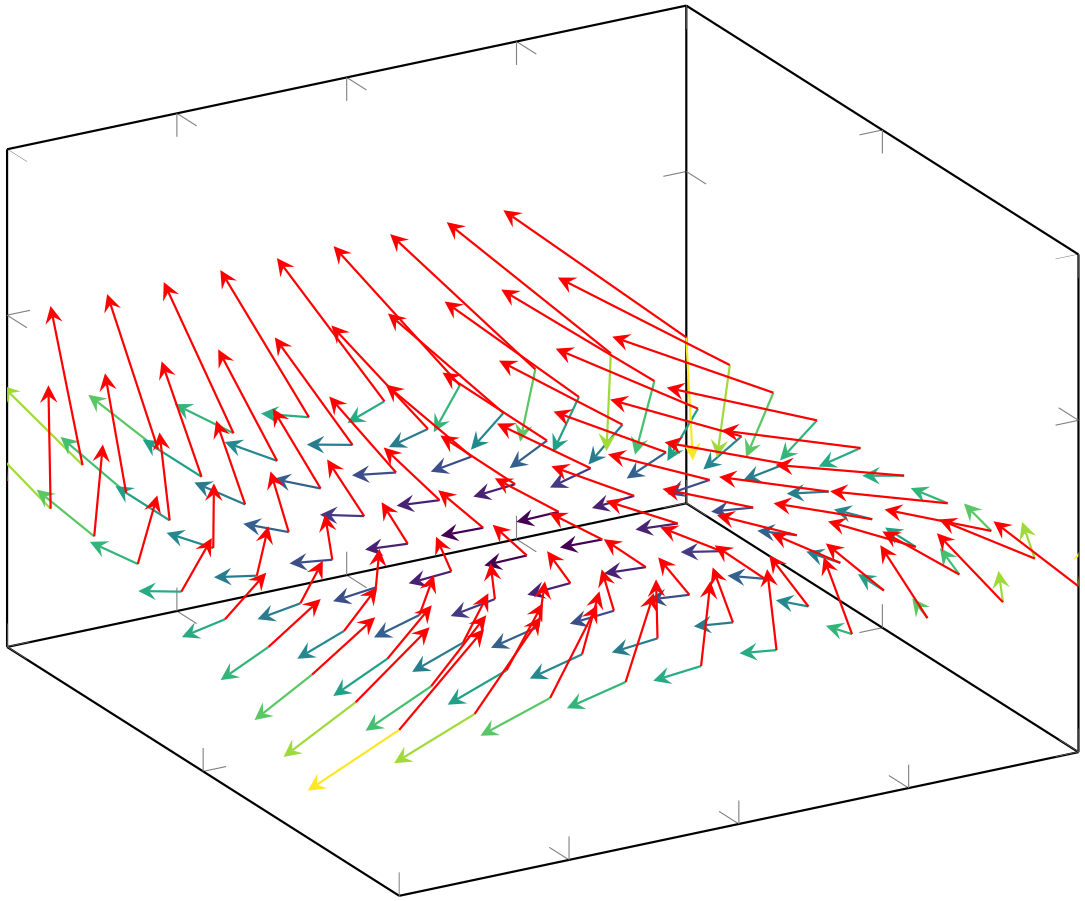


$\boldsymbol{u} = (x, y), \quad \nabla \cdot \boldsymbol{u} = 2$



Curl of a Vector Field

Lets consider vector fields, $\boldsymbol{F}(\boldsymbol{x}) = (F_1(\boldsymbol{x}), F_2(\boldsymbol{x}), F_3(\boldsymbol{x}))$ as before.



Curl of a vector field is a vector field, roughly corresponds to the rotation or twisting of $\boldsymbol{F}$.

Definition (Curl)

If $\boldsymbol{F} = F_1\boldsymbol{i} + F_2\boldsymbol{j} + F_3\boldsymbol{k}$ is a vector field, the **curl** of $\boldsymbol{F}$ is a vector field given by

$$\text{Curl}\boldsymbol{F} = \nabla \times \boldsymbol{F} = \begin{vmatrix} \boldsymbol{i} & \boldsymbol{j} & \boldsymbol{k} \\ \dfrac{\partial}{\partial x} & \dfrac{\partial}{\partial y} & \dfrac{\partial}{\partial z} \\ F_1 & F_2 & F_3 \end{vmatrix}$$

$$= \left(\frac{\partial F_3}{\partial y} - \frac{\partial F_2}{\partial z}\right)\boldsymbol{i} - \left(\frac{\partial F_3}{\partial x} - \frac{\partial F_1}{\partial z}\right)\boldsymbol{j} + \left(\frac{\partial F_2}{\partial x} - \frac{\partial F_1}{\partial y}\right)\boldsymbol{k}.$$

Example

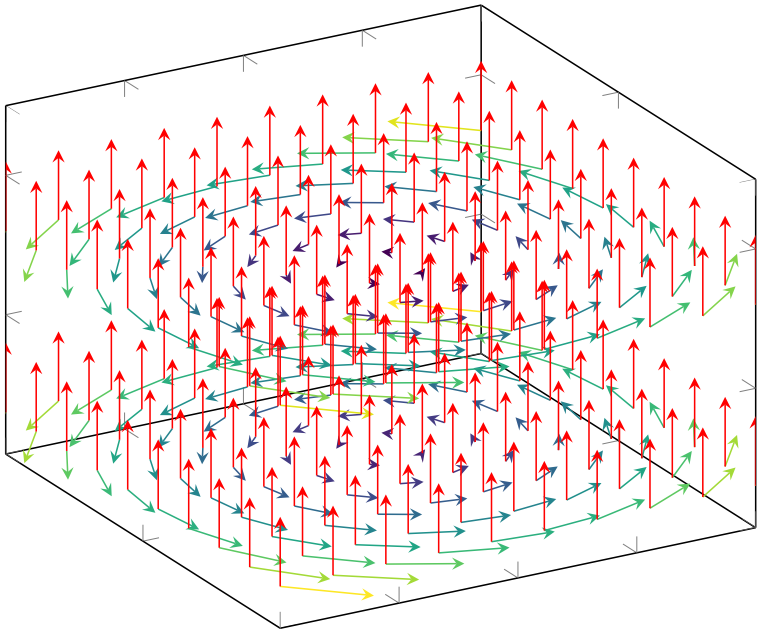
If $\boldsymbol{F} = y\boldsymbol{i} - x\boldsymbol{j} + z\boldsymbol{k}$, then $\nabla \times \boldsymbol{F} = -2\boldsymbol{k}$.

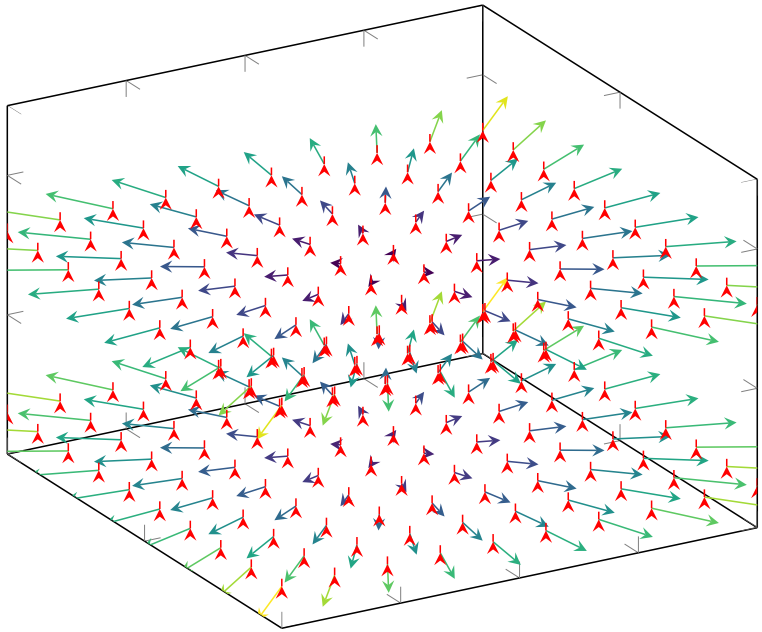
Exercise 5: Curl

Let $\boldsymbol{F} = x^2y\boldsymbol{i} + z\boldsymbol{j} - xyz\boldsymbol{k}$. Compute $\nabla \times \boldsymbol{F}$.

Curl Interpretations

Curl is related to twisting.





$\nabla \times (-y\boldsymbol{i} + x\boldsymbol{j}) = 2\boldsymbol{k}$

$\nabla \times (x\boldsymbol{i} + y\boldsymbol{j}) = 0$

Some Nice Interpretations

https://www.youtube.com/watch?v=rB83DpBJQsE.

Definition (Second Partial Derivatives and C^2 Functions)

Let $f : U \subseteq \mathbb{R}^3 \longrightarrow \mathbb{R}$ be a real-valued function differentiable function. The second partial derivates of f are

$$\frac{\partial}{\partial x}\frac{\partial f}{\partial x} = \frac{\partial^2 f}{\partial x^2}, \quad \frac{\partial}{\partial y}\frac{\partial f}{\partial y} = \frac{\partial^2 f}{\partial y^2}, \quad \frac{\partial}{\partial z}\frac{\partial f}{\partial z} = \frac{\partial^2 f}{\partial z^2}, \quad \frac{\partial}{\partial y}\frac{\partial f}{\partial x} = \frac{\partial^2 f}{\partial y\,\partial x},$$

$$\frac{\partial}{\partial y}\frac{\partial f}{\partial z} = \frac{\partial^2 f}{\partial y\,\partial z}, \text{ etc...}$$

There are 9 partial derivative, the function f is call twice continuously differentiable, or C^2, if all these partial derivatives exist.

Theorem (Equality of Mixed Derivatives)

If $f(x, y)$ is of class C^2, then mixed partial derivatives are equal, that is

$$\frac{\partial^2 f}{\partial x\,\partial y} = \frac{\partial^2 f}{\partial y\,\partial x}.$$

Laplacian is related to second derivatives of scalar and vector fields.

Definition (Laplacian of a Scalar Field)

If $f : U \subseteq \mathbb{R}^3 \longrightarrow \mathbb{R}$ is a scalar field, the Laplacian of f is defined as the divergence of gradient of f

$$\nabla \cdot \nabla f = \nabla^2 f = \frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2} + \frac{\partial^2 f}{\partial z^2}.$$

Example

If $f = xy$, then

$$\nabla^2 f = 0.$$

Summary: What we did...

- Multivariate Functions
  - Continuity and Differentiation
- Gradient ∇f
  - Scalar Fields
- Divergence $\nabla \cdot \boldsymbol{F}$
  - Vector fields
- Curl $\nabla \times \boldsymbol{F}$
  - Vector fields
- Laplacian $\nabla^2 f$
  - Scalar fields
- Next Time
  - Line, Surface, and Volume Integrals

Topic 3
Line, Surface, and Volume Integrals

$$\int_C f \, \|d\boldsymbol{r}\| = \int_t f(\boldsymbol{r}) \left\| \frac{d\boldsymbol{r}}{dt} \right\| dt$$

$$\int_S f \, \|d\boldsymbol{S}\| = \int_v \int_u f(\boldsymbol{\psi}) \left\| \frac{\partial \boldsymbol{\psi}}{\partial u} \times \frac{\partial \boldsymbol{\psi}}{\partial v} \right\| du dv$$

$$\int_V f dV = \int_w \int_v \int_u f(\boldsymbol{\phi}) \left| \frac{\partial \boldsymbol{\phi}}{\partial u} \cdot \frac{\partial \boldsymbol{\phi}}{\partial v} \times \frac{\partial \boldsymbol{\phi}}{\partial w} \right| du dv dw$$

$$\int_C \boldsymbol{F} \cdot d\boldsymbol{r} = \int_t \boldsymbol{F}(\boldsymbol{r}) \cdot \frac{d\boldsymbol{r}}{dt} dt$$

$$\int_S \boldsymbol{F} \cdot d\boldsymbol{S} = \int_v \int_u \boldsymbol{F}(\boldsymbol{\psi}) \cdot \frac{\partial \boldsymbol{\psi}}{\partial u} \times \frac{\partial \boldsymbol{\psi}}{\partial v} du dv$$

$$\int_V \boldsymbol{F} dV = \int_w \int_v \int_u \boldsymbol{F}(\boldsymbol{\phi}) \left| \frac{\partial \boldsymbol{\phi}}{\partial u} \cdot \frac{\partial \boldsymbol{\phi}}{\partial v} \times \frac{\partial \boldsymbol{\phi}}{\partial w} \right| du dv dw$$

Lecture Contents

1. Introduction
   - Module Aims and Assessment
   - Topics to be Covered
   - Reading List and References
2. Topic 1: Vector Algebra and Real-Valued Functions
   - Introduction
   - Vectors Algebra
   - Euclidean Space
   - Dot and Cross Products
   - Real-Valued Functions
3. Topic 2: Differentiation, Gradient, Divergence, Curl
   - Continuity of Multivariate Functions
   - Differentiation of Multivariate Functions
   - Gradient of a Scalar field
   - Divergence of a Vector Field
   - Curl of a Vector Field
   - Mixed Partial Derivative and Laplacian
4. Topic 3: Line, Surface, and Volume Integrals
   - Line Integrals
   - Surface Integrals
   - Volume Integrals
5. Topic 4: Integrals Theorems and Applications
   - Gauss's (Divergence) Theorem
   - Stokes' Theorem
6. Topic 1: Integers and Divisibility
   - Methods of Number Theory
   - Well-Ordering Principle and Archimedes Property
   - Polygonal Numbers
   - The Division Algorithm
   - Greatest Common Divisor
   - The Euclidean Algorithm
   - The Diophantine Equation $ax + by = c$
7. Topic 2: Primes and Their Distribution
   - Prime Numbers
   - Fundamental Theorem of Arithmetic
   - Distribution of Primes
   - Goldbach's Conjecture
   - Primes in Arithmetic Progression
8. Topic 3: The Theory of Congruences
   - Basic Properties of Congruences
   - Cancellation Rule
   - Representations of Integers
   - Linear Congruences
   - Chinese Remainder Theorem
9. Topic 4: Fermat's, Wilson's Theorems, and Number Theoretic Functions
   - Fermat's Little Theorem and Pseudoprimes
   - Wilson's Theorem
   - Number Theoretic Functions
   - Applications to RSA Cryptosystem

Intended Learning Outcomes

By the end of this session you will be able to...

1. Understand integration of scalar and vector fields.
2. Calculate line, surface, and volume integrals for real-valued functions

We can now study the integration methods for vector valued function.

Definition (Line/Path Integerals)

The **path** integral of $f(x, y, z)$ along a C^1 path $\boldsymbol{r}(t) : [a, b] \longrightarrow \mathbb{R}^3$ is defined by

$$\int_C f \, \|d\boldsymbol{r}\| = \int_a^b f(\boldsymbol{r}(t)) \left\| \frac{d\boldsymbol{r}}{dt} \right\| dt.$$

For a vector-valued function $\boldsymbol{F}(x, y, z)$, we have

$$\int_C \boldsymbol{F} \cdot d\boldsymbol{r} = \int_a^b \boldsymbol{F}(\boldsymbol{r}) \cdot \frac{d\boldsymbol{r}}{dt} dt.$$

Therefore, we evaluate f on each point of the path $\boldsymbol{r}(t)$, multiply by the infinitesimal path element $\left\| \frac{d\boldsymbol{r}}{dt} \right\|$ and then integrate.

Example

Let $f = yz$ and $\boldsymbol{F}(x, y, x) = (-y, x, 0)$ and path C be given by $\boldsymbol{r}(t) = (t, 3t, 2t)$ for $t \in [1, 3]$. Calculate the path integrals

1. $\int_C f \, \|d\boldsymbol{r}\|$,
2. $\int_C \boldsymbol{F} \cdot d\boldsymbol{r}$.

Exercise 1:

1. Let $f : \mathbb{R}^3 \longrightarrow \mathbb{R}$ and $\boldsymbol{r} : [a, b] \longrightarrow \mathbb{R}$ a path C. Compute $\int_C \nabla f \cdot d\boldsymbol{r}$.

Remark 1: Length of a Path

A path integral $\boldsymbol{r} : [a, b] \longrightarrow \mathbb{R}$ for a path C when $f = 1$ produces the length of C, that is

$$\mathcal{L}_C = \int_C \|d\boldsymbol{r}\| .$$

Definition (Surface Integerals)

The **surface** integral of $f(x, y, z)$ on a parametrised C^1 surface $\boldsymbol{\psi}(u, v) : [a, b] \times [c, d] \longrightarrow \mathbb{R}^3$ is defined by

$$\int_S f \, \|d\boldsymbol{S}\| = \int_c^d \int_a^b f(\boldsymbol{\psi}) \left\| \frac{\partial \boldsymbol{\psi}}{\partial u} \times \frac{\partial \boldsymbol{\psi}}{\partial v} \right\| du dv.$$

For a vector-valued function $\boldsymbol{F}(x, y, z)$, we have

$$\int_S \boldsymbol{F} \cdot d\boldsymbol{S} = \int_c^d \int_a^b \boldsymbol{F}(\boldsymbol{\psi}) \cdot \frac{\partial \boldsymbol{\psi}}{\partial u} \times \frac{\partial \boldsymbol{\psi}}{\partial v} du dv.$$

Example

Let $f = z^2$ and $\boldsymbol{F}(x, y, x) = (x, y, z)$ and surface S be given by $\boldsymbol{\psi}(\theta, z) = (\cos\theta, \sin\theta, z)$ for $\theta \in [0, 2\pi]$ and $z \in [-1, 1]$. Calculate the surface integrals

1. $\int_S f \, \|d\boldsymbol{S}\|$,
2. $\int_S \boldsymbol{F} \cdot d\boldsymbol{S}$.

Remark 2: Area of a Surface

A surface integral with $\boldsymbol{\psi}(u, v) : [a, b] \times [c, d] \longrightarrow \mathbb{R}^3$ for surface S when $f = 1$ produces the area of S, that is

$$\mathcal{A}_S = \int_S \|d\boldsymbol{S}\| .$$

Definition (Volume Integerals)

The **volume** integral of $f(x, y, z)$ on a parametrised C^1 volume $\boldsymbol{\phi}(u, v, w) : [a, b] \times [c, d] \times [e, f] \longrightarrow \mathbb{R}^3$ is defined by

$$\int_V f dV = \int_e^f \int_c^d \int_a^b f(\boldsymbol{\phi}) \left| \frac{\partial \boldsymbol{\phi}}{\partial u} \cdot \frac{\partial \boldsymbol{\phi}}{\partial v} \times \frac{\partial \boldsymbol{\phi}}{\partial w} \right| du dv dw.$$

For a vector-valued function $\boldsymbol{F}(x, y, z)$, we have

$$\int_V \boldsymbol{F} dV = \int_e^f \int_c^d \int_a^b \boldsymbol{F}(\boldsymbol{\phi}) \left| \frac{\partial \boldsymbol{\phi}}{\partial u} \cdot \frac{\partial \boldsymbol{\phi}}{\partial v} \times \frac{\partial \boldsymbol{\phi}}{\partial w} \right| du dv dw.$$

Example

Let $f = x + y$ and $\boldsymbol{F}(x, y, x) = (x, y, z)$ and volume V be given by $\boldsymbol{\phi}(r, \theta, z) = (r\cos\theta, r\sin\theta, z)$ for $r \in [0, 1]$, $\theta \in [0, 2\pi]$ and $z \in [-1, 1]$. Calculate the volume integrals

1. $\int_V f dV$,
2. $\int_V \boldsymbol{F} dV$.

Remark 3: Volume

A volume integral with $\boldsymbol{\phi}(u, v, w) : [a, b] \times [c, d] \times [e, f] \longrightarrow \mathbb{R}^3$ for V when $f = 1$ produces the volume of V, that is

$$\mathcal{V} = \int_V dV.$$

Summary: What we did...

- Line Integrals — $\int_C f \, \|d\boldsymbol{r}\|$ and $\int_C \boldsymbol{F} \cdot d\boldsymbol{r}$
- Surface Integrals — $\int_S f \, \|d\boldsymbol{S}\|$ and $\int_S \boldsymbol{F} \cdot d\boldsymbol{S}$
- Volume Integrals — $\int_V f \, dV$ and $\int_V \boldsymbol{F} dV$

Topic 4
Integrals Theorems and Applications

Gauss's Theorem:

$$\int_V \nabla \cdot \boldsymbol{F} dV = \int_{\partial V} \boldsymbol{F} \cdot d\boldsymbol{S}.$$

Stokes' Theorem

$$\int_S \nabla \times \boldsymbol{F} \cdot d\boldsymbol{S} = \int_{\partial S} \boldsymbol{F} \cdot d\boldsymbol{r}.$$

Lecture Contents

1. Introduction
   - Module Aims and Assessment
   - Topics to be Covered
   - Reading List and References
2. Topic 1: Vector Algebra and Real-Valued Functions
   - Introduction
   - Vectors Algebra
   - Euclidean Space
   - Dot and Cross Products
   - Real-Valued Functions
3. Topic 2: Differentiation, Gradient, Divergence, Curl
   - Continuity of Multivariate Functions
   - Differentiation of Multivariate Functions
   - Gradient of a Scalar field
   - Divergence of a Vector Field
   - Curl of a Vector Field
   - Mixed Partial Derivative and Laplacian
4. Topic 3: Line, Surface, and Volume Integrals
   - Line Integrals
   - Surface Integrals
   - Volume Integrals
5. Topic 4: Integrals Theorems and Applications
   - Gauss's (Divergence) Theorem
   - Stokes' Theorem
6. Topic 1: Integers and Divisibility
   - Methods of Number Theory
   - Well-Ordering Principle and Archimedes Property
   - Polygonal Numbers
   - The Division Algorithm
   - Greatest Common Divisor
   - The Euclidean Algorithm
   - The Diophantine Equation $ax + by = c$
7. Topic 2: Primes and Their Distribution
   - Prime Numbers
   - Fundamental Theorem of Arithmetic
   - Distribution of Primes
   - Goldbach's Conjecture
   - Primes in Arithmetic Progression
8. Topic 3: The Theory of Congruences
   - Basic Properties of Congruences
   - Cancellation Rule
   - Representations of Integers
   - Linear Congruences
   - Chinese Remainder Theorem
9. Topic 4: Fermat's, Wilson's Theorems, and Number Theoretic Functions
   - Fermat's Little Theorem and Pseudoprimes
   - Wilson's Theorem
   - Number Theoretic Functions
   - Applications to RSA Cryptosystem

Intended Learning Outcomes

By the end of this session you will be able to...

1. Learn about Stokes' and Gauss' Theorem.
2. Interchange relevant line, surface, and volume integrals using the above theorems.
3. Use integral theorems to understand physical problems.

Theorem (Gauss (Divergence))

Let $\boldsymbol{F}$ be a continuously differentiable vector field defined in a volume V. Let $S = \partial V$ be the closed surface forming the boundary of V. Then we have

$$\int_V \nabla \cdot \boldsymbol{F} dV = \int_{\partial V} \boldsymbol{F} \cdot d\boldsymbol{S}.$$

The Gauss's Theorem states that the total amount of expansion of $\boldsymbol{F}$ within the volume V is equal to the flux of $\boldsymbol{F}$ out of the surface S enclosing V.

Example

Let $\boldsymbol{F} = z^3\boldsymbol{k}$ and V be a volume given by $x^2 + y^2 + z^2 \leq 1$. Verify Gauss's Theorem, i.e., calculate the following.

1. $$\int_V \nabla \cdot \boldsymbol{F} dV$$

2. $$\int_{\partial V} \boldsymbol{F} \cdot d\boldsymbol{S}$$

Application: Conservation of Mass for a Fluid

- Consider a fluid with density $\rho(\boldsymbol{r}, t)$ flowing with velocity $\boldsymbol{u}(\boldsymbol{r}, t)$. Let V be an arbitrary volume fixed in space.
- The rate of change of mass in V is equal to the rate of mass flowing into the surface S of V

$$\frac{d}{dt}\int_V \rho dV = -\int_S \rho \boldsymbol{u} \cdot d\boldsymbol{S}.$$

- The above can be written as

$$\int_V \frac{\partial \rho}{\partial t} dV = -\int_S \rho \boldsymbol{u} \cdot d\boldsymbol{S}.$$

- Now use Gauss's Theorem on the r.h.s and since V is arbitrary we have

$$\int_V \frac{\partial \rho}{\partial t} dV = -\int_V \nabla \cdot (\rho \boldsymbol{u})\, dV \Longrightarrow \frac{\partial \rho}{\partial t} + \nabla \cdot (\rho \boldsymbol{u}) = 0.$$

Theorem (Stokes)

Let C be a closed curve which forms the boundary of a surface S. Let $\boldsymbol{F}$ be a continuously differentiable vector field defined on S. Then we have

$$\int_S \nabla \times \boldsymbol{F} \cdot d\boldsymbol{S} = \int_C \boldsymbol{F} \cdot d\boldsymbol{r}.$$

The Stokes' Theorem states that the total amount of curl of $\boldsymbol{F}$ within the surface S is equal to the rotation of $\boldsymbol{F}$ on the boundary C enclosing S.

Example

Let $\boldsymbol{F} = -y\boldsymbol{i} + x\boldsymbol{j} + z\boldsymbol{k}$ and S be a surface given by $x^2 + y^2 \leq 1$ and $z = 0$. Verify Stokes's Theorem, i.e., calculate the following.

1. $$\int_S \nabla \times \boldsymbol{F} \cdot d\boldsymbol{S}$$

2. $$\int_C \boldsymbol{F} \cdot d\boldsymbol{r}$$

Application: Amperes's Law

- Let $\boldsymbol{B}$ be the magnetic field strength and $\boldsymbol{J}$ be the current density.
- Then Amperes's Law states that

$$\int_C \boldsymbol{B} \cdot d\boldsymbol{r} = \mu_0 \int_S \boldsymbol{J} \cdot d\boldsymbol{S}$$

  for any surface S that spans the loop C for some constant of proportionality μ_0.
- Now use Stokes' Theorem on the l.h.s and since the loop was arbitrary

$$\int_S \nabla \times \boldsymbol{B} \cdot d\boldsymbol{S} = \int_S \mu_0 \boldsymbol{J} \cdot d\boldsymbol{S} \Longrightarrow \nabla \times \boldsymbol{B} = \mu_0 \boldsymbol{J}.$$

Summary: What we did...

- Gauss's Theorem: $\int_V \nabla \cdot \boldsymbol{F} dV = \int_{\partial V} \boldsymbol{F} \cdot d\boldsymbol{S}$
- Stokes' Theorem: $\int_S \nabla \times \boldsymbol{F} \cdot d\boldsymbol{S} = \int_{\partial S} \boldsymbol{F} \cdot d\boldsymbol{r}$
- Applications: Fluid Dynamics, Electromagnetism

Number Theory

Kayvan Nejabati Zenouz

University of Greenwich

April 27, 2020

"Mathematics is the queen of the sciences and number theory is the queen of mathematics"

Carl Friedrich Gauss 1777 - 1855

[1] Use these notes in conjunction with R demos accessible on https://kayvannejabati.shinyapps.io/MATH1172Demo/.

[2] Office: QM315, Email: K.NejabatiZenouz@greenwich.ac.uk, Student Drop-in Hours: MONDAYS 12:00-13:00 (MATHS ARCADE) AND TUESDAYS 15:00-16:00 (QM315)

Topic 1
Introduction, Integers and Divisibility

Pell's Equation

$$x^2 - Ny^2 = 1$$

Fermat's Last Theorem

$$x^n + y^n = z^n$$

Lecture Contents

1. Introduction
   - Module Aims and Assessment
   - Topics to be Covered
   - Reading List and References
2. Topic 1: Vector Algebra and Real-Valued Functions
   - Introduction
   - Vectors Algebra
   - Euclidean Space
   - Dot and Cross Products
   - Real-Valued Functions
3. Topic 2: Differentiation, Gradient, Divergence, Curl
   - Continuity of Multivariate Functions
   - Differentiation of Multivariate Functions
   - Gradient of a Scalar field
   - Divergence of a Vector Field
   - Curl of a Vector Field
   - Mixed Partial Derivative and Laplacian
4. Topic 3: Line, Surface, and Volume Integrals
   - Line Integrals
   - Surface Integrals
   - Volume Integrals
5. Topic 4: Integrals Theorems and Applications
   - Gauss's (Divergence) Theorem
   - Stokes' Theorem
6. Topic 1: Integers and Divisibility
   - Methods of Number Theory
   - Well-Ordering Principle and Archimedes Property
   - Polygonal Numbers
   - The Division Algorithm
   - Greatest Common Divisor
   - The Euclidean Algorithm
   - The Diophantine Equation $ax + by = c$
7. Topic 2: Primes and Their Distribution
   - Prime Numbers
   - Fundamental Theorem of Arithmetic
   - Distribution of Primes
   - Goldbach's Conjecture
   - Primes in Arithmetic Progression
8. Topic 3: The Theory of Congruences
   - Basic Properties of Congruences
   - Cancellation Rule
   - Representations of Integers
   - Linear Congruences
   - Chinese Remainder Theorem
9. Topic 4: Fermat's, Wilson's Theorems, and Number Theoretic Functions
   - Fermat's Little Theorem and Pseudoprimes
   - Wilson's Theorem
   - Number Theoretic Functions
   - Applications to RSA Cryptosystem

Intended Learning Outcomes

By the end of this session you will be able to...

1. Learn about integers, number theory, and its application.
2. Understand methods of proof in number theory and apply them to solve problems.
3. Learn about and apply the division algorithm to solve problems.
4. Prove rules governing divisibility of integers.
5. Understand and apply the Euclidean Algorithm to solve problems relating to greatest common divisor.
6. Solve linear Diophantine equation.

Number Theory

Is concerned with **properties** of **integers**, **prime numbers**

$$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\},$$

integer solution of equations, and **integer-valued** functions.

- Is the **second** large field of mathematics and one of the most **beautiful** topics of science.
- In **vector calculus** part we were concerned with functions and equations over $\mathbb{R}$,

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

We move in the number chain to $\mathbb{N}$ and $\mathbb{Z}$.

Applications

It is fundamental in cryptography, for example every financial transaction made, with its role in **public-key cryptosystem**.

History

- **Pythagoreans 569 B.C.** Pythagorean triples, irrationality of $\sqrt{2}$.

Numbers rule the universe.

- **Euclid 300 B.C.** Euclidean algorithm and prime factorisation.
- **Diophantus 250 A.D.** Equations for which integers solutions are sought.
- **Fibonacci 1180**, Fibonacci sequence.
- **Pierre de Fermat 1601**, Fermat's theorems.
- **Leonard Euler 1601**, Euler's ϕ function.
- **John Wilson 1741**, Wilson's Theorem.
- **Carl Friedrich Gauss 1777**, Disquisitiones Arithmeticae.
- **Helene (Hel) Braun 1914**, **Andrew Wiles 1953**...

Methods of Number Theory

- **Observe** properties of integers and construct **proofs**, rational arguments, for why these properties exist.
- There are many **methods** of proof:
  - Direct
  - Mathematical induction
  - Contradiction
  - Contraposition
  - Construction
  - Exhaustion
  - Nonconstructive
  - Probabilistic, etc...
- The work flow of number theory is to **observe** a pattern, play with some **examples** to understand the phenomena, and **create** a proof.

Direct Proof

The conclusion is established by logically **combining** the **axioms**.

Example

For example, prove if n is odd, then n^2 is odd.

Proof by Contradiction

It is shown that if some statement is assumed true, a logical contradiction occurs, hence the statement must be false.

Example

For example, prove $\sqrt{2}$ is irrational.

- We work with

$$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$$

- We call integers of the form $n = 2k$ are called **even** and integers of the form $n = 2k + 1$ are called **odd**.

Well-Ordering Principle and Archimedes Property

One of the principle governing integers is the **well-ordering**, which plays an important role in may proofs.

Well-Ordering Principle (WOP)

Every nonempty set S of nonnegative integers contains a least element; that is, there is some integer a in S such that $a \leq b$ for all b's belonging to S.

For example, a consequence of this principle is the following.

Theorem (Archimedes Property)

If a and b are any positive integers, then there exists a positive integer n such that $na \geq b$.

Proof.

Sketch. Proof by contradiction. Assume no such n exists. Consider the set $S = \{b - na \mid n > 0\}$. It has a least element by WOP. But you can find a smaller element. □

Theorem (Mathematical Induction)

Let S be a set of positive integers with the following properties:

(a) *The integer 1 belongs to S.*

(b) *Whenever k is in S, the next integer $k+1$ must be in S.*

Then S is the set of positive integers.

Proof.

This is a consequence of WOP. □

Example

For example, prove for any $n > 0$

$$1 + 2 + 2^2 + \cdots + 2^{n-1} = 2^n - 1.$$

Polygonal Numbers

- The polygonal numbers, which were studied by the Pythagoreans. The are obtained by arranging dots in regular polygons.
- For example, Each of the numbers

$$1 = 1,\ 2 = 1 + 2,\ 6 = 1 + 2 + 3,\ 10 = 1 + 2 + 3 + 4, \cdots$$

  represents the number of dots that can be arranged evenly in an equilateral triangle.
- This led the ancient Greeks to call a number triangular if it is the sum of consecutive integers, beginning with 1.

Exercise 1: Triangular Numbers

Prove the following facts concerning triangular numbers.

1. A number is triangular if and only if it is of the form

$$\frac{n(n+1)}{2}$$

   for some $n > 0$. (Pythagoras, circa 550 B.C.)
2. The integer n is a triangular number if and only if $8n + 1$ is a perfect square. (Plutarch, circa 100 A.D.)
3. The sum of any two consecutive triangular numbers is a perfect square. (Nicomachus, circa 100 A.D.)
4. If n is a triangular number, then so are $9n + 1$, $25n + 3$, and $49n + 6$. (Euler, 1775)

Theorem (Division Algorithm)

Given integers a and b, with $b > 0$, there exists unique q and r satisfying

$$a = qb + r, \ 0 \leq r < b.$$

Proof.

Sketch. Consider the set $S = \{a - xb \mid x \in \mathbb{Z}, \ a - xb \geq 0\}$. Show it is non-empty. Then by WOP it has a smallest element, say r for which there exists a q with $a - xb = r$. Argue $r < b$ by contradiction. Show r and q are unique. □

Example

For example if $a = 13$ and $b = 5$ we have $12 = 2 \times 5 + 3$, i.e., $q = 2$ and $r = 3$. Find r and q for $a = 131$ and $b = 6$.

Exercise 2: Consequence of Division Algorithm

Proposition

Square of any odd integer is of the form $8k + 1$.

Proof.

Let n be any integer. As a consequence of division algorithm we can write $n = 4k + r$ for unique integers $0 \leq r < 4$ and k. Now if n is odd, we must have $r = 1, 3$. Now squaring n, we have

$$n^2 = 16k^2 + 8r + r^2.$$

If $r = 1$, we have

$$n^2 = 8\left(2k^2 + 1\right) + 1,$$

and if $r = 3$, we have

$$n^2 = 16k^2 + 8r + 9 = 8\left(2k^2 + 3 + 1\right) + 1.$$

□

Definition (Divisibility)

An integer b is said to be **divisible** by an integer $a \neq 0$, in symbols $a \mid b$, if there exists some integer c such that $b = ac$. We write $a \nmid b$ to indicate that b is not divisible by a.

Example

We have that $2 \mid 4$ because $4 = 2 \times 2$ or $-3 \mid 12$ because $12 = 4 \times -3$, but $5 \nmid 7$.

Theorem

For integers a, b, c, the following hold.

1. $a \mid 0$, $1 \mid a$, *and* $a \mid a$.
2. $a \mid 1$ *if and only if* $a = \pm 1$.
3. *If* $a \mid b$ *and* $c \mid d$, *then* $ac \mid bd$.
4. *If* $a \mid b$ *and* $b \mid c$, *then* $a \mid c$.
5. *If* $a \mid b$ *and* $b \mid a$, *then* $a = \pm b$.
6. *If* $a \mid b$ *and* $b \neq 0$, *then* $|a| \leq |b|$.
7. *If* $a \mid b$ *and* $a \mid c$, *then* $a \mid (bx + cy)$ *for any two integers* x *and* y.

Definition (Greatest Common Divisor)

Let a and b be given integers, with at least one of them different from zero. The greatest common divisor of a and b, denoted by $\gcd(a, b)$, is the positive integer d satisfying the following.

1. $d \mid a$ and $d \mid b$.
2. If $c \mid a$ and $c \mid b$, then $c \leq d$.

Example

The greatest common divisor of -12 and 30 is 6.

Exercise 3: Greatest Common Divisor

Find $\gcd(8, 17)$, $\gcd(-8, 36)$, $\gcd(252, 98)$.

The following is an important and useful result.

Theorem

Given integers a and b, not both of which are zero, there exist integers x and y such that

$$\gcd(a, b) = ax + by.$$

Example

We have $\gcd(8, 17) = -2 \times 8 + 1 \times 17$.

Remark 1: Algorithm for gcd

We will soon see an algorithm on how to compute $\gcd(a, b)$ and x, y such that $\gcd(a, b) = ax + by$.

Relatively Prime Integers

Definition (Relatively Prime Integers)

Two integers a and b, not both of which are zero, are said to be relatively prime whenever $gcd(a, b) = 1$.

Example

We have $\gcd(8, 17) = 1$, so 8 and 17 are relatively prime.

Theorem

Let a and b be integers, not both zero. Then a and b are relatively prime if and only if there exist integers x and y such that $1 = ax + by$.

Corollary

- If $d = \gcd(a, b)$, then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.
- If $a \mid c$ and $b \mid c$, with $\gcd(a, b) = 1$, then $ab \mid c$.

Theorem (Euclid's lemma)

If $a \mid bc$, *with* $\gcd(a, b) = 1$, *then* $a \mid c$.

Proof.

Let a, b, and c be integers and suppose $a \mid bc$ and $\gcd(a, b) = 1$. By theorem on slide 55 we can find x and y so that

$$1 = ax + by.$$

Multiplying both sides by c we have

$$c = acx + bcy,$$

since $a \mid bc$, we have that $bc = am$ for some integer m, so

$$c = a\left(cx + my\right),$$

which implies that $a \mid c$ as required. □

The Euclidean Algorithm

- The **greatest common divisor** of two integers can be found by listing all their positive divisors and choosing the largest one common to each.
- A more efficient process, involving repeated application of the Division Algorithm, known as **Euclidean Algorithm** is usually used.

The Euclidean Algorithm Method

The Euclidean Algorithm may be described as follows.

- Let a and b be two integers whose greatest common divisor is desired and assume $a \geq b \geq 0$.
- Apply the Division Algorithm to a and b

$$a = q_1 b + r_1, \ 0 \leq r_1 < b.$$

  If $r_1 = 0$, then $\gcd(a, b) = b$.
- If $r_1 \neq 0$, Division Algorithm to b and r_1

$$b = q_2 r_1 + r_2, \ 0 \leq r_2 < r_1.$$

  If $r_2 = 0$, then $\gcd(a, b) = r_1$.
- If $r_2 \neq 0$, Division Algorithm to r_1 and r_2

$$r_1 = q_3 r_2 + r_3, \ 0 \leq r_3 < r_2.$$

  Again check if $r_2 \neq 0$, repeat the process with r_2 and r_3.
- This generates $b > r_1 > r_2 > \cdots > r_n \geq 0$. repeat the process until first n with $r_{n+1} = 0$. Then $\gcd(a, b) = r_n$.

Example

Using the Euclidean algorithm calculate the greatest common divisor of 843 and 165. **Solution.** Use the Euclidean algorithm

$$843 = 5 \times 165 + 18$$
$$165 = 9 \times 18 + 3$$
$$18 = 3 \times 6 + 0.$$

Therefore, we have $\gcd(843, 165) = 3$.

Exercise 4: Euclidean Algorithm

Using the Euclidean algorithm to find $\gcd(17, 8)$, $\gcd(36, 8)$, $\gcd(252, 98)$.

The reason the Euclidean algorithm works is as follows.

Lemma

If a and b are positive integers and $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

Using the result of this lemma, we simply work down the displayed system of equations, obtaining

$$\begin{aligned}\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots \\ = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n\end{aligned}$$

Find x, y for $\gcd(a, b) = ax + by$

Recall Theorem on slide 51 mentioned that given integers a and b, not both of which are zero, there exist integers x and y such that

$$\gcd(a, b) = ax + by.$$

We can reverse the Euclidean algorithm to find x, y as follows.

- Write
$$r_n = r_{n-2} + q_n r_{n-1}$$
- Use $r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}$ to get
$$\begin{aligned} r_n &= r_{n-2} + q_n \left(r_{n-3} - q_{n-1} r_{n-2}\right) \\ &= r_{n-2} \left(1 - q_n q_{n-1}\right) + q_n r_{n-3} \end{aligned}$$
- Write $r_{n-2} = r_{n-4} - q_{n-2} r_{n-3}$ and continue to arrive at a and b.

Example

Find integers x and y so that $\gcd(165, 843) = 165x + 843y$.

Solution. Now working backwards we have

$$\begin{aligned} 3 &= 165 - 9 \times 18 \\ &= 165 - 9 \times (843 - 5 \times 165) \\ &= 46 \times 165 - 9 \times 843 \end{aligned}$$

so we have

$$3 = 46 \times 165 - 9 \times 843,$$

i.e., $x = 46$ and $y = -9$.

Exercise 5: Extended Euclidean Algorithm

Find integers x and y so that $\gcd(6, 152) = 6x + 152y$.

The Diophantine Equation $ax + by = c$

- **Diophantine equation** refers to any equation in one or more unknowns that is to be solved in the **integers**.
- The **simplest** type of Diophantine equation is

$$ax + by = c$$

where a, b, c are given integers and a and b are not both zero.

- A **solution** of this equation is a pair of integers x_0, y_0 that, when substituted into the equation, satisfy it; that is, we ask that $ax_0 + by_0 = c$.
- We can have **several** solutions. For example, given $3x + 6y = 18$ we have

$$3 \times 4 + 6 \times 1 = 18.$$
$$3 \times -6 + 6 \times 8 = 18.$$

Theorem

The linear Diophantine equation $ax + by = c$ *has a solution if and only if* $d \mid c$, *where* $d = \gcd(a, b)$. *If* x_0, y_0 *is any particular solution of this equation, then all other solutions are given by*

$$x = x_0 + \frac{b}{d}t, \; y = y_0 - \frac{a}{d}t,$$

where t *is an arbitrary integer.*

Example

Find all integer solutions to the equation $5x + 22y = 18$.

Solution. Note the equation has a solution if and only if $\gcd(5, 22) = 1$ divides 18, which is the case. Apply the extended Euclidean algorithm to $\gcd(5, 22)$. First we have

$$\begin{aligned} 22 &= 4 \times 5 + 2 \\ 5 &= 2 \times 2 + 1, \text{ so} \\ 1 &= 5 - 2 \times 2 \\ &= 5 - 2 \times (22 - 4 \times 5) \\ &= 9 \times 5 - 2 \times 22, \end{aligned}$$

therefore, we have $1 = 9 \times 5 - 2 \times 22$. Now multiplying both sides by 18, we have $18 = 18 \times 9 \times 5 - 18 \times 2 \times 22$ and we have that

$$x_0 = 18 \times 9 = 162, \ y_0 = -18 \times 2 = -36$$

i.e., $5 \times 162 - 22 \times 36 = 18$. All other solutions are given by

$$x = x_0 + 22t = 162 + 22t, \ y = y_0 - 5t = -36 - 5t \text{ for } t \in \mathbb{Z}.$$

Exercise 6: Diophantine Equation

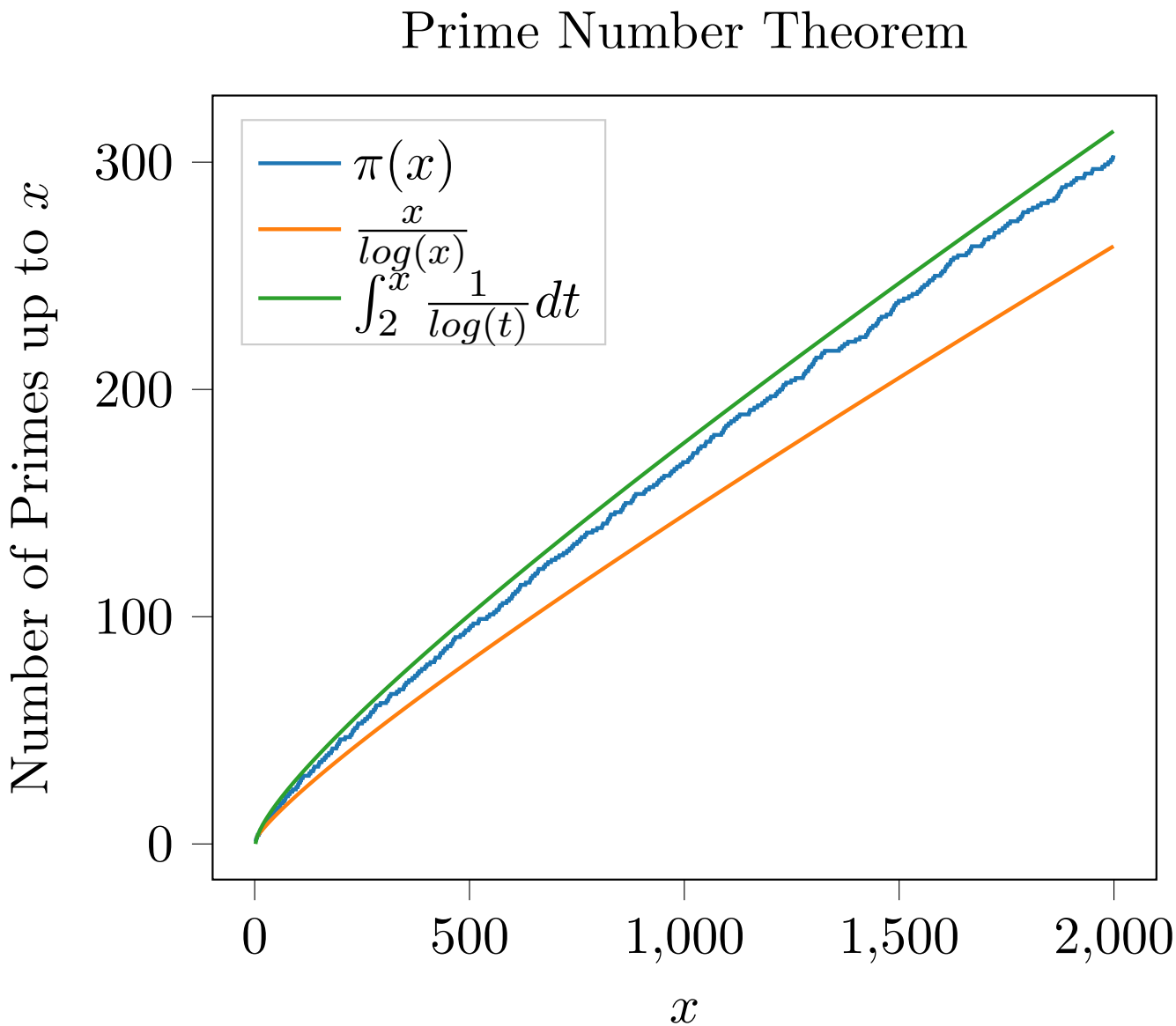
- Find solutions of the linear Diophantine equation

$$172x + 20y = 1000.$$

Summary: What we did...

- Number Theory
  - Integers, integer-valued functions, applications
- Methods of Proof
  - Direct, Induction, Contradiction, WOP
- Divisibility
  - Rules, gcd, relatively primes
- Euclidean Algorithm
  - Diophantine equation
- Next Time
  - Primes and unique factorisation

Topic 2
Primes and Their Distribution



Lecture Contents

1. Introduction
   - Module Aims and Assessment
   - Topics to be Covered
   - Reading List and References
2. Topic 1: Vector Algebra and Real-Valued Functions
   - Introduction
   - Vectors Algebra
   - Euclidean Space
   - Dot and Cross Products
   - Real-Valued Functions
3. Topic 2: Differentiation, Gradient, Divergence, Curl
   - Continuity of Multivariate Functions
   - Differentiation of Multivariate Functions
   - Gradient of a Scalar field
   - Divergence of a Vector Field
   - Curl of a Vector Field
   - Mixed Partial Derivative and Laplacian
4. Topic 3: Line, Surface, and Volume Integrals
   - Line Integrals
   - Surface Integrals
   - Volume Integrals
5. Topic 4: Integrals Theorems and Applications
   - Gauss's (Divergence) Theorem
   - Stokes' Theorem
6. Topic 1: Integers and Divisibility
   - Methods of Number Theory
   - Well-Ordering Principle and Archimedes Property
   - Polygonal Numbers
   - The Division Algorithm
   - Greatest Common Divisor
   - The Euclidean Algorithm
   - The Diophantine Equation $ax + by = c$
7. Topic 2: Primes and Their Distribution
   - Prime Numbers
   - Fundamental Theorem of Arithmetic
   - Distribution of Primes
   - Goldbach's Conjecture
   - Primes in Arithmetic Progression
8. Topic 3: The Theory of Congruences
   - Basic Properties of Congruences
   - Cancellation Rule
   - Representations of Integers
   - Linear Congruences
   - Chinese Remainder Theorem
9. Topic 4: Fermat's, Wilson's Theorems, and Number Theoretic Functions
   - Fermat's Little Theorem and Pseudoprimes
   - Wilson's Theorem
   - Number Theoretic Functions
   - Applications to RSA Cryptosystem

Intended Learning Outcomes

By the end of this session you will be able to...

1. Learn about prime numbers and their properties.
2. Understand the Fundamental Theorem of Arithmetic.
3. Determine if a number is prime and factorise integers.
4. Prove theorems about the distribution of primes.
5. Learn about unsolved problems relating to distribution of primes.

Prime Numbers

- In the previous topic we learnt that for any two integers a and $b \neq 0$, we can find unique q and r such that

$$a = bq + r, \ 0 \leq r < b.$$

- For the when $r = 0$, we say that b divides a and write $b \mid a$.
- We looked at common divisor of two integers a and b.
- Now we focus on integers which have only two divisor.

Definition (Prime Number)

An integer $p > 1$ is called a **prime number**, or simply a prime, if its only positive divisors are 1 and p. An integer greater than 1 that is not a prime is termed **composite**.

Example

The integers $2, 3, 5, 7$ are prime and $1, 4, 6, 8, 9$ are composite.

Applications

- It turns out every number $a > 1$ is either a prime or, by the *Fundamental Theorem*, can be broken down into unique prime factors and no further
- The primes serve as the building blocks from which all other integers can be made.
- The distribution of primes remains unknown for example see Riemann-Hypothesis.
- We will first proceed to show that every number can be written as a product of primes

Theorem

If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof.

Sketch. Use Euclid's Lemma. □

Corollary 1

If p is a prime and $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_k$ for some k, where $1 \leq k \leq n$.

Proof.

Exercise. Use Induction and theorem above. □

Corollary 2

If $p, q_1 q_2 \cdots q_n$ are a prime numbers and $p \mid q_1 q_2 \cdots q_n$, then $p = q_k$ for some k, where $1 \leq k \leq n$.

Proof.

Exercise. Use Corollary 1. □

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer $n > 1$ is either a prime or a product of primes; this representation is unique, apart from the order in which the factors occur.

Proof.

Sketch. Steps:

1. n is either prime or composite. If prime done.
2. If n composite, choose d, smallest divisor of n, it must be prime $d = p_1$.
3. Write $n = p_1 n_1$ and find divisors of $n_1 < n$.
4. Repeat until $n = p_1 p_2 \cdots p_r$, is a product of primes.
5. To establish uniqueness, assume $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, and show p_i and q_j coincide and $r = s$.

□

Corollary

Any positive integer $n > 1$ can be written uniquely in a canonical form

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

where, for $i = 1, 2, ..., r$, each k_i is a positive integer and each p_i is a prime, with $p_1 < p_2 < \cdots < p_r$.

Exercise 1: Factorisation

Factorise the following numbers.

$$360, 17460, 18527$$

Remark 1: Finding gcd

Note using the prime factorisations of two numbers, it is easy to find the greatest common divisors of two integers a and b. If

$$a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \text{ and } b = p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r},$$

where k_i and l_j can be zero, then

$$\gcd(a, b) = p_1^{\min(k_1, l_1)} p_2^{\min(k_2, l_2)} \cdots p_r^{\min(k_r, l_r)}.$$

Exercise 2: Finding gcd

Find $\gcd(4725, 17460)$ using the prime factorisations of 4725 and 17460.

Primality Testing

- Given a particular integer, how can we determine whether it is prime or composite?
- Approach by successively dividing the integer in question by each of the numbers preceding it.
- Not practical: for even if one is undaunted by large calculations, the amount of time and work involved may be prohibitive.

Lemma

If $n > 1$ is a composite integer, then n possess a divisor less than or equal to $\sqrt{n}$.

- In testing the primality of an integer $n > 1$, it therefore suffices to divide a by those primes not exceeding $\sqrt{n}$.

Example

Check the primality of 509.

The Sieve of Eratosthenes

- Eratosthenes of Cyrene (276-194 B.C.), known as "Beta" because, it was said, he stood at least second in every field.
- Recall if an integer $a > 1$ is not divisible by any prime $p < \sqrt{a}$, then a is of necessity a prime.
- Eratosthenes used this fact as the basis of a clever technique, called the Sieve of Eratosthenes, for finding all primes below a given integer n.
- Write down the integers from 2 to n in their natural order.
- Systematically eliminating all the composite numbers by striking out all multiples $2p, 3p, 4p, 5p, ...$ of the primes $p < \sqrt{n}$.
- The integers that are left on the list, those that do not fall through the "sieve", are primes.

Theorem (Euclid)

There is an infinite number of primes.

Proof.

- Proceed by contradiction. Suppose there are finitely many primes $p_1 = 2, p_2 = 3, ..., p_n$ arranged in ascending order.
- Consider the number $P = p_1 p_2 \cdots p_n + 1$.
- Now since $P > 1$, by Fundamental Theorem of Arithmetic, P is either prime or product of primes, i.e., P is divisible by some prime p.
- Since $p_1 = 2, p_2 = 3, ..., p_n$, we must have that $p = p_i$ for some $i = 1, ..., n$.
- But this implies that $p \mid P - p_1 p_2 \cdots p_n$, i.e., $p \mid 1$ and since $p > 1$, this leads to a contradiction, thus the assumption that the list of primes is finite is incorrect.

□

Size of Primes

Lemma

Let p_n be denote the nth of the prime numbers in their natural order. Then

$$p_{n+1} \leq p_1 p_2 \cdots p_n + 1.$$

Proof.

Consider a divisor p of $p_1 p_2 \cdots p_n + 1$. Then $p \neq p_i$ for $i = 1, ..., n$, so possibilities are $p = p_{n+1}, p_{n+2}, ...$, i.e., $p \geq p_{n+1}$. □

Theorem

If p_n is the nth of the prime, then $p_n \leq 2^{2^{n-1}}$.

Proof.

By induction on n and using Lemma. □

Corollary

For $n \geq 1$ there are at least $n + 1$ primes less than $2^{2^{n-1}}$.

More on Distribution of Primes

- The **distribution of primes** within the positive integers is most **mystifying**.
- It is an **unanswered** question whether there are infinitely many pairs of **twin primes**; that is, pairs of successive odd integers p and $p+2$ that are both primes.
- Electronic **computers** have discovered 152891 pairs of twin primes less than 30000000.
- The largest twins to date, each 100355 digits long,

$$65516468355 \times 2^{333333} \pm 1$$

  were discovered in 2009.
- Primes can be far apart; that is, arbitrarily **large gaps** can occur between consecutive primes.
- Given any positive integer n, there exist n consecutive integers, all of which are composite.

Conjecture (1742, Christian Goldbach)

Every even integer greater than 4 can be expressed as the sum of two primes.

- One of the **oldest** and best-known unsolved **problems** in number theory and all of mathematics.
- Some **progress** was made after 200 years by Hardy and Littlewood in 1922.
- Every even integer from some point on is the sum of either two or four primes.
- Thus, it is enough to answer the question for every odd integer n in the range $9 < n < 10^{1346}$, but 10^{1346} is **too large** for computers to handle.

Primes in Arithmetic Progression

- Recall according to the **Division Algorithm**, every positive integer can be written uniquely in one of the forms

$$4n,\ 4n+1,\ 4n+2,\ 4n+3.$$

- Therefore, every odd prime is of the form $4n+1$, for example $5, 13$, or $4n+3$ for example $7, 11$.
- In 1853, Tchebycheff **thought** there are more primes of the form $4n+3$ than $4n+1$.
- However, in 1914, J. E. Littlewood showed that the inequality **fails** infinitely often.

Primes of the Form $4n + 3$

Lemma

The product of two or more integers of the form $4n + 1$ is of the same form.

Theorem

There are an infinite number of primes of the form $4n + 3$.

Proof.

Sketch. Proof by contradiction using similar ideas to proving there are infinitely many primes and the lemma above. □

Theorem (Dirichlet 1837)

If a *and* b *are relatively prime positive integers, then the arithmetic progression* $a, a + b, a + 2b, a + 3b, \ldots$ *contains infinitely many primes.*

Proof.

Too difficult! □

Summary: What we did...

- Prime Numbers
  - Definition, Fundamental Theorem of Arithmetic
- Primality Testing
  - The Sieve of Eratosthenes
- Distribution of Primes
  - Euclid's Theorem, Twin Primes, Goldbach's Conjecture
- Arithmetic Progression
  - Pirmes of the form $4n + 3$, Dirichlet' Theorem
- Next Time
  - The Theory of Congruences

Topic 3
The Theory of Congruences

$$\begin{aligned} x &\equiv a_1 \mod n_1, \\ x &\equiv a_2 \mod n_2, \\ &\vdots \\ x &\equiv a_r \mod n_r. \end{aligned}$$

Lecture Contents

1. Introduction
   - Module Aims and Assessment
   - Topics to be Covered
   - Reading List and References
2. Topic 1: Vector Algebra and Real-Valued Functions
   - Introduction
   - Vectors Algebra
   - Euclidean Space
   - Dot and Cross Products
   - Real-Valued Functions
3. Topic 2: Differentiation, Gradient, Divergence, Curl
   - Continuity of Multivariate Functions
   - Differentiation of Multivariate Functions
   - Gradient of a Scalar field
   - Divergence of a Vector Field
   - Curl of a Vector Field
   - Mixed Partial Derivative and Laplacian
4. Topic 3: Line, Surface, and Volume Integrals
   - Line Integrals
   - Surface Integrals
   - Volume Integrals
5. Topic 4: Integrals Theorems and Applications
   - Gauss's (Divergence) Theorem
   - Stokes' Theorem
6. Topic 1: Integers and Divisibility
   - Methods of Number Theory
   - Well-Ordering Principle and Archimedes Property
   - Polygonal Numbers
   - The Division Algorithm
   - Greatest Common Divisor
   - The Euclidean Algorithm
   - The Diophantine Equation $ax + by = c$
7. Topic 2: Primes and Their Distribution
   - Prime Numbers
   - Fundamental Theorem of Arithmetic
   - Distribution of Primes
   - Goldbach's Conjecture
   - Primes in Arithmetic Progression
8. Topic 3: The Theory of Congruences
   - Basic Properties of Congruences
   - Cancellation Rule
   - Representations of Integers
   - Linear Congruences
   - Chinese Remainder Theorem
9. Topic 4: Fermat's, Wilson's Theorems, and Number Theoretic Functions
   - Fermat's Little Theorem and Pseudoprimes
   - Wilson's Theorem
   - Number Theoretic Functions
   - Applications to RSA Cryptosystem

Intended Learning Outcomes

By the end of this session you will be able to...

1. Learn about congruences and their properties.
2. Construct proofs for divisibility of numbers using congruences.
3. Solve linear congruences equations.
4. Understand the Chinese Remainder Theorem

Introduction

- **Recall** that for any integer a and $b \neq 0$, we can find unique q and r such that
$$a = bq + r,\ 0 \leq r < b.$$
- The **Theory of Congruences** is concerned with arithmetic of **remainders**.
- i.e., fixing a number n and considering the remainder of integers upon division by n.
- First **introduced** by the German mathematician **Carl Friedrich Gauss** (1777-1855) in his *Disquisitiones Arithmeticae*
- It is the **foundation** of many later developments in **pure mathematics**.

> *"It is really astonishing,"* said Kronecker, *"to think that a single man of such young years was able to bring to light such a wealth of results, and above all to present such a profound and well-organized treatment of an entirely new discipline".*

Definition (Congruent Modulo n)

Let n be a fixed positive integer. Two integers a and b are said to be congruent modulo n, symbolized by

$$a \equiv b \mod n,$$

if n divides the difference $a - b$; that is $a - b = kn$ for some integer k.

Example

For $n = 7$ we have

$$3 \equiv 24 \mod 7, \ -31 \equiv 11 \mod 7, \ -15 \equiv -64 \mod 7.$$

For $n = 10$, we have

$$11 \equiv 1 \mod 10, \ 5 \not\equiv 4 \mod 10.$$

Basic Properties of Congruences II

- Let us fix n. Now for **any integer** a we can **write** $a = qn + r$ for a **unique** integer $0 \leq r < n$, i.e., $a - r = qn$.
- This implies that any integer is **congruent** to a **unique** number $0 \leq r < n$ modulo n, i.e.,

$$a \equiv r \mod n.$$

- we see that every integer is congruent modulo n to exactly one of the values $0, 1, 2, ..., n-1$.
- In particular, $a \equiv 0 \mod n$ if and only if $n \mid a$.
- The set of integers $0, 1, 2, ..., n-1$ is called the set of **least nonnegative residues modulo n**.
- Congruence may be viewed as a **generalized** form of equality: its behaviour with respect to addition and multiplication is reminiscent of ordinary equality.

Theorem

For arbitrary integers a and b, $a \equiv b \mod n$ if and only if a and b leave the same nonnegative remainder when divided by n.

Proof.

Exercise. □

Theorem

Let $n > 1$ be fixed and a, b, c, d be arbitrary integers. Then the following properties hold.

Equivalence Relation

1. $a \equiv a \mod n$
2. *If* $a \equiv b \mod n$, *then* $b \equiv a \mod n$
3. *If* $a \equiv b \mod n$ *and* $b \equiv c \mod n$, *then* $a \equiv c \mod n$

Operation Axioms

4. *If* $a \equiv b \mod n$ *and* $c \equiv d \mod n$, *then* $a + c \equiv b + d \mod n$
5. *If* $a \equiv b \mod n$ *and* $c \equiv d \mod n$, *then* $ac \equiv bd \mod n$
6. *If* $a \equiv b \mod n$, *then* $a + c \equiv b + c \mod n$ *and* $ac = bc \mod n$
7. *If* $a \equiv b \mod n$ *then* $a^k \equiv b^k \mod n$

Remark 1: Algebraic Ring

The set of residues modulo n form an algebraic object known as a **ring** denoted by $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$. That is $\mathbb{Z}/n\mathbb{Z}$ is a set with operations $+$ and $\cdot$ such that $(\mathbb{Z}/n\mathbb{Z}, +)$ is an **abelian group**, multiplication is **associative** and **distributes** over addition, and there exists a **multiplicative identity** $1 \mod n$.

Example

Prove $3^{21}+1$ is divisible by 7.

Solution. Note we have $3^2 = 9 \equiv 2 \mod 7$, so

$$3^{21} = 3 \times \left(3^2\right)^{10} \equiv 3 \times 2^{10} \mod 7.$$

Now $2^3 = 8 \equiv 1 \mod 7$, so

$$3 \times 2^{10} = 3 \times 2 \times \left(2^3\right)^3 \equiv 6 \times 1^3 \equiv -1 \mod 7,$$

therefore we have

$$3^{21} \equiv -1 \mod 7,$$

i.e, $3^{21}+1 \equiv 0 \mod 7$.

Exercise 1: Congruences

Find the residue of 3^{20} modulo 41.

Cancellation Rule

- Note if $a \equiv b \mod n$, then $ac \equiv bc \mod n$ for any c.
- However, the converse is not always true, i.e, if $ac \equiv bc \mod n$, then we cannot always say $a \equiv b$.
- For example, $2 \times 4 \equiv 2 \times 1 \mod 6$, but $4 \not\equiv 1 \mod 6$.

Theorem (Cancellation Rule)

If $ca \equiv cb \mod n$, *then* $a \equiv b \mod n/d$, *where* $d = \gcd(c, n)$.

Proof.

If $ca \equiv cb \mod n$, then $c(a-b) = kn$ for some k. Let $d = \gcd(c, n)$. Then $c = dr$ and$n = ds$ for r, s relatively prime. We have $dr(a-b) = kds$, thus by Euclid's lemma $s \mid (a-b)$. □

Corollaries

1. If $ca \equiv cb \mod n$ and $\gcd(c, n) = 1$, then $a \equiv b \mod n$.
2. If $ca \equiv cb \mod p$ and $p \nmid c$, then $a \equiv b \mod p$, where p is a prime number.

Application: Representations of Integers

- One application of congruence theory involves finding special criteria under which a given integer is divisible by another integer.
- Given an integer $b > 1$, any positive integer N can be written uniquely in terms of powers of b as

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0,$$

with $0 \leq a_k \leq b - 1$.

- This also may be replaced by the simpler symbol

$$N = (a_m a_{m-1} \cdots a_2 a_1 a_0)_b \,.$$

Theorem

A number $N = (a_m a_{m-1} \cdots a_2 a_1 a_0)_{10}$ *is divisible by* 11 *if and only if the alternating sum of its digits is divisible by* 11, *i.e,*

$$(-1)^m a_m + (-1)^{m-1} a_{m-1} \cdots + a_2 - a_1 + a_0 \equiv 0 \mod 11.$$

Linear Congruences

- Linear Congruences are concerned with solving **linear equations** modulo n.
- That given a, b, n find x so that

$$ax \equiv b \mod n.$$

- For example, consider the equation $3x \equiv 9 \mod 12$.
- Note, if x_0 is a solution, then it means that we have

$$n \mid ax_0 - b \Longrightarrow ax_0 - b = ny \text{ for some } y.$$

- Now this is a Diophantine equation

$$ax - ny = b,$$

which we know has a solution if and only if $\gcd(a, n) \mid b$.

Theorem

The linear congruence $ax \equiv b \mod n$ *has a solution if and only if* $d \mid b$, *where* $d = \gcd(a, n)$. *If* $d \mid b$, *then it has* d *mutually incongruent solutions modulo* n *given by*

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, ..., x_0 + \frac{(d-1)n}{d}.$$

Corollary

If $\gcd(a, n) = 1$, then the linear congruence $ax \equiv b \mod n$ has a unique solution modulo n.

Remark 2: Multiplicative Inverse

Given relatively prime integers a and n, the congruence $ax \equiv 1 \mod n$ has a unique solution. This solution is sometimes called the (multiplicative) inverse of a modulo n.

Example

Solve the congruence equation $18x \equiv 30 \mod 42$.

Solution. Note, $\gcd(18, 42) = 6$ divides 30, so we have 6 solutions. Now $42 = 2 \times 18 + 6$, so multiplying both side by -5 we have

$$-5 \times 42 = -10 \times 18 - 30,$$

i.e, $18 \times -10 \equiv 18 \times (42 - 10) \equiv 30 \mod 42.$, other solutions are given by

$$32 + t\left(\frac{42}{6}\right) = 32 + 7t \mod 42, \text{ for } t = 0, 1, ..., 5.$$

Exercise 2: Multiplicative Inverse

Find the multiplicative inverse of 3 modulo 10.

Simultaneous Linear Congruences

- The Chinese Remainder Theorem is concerned with solving simultaneous linear congruences

$$a_1x \equiv b_1 \mod m_1, a_2x \equiv b_2 \mod m_2, ..., a_rx \equiv b_r \mod m_r.$$

- We shall assume that the moduli m_k are relatively prime in pairs.
- The system will admit no solution unless each individual congruence is solvable.
- The solutions of the individual congruences assume the form

$$x \equiv c_1 \mod m_1, x \equiv c_2 \mod m_2, ..., x \equiv c_r \mod m_r.$$

Theorem (Chinese Remainder Theorem)

Let $n_1, n_2, ..., n_r$ be positive integers such that $\gcd(n_i, n_j) = i$ for $i \neq j$. Then the system of linear congruences

$$\begin{aligned} x &\equiv a_1 \mod n_1, \\ x &\equiv a_2 \mod n_2, \\ &\vdots \\ x &\equiv a_r \mod n_r. \end{aligned}$$

has a simultaneous solution, which is unique modulo the integer $n_1 n_2 \cdots n_r$.

Proof.

Sketch. Let $n = n_1 n_2 \cdots n_r$ and $N_k = \frac{n}{n_k}$. Fine solution x_k for $N_k x \equiv 1 \mod n_k$ for each $k = 1, ..., r$. Prove that $\widetilde{x} = a_1 N_1 x_1 + \cdots + a_k N_k x_k$ is a simultaneous solution. □

Example

The problem posed by Sun-Tsu corresponds to the system of three congruences

$$\begin{aligned} x &\equiv 2 \mod 3, \\ x &\equiv 3 \mod 5, \\ x &\equiv 2 \mod 7. \end{aligned}$$

Find a solution.

Exercise 3: Simultaneous Linear Congruences

Solve the linear congruence

$$17x \equiv 9 \mod 276.$$

Theorem

The system of linear congruences

$$\begin{aligned} ax + by &= r \mod n \\ cx + dy &= s \mod n \end{aligned}$$

has a unique solution modulo n whenever $\gcd(ad - bc, n) = 1$.

Example

Solve the system of equations

$$\begin{aligned} 7x + 3y &= 10 \mod 16 \\ 2x + 5y &= 9 \mod 16 \end{aligned}$$

Summary: What we did...

- Congruences
  - Definition, Properties
- Applications
  - Cancellation Rule, Representations of Integers
- Linear Congruences
  - Multiplicative Inverse
- Simultaneous Linear Congruences
  - Chinese Remainder Theorem
- Next Time
  - Fermat's and Wilson's Theorems and Number Theoretic Functions

Topic 4
Fermat's, Wilson's Theorems, and Number Theoretic Functions

$$a^p \equiv a \mod p,$$
$$(p-1)! \equiv -1 \mod p$$
$$a^{\phi(n)+1} \equiv a \mod n.$$

Lecture Contents

1. Introduction
   - Module Aims and Assessment
   - Topics to be Covered
   - Reading List and References
2. Topic 1: Vector Algebra and Real-Valued Functions
   - Introduction
   - Vectors Algebra
   - Euclidean Space
   - Dot and Cross Products
   - Real-Valued Functions
3. Topic 2: Differentiation, Gradient, Divergence, Curl
   - Continuity of Multivariate Functions
   - Differentiation of Multivariate Functions
   - Gradient of a Scalar field
   - Divergence of a Vector Field
   - Curl of a Vector Field
   - Mixed Partial Derivative and Laplacian
4. Topic 3: Line, Surface, and Volume Integrals
   - Line Integrals
   - Surface Integrals
   - Volume Integrals
5. Topic 4: Integrals Theorems and Applications
   - Gauss's (Divergence) Theorem
   - Stokes' Theorem
6. Topic 1: Integers and Divisibility
   - Methods of Number Theory
   - Well-Ordering Principle and Archimedes Property
   - Polygonal Numbers
   - The Division Algorithm
   - Greatest Common Divisor
   - The Euclidean Algorithm
   - The Diophantine Equation $ax + by = c$
7. Topic 2: Primes and Their Distribution
   - Prime Numbers
   - Fundamental Theorem of Arithmetic
   - Distribution of Primes
   - Goldbach's Conjecture
   - Primes in Arithmetic Progression
8. Topic 3: The Theory of Congruences
   - Basic Properties of Congruences
   - Cancellation Rule
   - Representations of Integers
   - Linear Congruences
   - Chinese Remainder Theorem
9. Topic 4: Fermat's, Wilson's Theorems, and Number Theoretic Functions
   - Fermat's Little Theorem and Pseudoprimes
   - Wilson's Theorem
   - Number Theoretic Functions
   - Applications to RSA Cryptosystem

Intended Learning Outcomes

By the end of this session you will be able to...

1. Learn about Fermat's and Wilson's theorems.
2. Understand number theoretic functions.

Introduction

- Pierre de Fermat (1601-1665) the "Prince of Amateurs," was the last great mathematician to pursue the subject as a sideline to a nonscientific career.
- By profession a lawyer and magistrate attached to the provincial parliament at Toulouse
- He sought refuge from controversy in the abstraction of mathematics.
- Fermat evidently had no particular mathematical training and he evidenced no interest in its study until he was past 30.
- To him, it was merely a hobby to be cultivated in leisure time.
- Fermat preferred the pleasure he derived from mathematical research itself to any reputation that it might bring him.

Fermat's Little Theorem

- Fermat's little theorem is an striking and simple statement for it say if p is a prime and a and integer with $p \nmid a$, then $p \mid a^{p-1} - 1$. Try $1^4, 2^4, 3^4, 4^4$ upon division by 5.
- **Recall** in the previous lecture for n a fixed positive integer we wrote

$$a \equiv b \mod n$$

if n divides the difference $a - b$.

Theorem (Fermat's Little Theorem)

Let p be a prime and suppose that $p \nmid a$. Then

$$a^{p-1} \equiv 1 \mod p.$$

Proof.

Sketch. The numbers $a, 2a, ..., (p-1)a$, are nonzero, not congruent to each other, and are congruent to $1, ..., p-1$ modulo p is some order. Take their product. □

Corollary

If p is a prime, then $a^p \equiv a \mod p$ for any integer a.

Example

Compute $5^{38} \mod 11$.

Solution. Note by FLT we have $5^{10} \equiv 1 \mod 11$. Now $38 = 3 \times 10 + 8$, so we have

$$\begin{aligned} 5^{38} &= 5^{3\times 10+8} = (5^{10})^3 5^8 \\ &\equiv 5^8 \mod 11 = 25^4 \mod 11 \equiv 3^4 \mod 11 \\ &\equiv 4 \mod 11. \end{aligned}$$

Exercise 1: Fermat's Little Theorem

Compute $2^{32004} \mod 17$.

Primality Testing

- Another use of Fermat's theorem is as a tool in testing the primality of a given integer n.
- If it could be shown that the congruence $a^n \equiv a \mod n$ fails to hold for some choice of a, then n is necessarily composite.
- For example test primality of 117, with say 2. We have $2^{116} = 2^{16\times 7+4}$ and $2^7 = 128 \equiv 11 \mod 117$, so

$$2^{116} \equiv 11^{16} + 2^4 \mod 117,$$

now we have $11^2 = 121 \equiv 4 \mod 117$, so

$$2^{116} \equiv 11^{16} + 2^4 \equiv 4^8 2^4 \equiv 2^{20} \equiv 11^2 2^6 \equiv 2^{10} \equiv 44 \mod 117.$$

- Therefore we have

$$2^{116} \equiv 44 \not\equiv 1 \mod 117,$$

which implies that 117 is not prime, indeed $117 = 13 \times 9$!

Converse of Fermat's

- Note the converse of Fermat's theorem may fail, in other words, if $a^{n-1} = 1 \mod n$ for some integer a, then n need not be prime.
- The following interesting lemma gives us some ideas about when the converse of Fermat's theorem fails.

Lemma

If p and q are distinct primes with $a^p \equiv a \mod q$ and $a^q \equiv a \mod p$, then $a^{pq} \equiv a \mod pq$.

Proof.

Note if $a^p \equiv a \mod q$, then $(a^p)^q \equiv a^q \equiv a \mod q$, so $a^{pq} \equiv a \mod q$, similarly we have $a^{pq} \equiv a \mod p$. Now this implies that $a^{pq} - a = kq$ and $a^{pq} - a = sp$, since $p \neq q$, we have that $p \mid k$, so $a^{pq} - a = rpq$, thus $a^{pq} \equiv a \mod pq$. □

Example

Show that $2^{340} \equiv 1 \mod 341$. Note $341 = 11 \times 31$.

- A composite integer n is called a pseudoprime whenever $n \mid 2^n - 2$.
- It can be shown that there are infinitely many such pseudoprimes, the smallest four being $341, 561, 645, 1105$.

Theorem

If n is an odd pseudoprime, then $M_n = 2^n - 1$ is a larger one.

Proof.

Sketch. Show M_n is composite. Note we have $n \mid 2^n - 2$, so $2^n - 2 = kn$, now $2^{M_n - 1} = 2^{2^n - 2} = 2^{kn}$, and check $2^{kn} - 1 \equiv 0 \mod M_n$. □

Wilson's Theorem

- Another important development of number theory is the Wilson's theorem.
- If p is a prime number, then p divides $(p-1)!+1$.
- Wilson appears to have guessed this on the basis of numerical computations!
- Theorems was hard to prove 1770 because of the absence of a notation to express prime numbers.

Theorem (Wilson's Theorem (Proved by Lagrange))

If p is a prime, then $(p-1)! \equiv -1 \mod p$. The converse of Wilson's theorem is also true.

- We can use Wilson's theorem to the study **quadratic congruences**.
- It is understood that quadratic congruence means a congruence of the form

$$ax^2 + bx + c = 0 \mod n$$

with $a \not\equiv 0 \mod n$.

Theorem

The quadratic congruence $x^2 + 1 \equiv 0 \mod p$, *where* p *is an odd prime, has a solution if and only if* $p \equiv 1 \mod 4$.

- Certain functions are found to be of special importance in connection with the study of the divisors of an integer.
- Any function whose domain of definition is the set of positive integers is said to be a number-theoretic, that is

$$f : \mathbb{Z}_{\geq 0} \longrightarrow \mathbb{C}.$$

- Although the value of a number-theoretic function is not required to be a positive integer or, for that matter, even an integer.

Example

Given a positive integer n, let $\tau(n)$ denote the number of positive divisors of n and $\sigma(n)$ denote the sum of these divisors.

Multiplicative Property

Definition (Multiplicative Functions)

A number-theoretic function f is said to be multiplicative if $f(mn) = f(m)f(n)$ whenever $\gcd(m, n) = 1$.

- Many of the number theoretic functions we will come across have the multiplicative property.
- Note given the definition above, for a multiplicative function f if $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ for distinct primes p_i, then we must have
$$f(n) = f\left(p_1^{k_1}\right) f\left(p_2^{k_2}\right) f\left(p_r^{k_r}\right).$$
- Also suppose there exist n with $f(n) \neq 0$, then $f(n) = f(n \cdot 1) = f(n)f(1)$, which implies that $f(1) = 1$.

Theorem

Let f be a multiplicative function. Define F by $F(n) \sum_{d|n} f(d)$ Then F is multiplicative.

Euler's phi-function

- A century after Fermat a first-class mathematician, Leonhard Euler (1707-1783) appreciated the significance of number theory.
- Many of the theorems announced without proof by Fermat yielded to Euler's skill.
- Euler's phi-function has vast application both in number theory and in cryptography.

Definition (Euler's phi-function)

For $n \geq 1$, let $\phi(n)$ denote the number of positive integers not exceeding n that are relatively prime to n.

Example

For $n = 8$, we have the numbers which are relatively prime to n are $1, 3, 5, 7$, so $\phi(n) = 4$. For a p we have $\phi(p) = p - 1$. In fact $\phi(p^k) = p^k - p^{k-1}$.

Theorem

Let n be a positive integer $\tau(n)$ the number of positive divisors, $\sigma(n)$ the sum of these divisors, and $\phi(n)$ the Euler's phi-function of n. Suppose $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. Then we have

$$\tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1), \tag{1}$$

$$\sigma(n) = \left(\frac{p_1^{k_1+1} - 1}{p_1 - 1}\right)\left(\frac{p_2^{k_2+1} - 1}{p_2 - 1}\right) \cdots \left(\frac{p_r^{k_r+1} - 1}{p_r - 1}\right), \tag{2}$$

$$\phi(n) = \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right) \cdots \left(p_r^{k_r} - p_r^{k_r-1}\right), \tag{3}$$

in particular all the above functions are multiplicative.

Theorem (Euler's Generalization of Fermat's Theorem)

If $n \geq 1$ and $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \mod n$.

Applications to RSA (cryptosystem)

- RSA (Rivest–Shamir–Adleman) is one of the first public-key cryptosystems and is widely used for secure data transmission.
- It is based on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem".
- It heavily relies on number theoretic functions.
- Watch the video https://www.youtube.com/watch?v=wXB-V_Keiu8.

Summary: What we did...

Fermat's Little Theorem	
	Primality, Pseudoprimes
Wilson's Theorem	
	Primality
Number Theoretic Functions	
	Euler's phi-function, RSA
Next Time	
	There won't be any (revision)!
Thanks for Your Attention!	
	Have a good holiday!

See You Next Time

Please Do Not Forget To

- Ask any **questions** now or through my contact details.
- Drop me **comments** and **feedback** relating to any aspects of the course.
- Come and see me during Student Drop-in Hours:
  MONDAYS 12:00-13:00 (MATHS ARCADE) AND
  TUESDAYS 15:00-16:00 (QM315).
  Alternatively, email to make an appointment.

Thank You!