ISI-CMI Book

SciAstra

September 6, 2024

Preface

The pursuit of excellence in mathematics, especially at the level of competitive exams like those for the Indian Statistical Institute (ISI) and the Chennai Mathematical Institute (CMI), requires more than just rote memorization or superficial understanding. It demands a deep comprehension of fundamental concepts, the ability to apply these concepts creatively, and, most importantly, the cultivation of rigorous mathematical thinking. With this in mind, we have crafted this problem book to serve as a comprehensive guide for students aspiring to excel in such prestigious entrance exams, as well as other olympiad-level competitions.

This book is designed to address the needs of a wide spectrum of learners by starting with the basics and systematically progressing to advanced topics. We recognize that a strong foundation is essential for tackling complex problems, and thus, every chapter begins with an introduction to the fundamental ideas. These core concepts are gradually built upon, ensuring that the learner's understanding is both deepened and solidified at every step. This approach allows students to develop a crystal-clear grasp of the subject matter, which is vital not only for success in competitive exams but also for future academic pursuits in mathematics and related fields.

Each section is followed by a carefully curated set of exercises that challenge the reader to apply the newly acquired knowledge. These exercises are crafted to reinforce understanding, while simultaneously introducing subtle nuances of the concepts. After completing each section, students will find themselves equipped with both theoretical understanding and practical problem-solving skills. In addition, we have included a collection of past examination problems, with detailed solutions, to provide students with insights into the types of questions they can expect in the actual exams. These solved problems are invaluable in helping students develop strategies for tackling exam-style questions effectively.

To ensure comprehensive preparation, we have incorporated a range of question types, including multiple-choice questions (MCQs), which are integral to many entrance exams. These questions not only test the student's ability to apply concepts quickly and accurately but also help develop the critical thinking required for objective portions of competitive exams.

For those looking to push the boundaries of their understanding, we have also included challenging problems at the end of each module. These harder problems go beyond the typical exam syllabus and provide an opportunity to explore deeper mathematical ideas. By grappling with these problems, students can extend their problem-solving abilities and experience the joy of discovery that lies at the heart of mathematics.

One of the central tenets of our philosophy in writing this book is that understanding the "why" in mathematics is far more important than simply knowing the "how." Mathematics is not just a collection of techniques and algorithms—it is the language of logical reasoning, and its power lies in its universal applicability to science, technology, and beyond. In line with this belief, we have taken great care in writing clear and rigorous proofs for the examples and problems presented throughout the book. Each proof serves as a model of "correct reasoning," demonstrating the elegance and power of mathematical logic.

This book addresses topics at an olympiad level, bridging the gap between traditional school-level mathematics and the advanced, problem-solving skills required for success in competitive exams. It is our hope that this approach not only helps students excel in their exams but also fosters a deeper appreciation for mathematics as a discipline. We believe that the process of mastering these topics will equip students with the confidence, creativity, and critical thinking skills needed to excel in their academic journeys.

Ultimately, this book is more than a study aid—it is a guide to developing a mindset that values deep understanding and rigorous reasoning. We are confident that students who engage fully with the material will not only be well-prepared for the ISI, CMI, and other olympiad-level exams but will also come to appreciate the beauty and depth of mathematics itself.

We wish you the best of luck in your preparation and hope that this book becomes an indispensable companion on your journey to success.

SciAstra ISI-CMI Team

Contents

1 Number Systems

1.1 Constuctions and Extensions

The *natural numbers* $1, 2, 3, 4, \ldots n, \ldots$ have been with each one of us since childhood. Almost all the important properties of this number set, which we shall call $\mathbb{N}$, have been accepted by us intuitively from experience. These properties may be listed now as follows. We add a few comments where necessary.

1. The set $\mathbb{N}$ is an endless set. That is, there is no last number. The sequence of natural numbers goes on and on.
2. There is a built-in order in the set in the way we write it:
$$1, 2, 3, 4, \ldots, a, \ldots, b, \ldots$$
If b appears later in the sequence than a then b is said to be greater than a. We write this: $b > a$; or, what is the same thing, $a < b$, i.e., a is less than b.
3. Every number has a successor number and, except for 1, every number has a predecessor number.
4. Any two numbers in the set can be 'added' to produce another number in the set. Recall that after one learns to count, the next thing that is learnt is to 'add'.
5. Whether one adds a to b or b to a it is the same thing—in the sense the result is the same. In other words, addition '+' is a commutative process; i.e.,
$$a + b = b + a \quad \text{for all } a, b \in \mathbb{N} \tag{1}$$
6. Repeated addition of the same number to itself is known as 'multiplication'. Thus, for instance, 4 added to itself 5 times is nothing but 4×5, that is, 20.
7. This multiplication is also commutative. That is,
$$a \times b = b \times a \quad \text{for all } a, b \in \mathbb{N} \tag{2}$$
8. Both the operations, addition and multiplication, have another property, called 'associativity'. This means: $a + b$ added to c and a added to $b + c$ are both the same. Symbolically,
$$(a + b) + c = a + (b + c) \quad \text{for all } a, b, c \in \mathbb{N} \tag{3}$$
In the same way, we have, for multiplication,
$$(a \times b) \times c = a \times (b \times c) \quad \text{for all } a, b, c \in \mathbb{N} \tag{4}$$
9. Further, there is a 'compatibility' between the two processes 'addition' and 'multiplication'; namely,
$$a \times (b + c) = (a \times b) + (a \times c)$$
and
$$(a + b) \times c = (a \times c) + (b \times c) \quad \text{for all } a, b, c \in \mathbb{N} \tag{5}$$
This is known as the distribution of multiplication with respect to addition.

These nine properties of the set $\mathbb{N}$ shall now be assumed without any further justification. Higher mathematics may require the construction of natural numbers from scratch and the derivation of these properties thereof. We do not have either the luxury of time or the necessity of logic to get into all that now, at this level.

One of the first things that we learn as we grow learning mathematics is that the system $\mathbb{N}$ of natural numbers has several deficiencies. For instance, we can solve for x, the equation: $2 + x = 3$ within the system $\mathbb{N}$. The answer is $x = 1$. Whereas, an equation like: $3 + x = 2$ is not solvable in $\mathbb{N}$. In other words, there is no value of x in $\mathbb{N}$ satisfying $3 + x = 2$. We know the answer is -1 but -1 is not a natural number. Thus the system $\mathbb{N}$ of natural numbers does not have solutions of the equation $a + x = b$, i.e., this equation has no solution for x in $\mathbb{N}$ unless $a < b$. Mathematics develops by concerning itself with such questions and resolving the issue. In the above situation, the resolution comes like this. Mathematics invents new numbers, namely, $0, -1, -2, -3, \ldots$ expressly to satisfy the need to solve the equations $a+x = b$ even when $a \geq b$. For instance, if $a = b$, the equation is $a+x = a$. We invent the new number "0" (zero) to be the solution of

$$a + x = a = x + a.$$

Once we include a new number 0 to the system $\mathbb{N}$ we want also to solve equations like

$$1 + x = 0; \quad 2 + x = 0; \quad 3 + x = 0; \ldots$$

The solutions of these are called the negatives of $1, 2, 3, \ldots$ and are written

$$-1, -2, -3, \ldots$$

Thus the enlarged system now contains zero and all the negative integers and $\mathbb{N}$. This new system is denoted by $\mathbb{Z}$ and is called the *set of all integers*. Thus

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

It can also be written as below, where we bring out the 'order' relation in $\mathbb{Z}$. In other words, in the following style of listing the elements of $\mathbb{Z}$, if a precedes b then $a < b$, or what is the same thing, $b > a$.

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

There are several points we have to note about this enlargement of $\mathbb{N}$ to $\mathbb{Z}$. In enlarging $\mathbb{N}$ to $\mathbb{Z}$ we have been able to 'protect' or 'preserve' as many properties of $\mathbb{N}$ as possible. Precisely we mean the following:

1. $\mathbb{Z}$ is an infinite (= endless) sequence as $\mathbb{N}$ was (and is!).

2. The built-in order in $\mathbb{N}$ is still preserved. It has in fact been extended to $\mathbb{Z}$. In other words 'a ¿ b' has a meaning in $\mathbb{Z}$ for every a and b in $\mathbb{Z}$ and further, if $a > b$ in $\mathbb{N}$ for two elements $a, b \in \mathbb{N}$, it is so in $\mathbb{Z}$, even as elements of $\mathbb{Z}$.

3. Every number in $\mathbb{Z}$ has a successor and a predecessor. Recall that in $\mathbb{N}$ the number 1 does not have a predecessor. Also any number in $\mathbb{N}$ whether considered as a member in $\mathbb{N}$ or a member in $\mathbb{Z}$ has the same successor. Similarly, any number $\neq 1$ in $\mathbb{N}$ has the same predecessor in $\mathbb{N}$ or $\mathbb{Z}$. We express this by saying that the 'successor-predecessor' concept has been extended to $\mathbb{Z}$ without damage to the concept already existing in $\mathbb{N}$.

4. The operation of addition already available in $\mathbb{N}$ carries over to $\mathbb{Z}$. If $x = -a$ where $a \in \mathbb{N}$, $y = -b$ where $b \in \mathbb{N}$, we may define $x + y = -(a + b)$ where $+$ in the R.H.S. is the addition in $\mathbb{N}$. Since $(a + b) \in \mathbb{N}, -(a + b) \in \mathbb{Z}$. Thus we get the familiar equality.
$$(-a) + (-b) = -(a + b)$$
   Again, if $x = -a, a \in \mathbb{N}$, is 'added' to $c \in \mathbb{N}$ we will have $x + c = (-a) + c$. This is to be taken as
$$-(a - c) \text{ if } a > c$$

and as

$$c - a \text{ if } c > a \text{ or } c = a.$$

Proceeding in this way and carefully going through every new situation we get a thorough definition of addition in $\mathbb{Z}$. We see that 'addition' is closed in $\mathbb{Z}$ — by which, we mean, two numbers in $\mathbb{Z}$ always lead to a number in $\mathbb{Z}$ by the addition process. If two numbers are already in $\mathbb{N}$ their sum is what it is in the system $\mathbb{N}$. Thus the extension of $\mathbb{N}$ and the addition therein to $\mathbb{Z}$ has been achieved without 'damaging' the addition in $\mathbb{N}$. This process of enlarging a number system, preserving its algebraic structure is called an *extension* of the system. Addition of zero to any number, again satisfies,

$$a + 0 = 0 + a \quad \text{for all } a \in \mathbb{Z}.$$

5. Addition in $\mathbb{Z}$ continues to be commutative. In other words,

$$a + b = b + a \quad \text{for all } a, b \in \mathbb{Z} \tag{1'}$$

6. Multiplication in $\mathbb{N}$ can be extended to a multiplication in $\mathbb{Z}$, without damaging the meaning of multiplication in $\mathbb{N}$ — except that, we have to make proper rules for handling the negative sign, thus: If $a, b \in \mathbb{N}$, then

$$a \times b = ab \quad (\text{as in } \mathbb{N})$$

$$(-a) \times (-b) = ab$$
$$(-a) \times b = -(ab)$$
$$a \times (-b) = -(ab).$$

Multiplication by zero however has to be controlled by a new rule, viz.,

$$a \times 0 = 0 = 0 \times a \quad \text{for all } a \in \mathbb{Z}.$$

7. Multiplication in $\mathbb{Z}$ is commutative. In other words,

$$a \times b = b \times a \quad \text{for all } a, b \in \mathbb{Z} \tag{2'}$$

8. The associative properties of both addition and multiplication continue to be valid in $\mathbb{Z}$. In other words

$$a + (b + c) = (a + b) + c \quad \text{for all } a, b, c \in \mathbb{Z} \tag{3'}$$

and

$$a \times (b \times c) = (a \times b) \times c \quad \text{for all } a, b, c \in \mathbb{Z} \tag{4'}$$

9. The distributive property

$$a(b + c) = ab + ac$$
$$(a + b)c = ac + bc \quad \text{for all } a, b, c \in \mathbb{Z} \tag{5'}$$

holds, as it holds in $\mathbb{N}$.

10. Finally, we record, at one place, the special roles of the numbers 0 and 1 in $\mathbb{Z}$ as follows:

10.1. In $\mathbb{Z}$, 0 is the unique number which has the property:

$$0 + a = a = a + 0 \quad \text{for all } a \in \mathbb{Z} \tag{6'}$$

10.2. In $\mathbb{Z}$, 1 is the unique number which has the property

$$a \times 1 = a = 1 \times a \quad \text{for all } a \in \mathbb{Z}$$

Now let us look at the second stage of extensions which is from the set of integers to the set of rational numbers. Thus we have the following so far

$$\mathbb{N} \to \mathbb{Z} \to \mathbb{Q}$$

The set of rational numbers is defined as follows

$$\mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0 \text{ and } \gcd(p, q) = 1 \right\}$$

We need $\mathbb{Q}$ to solve equations like $ax = b$, where $a, b \in \mathbb{Z}$ which cannot be solved in $\mathbb{Z}$ or $\mathbb{N}$. Now let us look at properties of $\mathbb{Q}$

Defintion 1: Two rational numbers $\frac{a}{b}$ and $\frac{c}{d}$ are said to be equal if $ad = bc$ We also write every $n \in \mathbb{Z}$ as $\frac{n}{1}$ in $\mathbb{Q}$

Defintion 2: For $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$, where $a, b, c, d \in \mathbb{Z}$ and $b, d > 0$, we have

$$\frac{a}{b} \geq \frac{c}{d} \text{ if and only if } ad \geq bc$$

Now the question is "Is $\mathbb{Q}$ enough or do we need an even larger set?". Observe that if we look at the equation $x^2 = 2$, this does not have a solution in $\mathbb{Q}$. One might say that $x = \pm\sqrt{2}$ but what exactly is $\sqrt{2}$?. The following theorem proves that if $\sqrt{2}$ exists then it is not

Theorem 1: There is no rational number x such that $x^2 = 2$

Proof: Suppose there is some rational number $x = p/q$ such that $x^2 = 2$. This implies that $p^2 = 2q^2$. The right hand side is even which implies that p must be even as well. We know even numbers are of the form $2k$ where $k \in \mathbb{Z}$. Suppose $p = 2p_1$. Substuituting this in the previous equation and canelling out a factor of 2 we get that $2p_1^2 = q^2$ which in turn implies that q is also even. But this would imply that $\gcd p, q \geq 2$ which is a contradiction. Thus there is no rational number x such that $x^2 = 2$

Thus we require a completely new set of numbers which look like $\sqrt{2}, \sqrt{3}, \sqrt{5}, \cdots$. We call these numbers irrational numbers. The simplest way of defining irrational numbers is the set of numbers whose decimal expansion is neither recurring nor terminating. Now combing the rationals and irrationals we get the set of real numbers,$\mathbb{R}$. But is this enough?

Turns out no. We still cant solve equations like $x^2 + 1 = 0$ in $\mathbb{R}$. This gives rise to the set of Complex numbers $\mathbb{C}$ where we work with square roots of negative numbers but that is different chapter in itself.

Now let us look at some solved examples

1.2 Solved Examples

Example 1: Suppose $a/b < c/d$ where $a, b, c, d \in \mathbb{Z}$ and $b, d > 0$ then we have

$$\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$$

Solution: Observe that $a/b < c/d$ implies that $ad < bc$. Adding ab on both sides we get that

$$ab + ad < ab + bc$$

This means that $a(b+d) < b(c+a)$ which gives us $\frac{a}{b} < \frac{a+c}{b+d}$

Similarly if we add cd instead of ab, we get the upper bound.

Example 2: Let a, b be positive integers then show that $\sqrt{2}$ lies between a/b and $(a+2b)/(a+b)$

Solution: There are two possibilities $a/b > \sqrt{2}$ or $a/b < \sqrt{2}$. In the first case, squaring both sides we get that $a^2 > 2b^2$. Now

$$a^2 + 4b^2 = a^2 + 2b^2 + 2b^2 < 2(a^2 + b^2)$$
$$(a+2b)^2 = a^2 + 4b^2 + 4ab < 2(a^2 + b^2 + 2ab) = 2(a+b)^2$$

The second equation gives us $(a+2b)/(a+b) < \sqrt{2}$. Thus we get the bounds

$$\frac{a+2b}{a+b} < \sqrt{2} < \frac{a}{b}$$

Similarly we can prove it for the second case where the directions of all the inequalities changes.

Example 3: Find the rational number whose decimal expansion is $0.123454545\cdots$

Solution: Note: These numbers are also expressed as $x = 0.123\overline{45}$ where the bar on the top denotes the recurring part i.e. the part that gets repeated.

$$x = 0.123\overline{45}$$
$$10^3 x = 123.\overline{45}$$
$$10^5 x = 12345.\overline{45}$$

Subtracting the second and the third equations, we get that

$$(10^5 - 10^3)x = 12222 \implies x = \frac{12222}{99000}$$

1.3 Exercises

1. Given any real number $x > 0$ prove that there exists an irrational number α such that $0 < \alpha < x$.

2. Prove that $\sqrt{2} + \sqrt{5}$ is irrational.

3. Find all positive integers n for which $\sqrt{n-1} + \sqrt{n+1}$ is rational.

4. If $a + \sqrt{b} = c + \sqrt{d}$ where a, b, c, d are rationals then $a = c$ and $b = d$ unless b, d are squares of rational numbers.

5. If $a + b\sqrt[3]{p} + c\sqrt[3]{p^2} = 0$ where a, b, c, p are rational and p is not a perfect cube then $a = b = c = 0$

6. Prove that $\sqrt{2} + \sqrt{3} + \sqrt{5}$ is an irrational number.

---

2 Working with Integers

2.1 Principle of Induction

In this chapter we will see certain fundamental properties of $\mathbb{N}$ and $\mathbb{Z}$. Consider the following statements about positive integers

1. $n(n+1)(n+2)$ is always divisible by 6
2. Sum of the first n natural numbers is $S_n = n(n+1)/2$
3. $2^n > n$ for all natural numbers

These are all statements about positive integers n. Now suppose we want to check the validity of these statements then how should one go about doing that?

Suppose we consider the statement about the sum of natural numbers. Statement (2) says that $S_n = n(n+1)/2$. Let us look at the the values for the first couple of natural numbers. $S_1 = 1, S_2 = 3, S_3 = 6, S_4 = 10, S_5 = 15$ which all satisfy $S_n = n(n+1)/2$. But how do we prove it for a general n. One thing that might help is the following

$$S_{k+1} = 1 + 2 + \cdots + k + (k+1) = S_k + (k+1)$$

If we have checked or verified that $S_n = n(n+1)/2$ for all $n \leq k$ then plugging that into the equation above we can say that

$$\begin{aligned} S_{k+1} &= S_k + (k+1) \\ &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{(k+1)(k+2)}{2} \end{aligned}$$

Hence we proved the statement for $n = k$ and using the same idea we can prove it for numbers after k. The underlying principle in the above argument is the **Principe of Mathematical Induction**

Let $P(n)$ be a statement about natural numbers such that

1. $P(1)$ is true that is the statement is true for $n = 1$
2. Whenever $P(k)$ is true, we have $P(k+1)$ is true

If these two conditions hold then the Principle of Mathematical induction tells us the statement is true for all natural number n

2.2 Solved Examples

Example 1: Let x be a real (or complex) number such that $x \neq 1$ then

$$1 + x + x^2 + \cdots x^{n-1} = S_n = \frac{1-x^n}{1-x}$$

Solution: Let us prove this using induction on n. Oberse that for $n = 1$, we have $S_1 = 1 = \frac{1-x}{1-x}$ which proves that the statement is true for $n = 1$. Now suppose we assume the statement is true for $n = k$ that is

$$S_k = 1 + x + x^2 + \cdots + x^{k-1} = \frac{1-x^k}{1-x}$$

Then for $n = k+1$, we have

$$S_{k+1} = S_k + x^k = \Big(\frac{1-x^k}{1-x}\Big) + x^k = \frac{1-x^{k+1}}{1-x}$$

Thus we showed that the statement is true for $n = 1$ and whenever it is true for some $n = k$, it is also true for $n = k + 1$. Thus by the Principle of Mathematical Induction we can conclude that the statement is true for all natural numbers.

Note: The sum given in the previous equation is known as a the sum of a Geometric Progression upto n terms with common difference x and first term 1.

Example 2: Prove that

$$\frac{1}{1 \times 2} + \frac{1}{2 \times 3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$$

Solution: For $n = 1$, the left hand side of the equation is just $1/1.2 = 1/2$ which equals the right hand side and hence the statement is true for $n = 1$. Now assume that for $n = k$ we have

$$S_k = \frac{1}{1.2} + \frac{1}{2.3} + \cdots + \frac{1}{k(k+1)} = \frac{k}{k+1}$$

Now, we have

$$\begin{aligned} S_{k+1} &= S_k + \frac{1}{(k+1)(k+2)} \\ &= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)} \\ &= \frac{k^2 + 2k + 1}{(k+1)(k+2)} = \frac{k+1}{k+2} \end{aligned}$$

This proves the statement for $n = k + 1$ and hence the statement is true for all natural numbers n.

Definition: The Fibonacci sequence is a special sequence defined as $\{a_n\}$ $n \geq 1$ with $a_1 = a_2 = 1$ and $a_n = a_{n-1} + a_{n-2}$ for all $n \geq 3$. In simple terms any term staring from the third term is the sum of the previous two terms. So the first couple of terms of the Fibonacci sequence are given by

$$1, 1, 2, 3, 5, 8, 13, 21, \cdots$$

Let us try proving some properties of the Fibonacci sequence using induction

Example 3: Let $\{a_n\}$ be the Fibonacci sequence. Prove that for any n

$$a_1 + a_2 + \cdots + a_n = a_{n+2} - 1$$

Solution: Observe that for $n = 1$, we have $a_1 = 1 = 2 - 1 = a_3 - 1$. Hence the statement is true for $n = 1$. Now assume that the statement is true for some $n = k$ that is $S_k = a_1 + a_2 + \cdots + a_k = a_{k+2} - 1$. Now, for $n = k + 1$, we have

$$S_{k+1} = S_k + a_{k+1} = a_{k+1} + a_{k+2} - 1 = a_{k+3} - 1$$

Thus the statement is true for $n = k + 1$ and hence by induction the statement is true for all natural numbers n

Example 4: Prove that $5^{2n} - 6n + 8$ is divisible by n for every natural number n

Solution: Let x_n denote the number $5^{2n} - 6n + 8$. Then $x_1 = 5^2 - 6 + 8 = 27$ which is divisible by 9 and hence the statement is true for $n = 1$. Now assume that 9 divides $x_n = 5^{2n} - 6n + 8$. This means that x_n is a multiple of 9 and hence we can write $5^{2n} - 6n + 8 = 9k$ for some positive integer k. Now,

$$\begin{aligned} x_{n+1} &= 5^{2(n+1)} - 6(n+1) + 8 \\ &= 25(5^{2n}) - 6n + 2 \\ &= 25(9k + 6n - 8) - 6n + 2 \\ &= 9(25k) + 144n - 198 \end{aligned}$$

The expression in the last line is divisible by 9 and hence 9 divides x_{n+1}. Thus by induction the statement is true for all natural numbers n.

2.3 Exercise 2.1

1. If there are n participants in a knock-out tournament then prove that $n-1$ matches would be required to declare the champion

2. Prove that $1^2+2^2+\cdots n^2=\frac{n(n+1)(2n+1)}{6}$ for any natural number n

3. Prove that $1^3+2^3+\cdots n^3=\left(\frac{n(n+1)}{2}\right)^2$ for any natural number n

4. Prove that the sum of the first n odd numbers is n^2

5. Prove that $2^n>n^3$ for every $n>9$

6. Show that $2.7^n+3.5^n-5$ is divisible by 24 for all positive integers n. (its 3×5^n....)

7. If $S_n=(3+\sqrt{5})^n+(3-\sqrt{5})^n$. Show that $S_{n+1}=6S_n-4S_{n-1}$. Using this prove that S_n is an integer for all n and 2^n divides S_n for all n.

8. For the Fibonacci sequence prove that

1. $a_1+a_3+a_5+c\cdots+a_{2n-1}=a_{2n}$
2. $a_2+a_4+a_6+\cdots+a_{2n}=a_{2n+1}-1$
3. $a_1a_2+a_2a_3+\cdots+a_{2n-1}a_{2n}=(a_{2n})^2$
4. $a_1a_2+a_2a_3+\cdots+a_{2n}a_{2n+1}=(a_{2n+1})^2-1$

9. Let x_n be the n-th non-square positive integer. Thus $x_1=2$, $x_2=3$, $x_3=5$, $x_4=6$, etc. For a positive real number x, denote the integer closest to it by $\langle x\rangle$. If $x=m+0.5$, where m is an integer, then define $\langle x\rangle=m$. For example, $\langle 1.2\rangle=1$, $\langle 2.8\rangle=3$, $\langle 3.5\rangle=3$. Show that

$$x_n=n+\langle\sqrt{n}\rangle.$$

10. [ISI-11] For $n\in\mathbb{N}$ prove that

$$\frac{1}{2}\cdot\frac{3}{4}\cdot\frac{5}{6}\cdots\frac{2n-1}{2n}\leq\frac{1}{\sqrt{2n+1}}.$$

2.4 Divisibility

Recall that in the first chapter we say that the equation $ax = b$ where $a, b \in \mathbb{Z}$ might not always have solutions in $\mathbb{Z}$. For example $3x = 12$ has an integer solution $x = 4$ however $5x = 12$ doesn't have one. This leads to the following definition

Definition: An integer a divides another integer b if there exists an integer c such that

$$b = ac$$

We call a, a factor of b or we say that b is a multiple of a. For example every even number is divisible by 2 which gives us the general form of even number as $2k$ where $k \in \mathbb{Z}$. If a divides b, we write it as $a|b$

Let us look at some elementary properties of divisibility

1. If $a|b$ then $a|bc$ for any integer c
2. If $a|b$ and $b|c$ then $a|c$
3. If $a|b$ and $a|c$ then $a|bx + cy$ for any $x, y \in \mathbb{Z}$
4. if $a|b$ then $|a| \leq |b|$
5. if $a|b$ and $b|a$ then $a = \pm b$

Proof:

1. $a|b$ implies $b = ak$ for some $k \in \mathbb{Z}$. Now $bc = akc = a(kc) \implies a|bc$
2. $a|b$ implies $b = ak_1$ and $b|c$ implies $c = bk_2$. Combining these we get that $c = ak_1k_2$ which implies that $a|c$
3. $a|b$ implies $b = ak_1$ and $a|c$ implies $c = ak_2$. Now $bx + cy = ak_1x + ak_2y = a(k_1x + k_2y)$ which implies $a|bx + cy$ for any integers x, y
4. If $a|b$ then $b = ak \implies |b| = |a||k|$. Now $k \in \mathbb{Z}$ hence $|k| \geq 1$. Now multiplying both sides by $|a|$, we get that $|b| \geq |a|$
5. $a|b$ implies that $b = ak_1$ and $b|a$ implies that $b = ak_2$. Substituting this in the first equation, we get that $ak_1k_2 = a$ which implies $k_1k_2 = 1$. Now the possible integer solutions of this equation are $k_1 = k_2 = 1$ or $k_1 = k_2 = -1$ which gives us the two possibilities $a = b$ or $a = -b$

Before we look at any more theorems let us look at an elementary property of subsets of natural numbers.

Lemma (Well Ordering Principle): Any non empty subset of natural numbers has a least element. In other words if $S \subseteq \mathbb{N}$ which is non empty then there exists $a \in S$ such that $s \geq a$ for every $s \in S$

Though this is a very simple lemma, observe that there are sets for which this statement is not true. For example if we look at subsets of $\mathbb{Z}$ say $S = \cdots, -3, -2, -1, 0, 1\}$, this set does not have a least element.

Theorem 2: (Division Algorithm) Given any integers a and b with $a \neq 0$, there exists unique integers q and r such that $b = aq + r$ and $0 \leq r < |a|$. In case a does not divide b then r satisfies the stronger inequality $0 < r < a$

Proof: If $a|b$ then we are done. We get $r = 0$. In case $a \nmid b$ then we prove it using the well ordering principle. Define a set S as follows

$$S = \{b - ak \Big| b - ak > 0, k \in \mathbb{Z}\}$$

Since we are only looking at positive integers, we can say that $S \subseteq \mathbb{N}$. Now observe that if we choose k such that $ak = |ab|$ then clearly $b + |ab| > 0$ and belongs to S and hence S is non empty, Thus using the well ordering principle we can say that S has a least element. Say r is the least element of S. Since $r \in S$, there is some integer q such that $b - aq = r$ that is $b = aq + r$. Now all we need to show is that r satisfies the bounds $0 < r < |a|$.

If $r \geq |a|$ then $0 \leq r - |a| < r$. Also $r - |a|$ is of the form $b - ak'$ for some k' but this contradicts the minimality of r as a smaller element than r belongs to S. Hence we cant have $r \geq |a|$. Since $r \in S$ hence $r > 0$. This gives is the bounds $0 < r < |a|$

The proof for uniqueness is very simple and left as an exercise.

The most important result that follows from the Division Algorithm is that if we divide a number by a natural number n the the set of possible remainders are $\{0, 1, \cdots, n-1\}$. Using this we can say that for any given n, any natural number has to be of one of the following forms

$$nk, nk+1, nk+2, \cdots nk+(n-1)$$

For example with respect to 2, numbers have to of the form $2k$ or $2k+1$ which are nothing but the set of even numbers and odd numbers respectively. Similarly with respect to 3, numbers are of the form $3k, 3k+1$ or $3k+2$ and so on so forth.

Note: The form $3k+2$ is the same as the form $3k-1$. We sometimes use the form $nk-r$ as you will see in the upcoming problems.

Let us look at some basic problems based on divisibility and the division algorithm.

Example 1: Find all integers n such that n^2+1 is divisible by $n+1$.

Solution: Observe that we have a number which is very close to n^2+1 which is divisible by $n+1$ for all natural numbers n. This number is nothing but n^2-1. Now we have from the question that $n+1|n^2+1$ and we know $n+1|n^2-1$. Thus $n+1$ should also divide the difference of these two numbers. This gives us $n+1|2$. Now the integer divisors of 2 are ± 1 and ± 2. Equating these with $n+1$, we get the required value of n as $-3, -2, 0, 1$

Example 2: Show that the square of any number is of the form $4k$ or $8k+1$

Solution: We know that any natural nuber n is of the form $2k$ or $2k+1$. If $n = 2k$, we get $n^2 = 4k^2$ which is of the form $4k$. If $n = 2k+1$ then

$$n^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1 = 8m + 1$$

here the last line follows because $k(k+1)$ is the product of two consecutive integers which is always even. This proves the required statement.

Definition: An integer d is called a common divisor of a and b if and only if $d|a$ and $d|b$. Let a, b be integers not both zero. A positive integer g is said to be the **greatest common divisor** of a and b if and only if

1. $g|a$ and $g|b$ that is g is a common divisor of both a and b
2. If there exists $d \in \mathbb{N}$ such that $d|a$ and $d|b$ then $d|g$. This statement ensures that g is the largest among the common divisors.

Theorem (Bezout's Theorem) If a, b are integers not both zero, then there exists integers x_0, y_0 such that

$$\gcd(a, b) = ax_0 + by_0$$

Proof: Consider the set $S = \{ax + by \big| x, y \in \mathbb{Z}, ax + by > 0\}$. S is clearly a subset of $\mathbb{N}$ and we can choose x and y such that we get the element $|a|^2 + |b|^2$, hence S is non empty as well. Thus S has a least element say g. There $g = ax_0 + by_0$ for some $x_0, y_0 \in \mathbb{Z}$.

Now assume $g \nmid a$. Then using the division algorithm we can say that $a = gq + r$ for some $q, r \in \mathbb{Z}$ and $0 < r < g$. But then $r = a - gq = a(1 - qx_0) + b(-qy_0)$ which implies that $r \in S$. But since $r < g$, this contradicts the minimality of g. Thus we can say that $g|a$. Similarly we can say that $g|b$. Oberve that if $d|a$ and $d|b$ then $d|ax_0 + by_0 = g$. Thus we can conclude that $g = \gcd(a, b) = ax_0 + by_0$ for some $x_0, y_0 \in \mathbb{Z}$

Now if you look carefully, Bezout's theorem tells us about the existence of one pair (x_0, y_0) such that $\gcd(a, b) = ax_0 + by_0$. But is this pair unique? If not how many such pairs are there? Are there finitely many such pairs or infinitely many pairs?

The answer to this question is that there are infinitely many such pairs and the proof is very simple. Say (x_0, y_0) is the pair we get from Bezout's. Then,

$$a(x_0 + bk) + b(y_0 - ak) = ax_0 + abk + by_0 - abk = ax_0 + by_0 = \gcd(a, b)$$

Thus the pair $(x_0 + ak, y_0 - bk)$ also satisfies the condition for any $k \in \mathbb{Z}$. Thus there are infinitely many such pairs.

Definition: Two integers a, b which are not both zero are said to be relatively prime or coprime if $\gcd(a, b) = 1$

For example the numbers 9 and 16 are relatively prime so are 8 and 15 but the same time 6 and 15 are not. Two consecutive numbers are always relatively prime and so are two consecutive odd numbers.

Corollary 1: Let $a, b \in \mathbb{Z}$ not both zero. Then a and b are coprime if and only if there exists integers x, y such that $ax + by = 1$

Proof: If a and b are coprime then $\gcd(a, b) = 1$ and hence by Bezout's theorem there exists integers x, y such that $ax + by = 1$.

On the other hand if we have $a, b \in \mathbb{Z}$ such that $ax + by = 1$ then if $d = \gcd(a, b)$ then $d|a$ and $d|b$ which implies $d|ax + by = 1$. Now the only positive integer that divides 1 is 1 hence $d = 1$ thus the numbers are coprime

Corollary 2: If $a, b \in \mathbb{Z}$ are coprime numbers then any integer n can be expressed as $ax+by$ for some $x, y \in \mathbb{Z}$

Proof: Since a, b are coprime, there exists $u, v \in \mathbb{Z}$ such that $au + bv = 1$. Multiplying both sides by n we get that $n = a(un) + b(vn)$. Thus n can be expressed as $ax + by$ with $x = nu$ and $y = nv$

Corollary 3: if $d = \gcd(a, b)$ then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Proof: $d = \gcd(a, b)$ implies that $a = dx$ and $b = dy$ for some integers x, y. Now, we know that there exits integers r, s such that $ar + bs = d$. This implies $dxr + dys = d$ which gives us $rx + sy = 1$ and according to the previous lemma this implies that $\gcd(r, s) = 1$. This proves the required statement.

Example 4: Show that there are no integers a, b such that $\gcd(a, b) = 3$ and $a + b = 100$.

Solution: Observe that if $\gcd(a, b) = 3$ then $3|a$ and $3|b$ which implies that $3|a + b$. But we know that $3 \nmid 100$ which implies that such integers a, b cannot exist.

Note: We sometimes denote $\gcd(a, b)$ as (a, b) when the context is clear.

Example 5: If $(a, n) = 1$ and $(b, n) = 1$ then $(ab, n) = 1$

Solution: As $(a, n) = 1$ and $(b, n) = 1$, by corollary 1 there are integers x, y and u, v such that $ax + ny = 1$ and $bu + nv = 1$. Multiplying these two equations, we get that

$$ab(xu) + n(vax + ybu + ynv) = 1$$

and hence from corollay 1 it follows that $(ab, n) = 1$

Example 6: For any $x \in \mathbb{Z}$, $(a, b) = (a, b + ax)$

Solution: Let $(a, b) = d$ and $(a, b + ax) = e$ then for some integers r, s, u, v we have

$$ar + bs = d$$

$$au + (b + ax)v = e$$

Now as $d|a$ and $d|b$, we have $d|e$. Similarly $e|a$ and $e|(b + ax)$ which gives us that $e|b$ which further implies that $e|d$. Hence we can say that $d = e$

The following remark follows directly from the previous example.

Remark: Observe that if $b = aq + r$ and $0 \leq r < |a|$ then $(a, b) = (a, r)$

Theorem 4 (The Eucledian algorithm) Given integers b and c with $c > 0$, we can make repeated use of the division algorithm to obtain the following sequence of equations:

$$\begin{aligned}
b &= cq + r_1, & 0 < r_1 < c,\\
c &= r_1 q_1 + r_2, & 0 < r_2 < r_1,\\
r_1 &= r_2 q_2 + r_3, & 0 < r_3 < r_2,\\
&\vdots & \vdots\\
r_{j-2} &= r_{j-1} q_{j-1} + r_j, & 0 < r_j < r_{j-1},\\
r_{j-1} &= r_j q_j.
\end{aligned}$$

Then $(b, c) = r_j$, the last non zero remainder in the division process. Moreover if $(b.c) = bx_0 + cy_0$ then the values of x_0 and y_0 can be obtained by eliminating $r_{j-1}, \cdots, r_2, r_1$ from the above set of equations.

Proof: If $(b, c) = g$ then $g|b$ and $g|c$. Hence $g|b - cq$. But $b - cq = r_1$ and hence $g|r_1$. Now, in the second equation we have that $g|c$ and $g|r_1$ hence $g|r_2$. Continuing this way we can say that $g|r_i$ for $1 \leq i \leq j$. In particular $g|r_j$. Conversely note that $r_j|r_{j-1}$. Hence $r_j|r_{j-1}q_{j-1} + r_j$ which implies that $r_j|r_{j-1}$. Continuing this we can say that $r_j|r_{j-3}$, $r_j|r_{j-4} \cdots r_j|b, r_j|c$. Thus r_j is a common divisor of both b and c. Hence $r_j|(b, c) = g$. But we also showed that $g|r_j$ which implies $g = r_j$

Example 7: Prove that the fraction $\frac{21n+4}{14n+3}$ is irreducible for every natural number n.

Solution: Note that irreducible means the fraction is in its lowest form i.e. there are no common factors between the numerator and the denominator. So all we need to show in this question is that $(21n + 4, 14n + 3) = 1$. Using the Euclidean algorithm we have that

$$\begin{aligned}
21n + 4 &= 1(14n + 3) + (7n + 1)\\
14n + 3 &= 2(7n + 1) + 1\\
7n + 17 &= 1(7n + 1)
\end{aligned}$$

Hence we can say that $(21n + 4, 14n + 3) = 1$ which proves the required statement.

2.5 Primes and Factorization

Definition: An integer $p > 1$ is called a prime number or a prime if it has no divisor d such that $1 < d < p$. In other words the only divisor of the number p are 1 and itself. If an integer is not a prime, it is called a composite number.

Example 8: If p is a prime and $p \nmid a$ then $(a, p) = 1$

Solution: Let $(p, a) = d$. Then $d|p$ and $d|a$. But p is a prime hence $d = 1$ or $d = p$. But p$\nmid a$ which implies that $d = 1$.

Theorem 5 (Euclid's Lemma) If $(a, m) = 1$ and $m|ab$ then $m|b$

Proof: Since $(a, m) = 1$, there exists integers x, y such that $ax + my = 1$. Hence $abx + mby = b$. Since $m|ab$, we get that $m|(abx + mby)$ which implies that $m|b$

Example 9: Prove that if p is a prime then $\sqrt{p}$ is an irrational number

Solution: Suppose $\sqrt{p}$ is a rational number say a/b where $a, b \in \mathbb{Z}$ and $(a, b) = 1$. Then we have $p^2 = \frac{a^2}{b^2}$ which in turn gives us $pb^2 = a^2$. Hence we can say that $p^2|a$. By Euclid's Lemma $p|a$ hence $p^2|a^2$. But $a^2 = pb^2$ hence $p^2|b^2$ that is $p|b$ which gives us a contradiction. Hence $\sqrt{p}$ is an irrational number.

Theorem 6 (The Fundamental Theorem of Arithmetic) Every positive integer $n > 1$ can be expressed as a product of primes in an unique way except for the order of the prime factors. This means every integer can be written as

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where $p_i \neq p_j$ and $\alpha_i \geq 0$ for every i

Definition: Let a, b be non-zero integers. An integer m is called a common multiple of a and b in case $a|m$ and $b|m$. Futher a positive integer l is said to be the **least common multiple(lcm)** of a and b if and only if the following hold

1. $a|l$ and $b|l$
2. if $a|m$ and $b|m$ then $l|m$

Example 10: The sum of two positive integers is 52 and their lcm is 168. Find the numbers

Solution: Let be numbers be a, b with $a \leq b$. Let $d = (a, m)$ such that $a = dm$ and $b = dn$ and $(m, n) = 1$. Thus we have

$$a + b = d(m + n) = 52 = 4 \times 13$$

$$\text{lcm}(a, b) = dmn = 168 = 4 \times 2 \times 7 \times 3$$

As $(m, n) = 1$, $((m + n)d, mnd) = d$ and hence from the two equation above we have $d = 4$ and $m + n = 13$. This gives us $mn = 42$. So $m = 6, = 7$ and the numbers are 24 and 28.

Theorem 7: There are infinitely many primes

Proof: Assume there are finitely many primes , say $2 = p_1, p_2, \cdots, p_r$. Let N be the product of all these primes $N = p_1p_2 \cdots p_r$. Now if we look at N, $p_i|N$ for all $1 \leq i \leq r$. But this would mean that $p_i \nmid N + 1$ for all i. This gives us two possibilities, either $N + 1$ itself is a prime or there exists some prime outside this set that divides $N + 1$. Either way we get a contradiction and hence the number of primes cannot be finite.

Theorem 8: Given any positive integer n, there exist n consecutive composite integers.

Proof: Consider the n integers

$$(n + 1)! + 2, (n + 1)! + 3, \ldots, (n + 1)! + n, (n + 1)! + (n + 1).$$

Note that k divides $(n + 1)! + k$ if $2 \leq k \leq (n + 1)$ and $(n + 1)! + k > k$. Thus, every number of the sequence is a composite number. Hence, we get n consecutive composite numbers. Thus, there are arbitrarily large gaps in the sequence of primes.

Example 15: If p is a prime greater than 3 then show that $2p+1$ and $4p+1$ cannot be primes simultaneously.

Solution: Since p is a prime greater than 3, p is either of the type $3k + 1$ or $3k + 2$. If p is of the type $3k + 1$ then $2p + 1 = 2(3k + 1) + 1 = 6k + 3 = 3(2k + 1)$. Hence, $3|(2p + 1)$ and $2p + 1$ cannot be a prime. Similarly, if p is of the type $3k + 2$ then 3 divides $4p + 1$ and it cannot be a prime.

2.6 Exercise 2.2

1. Prove that no integer in the sequence $11, 111, 1111, \ldots$ is a perfect square.

2. Show that for any positive integer m, $(ma, mb) = m(a, b)$.

3. Show that if $d|a$ and $d|b$ and $d > 0$ then

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a, b)}{d}.$$

4. Let d be any positive integer not equal to $2, 5$ or 13. Show that one can find distinct a, b in the set $\{2, 5, 13, d\}$ such that $ab - 1$ is not a perfect square (I.M.O. 1986).

5. By using Euclidean algorithm find the gcd of

$$(i)\ 7645 \text{ and } 2872 \quad (ii)\ 3645 \text{ and } 2357.$$

Also express the gcd as the linear combination of the given numbers.

6. Find $(a^{2^n} + 1, a^{2^n} + 1)$. Hence, show that there are infinitely many primes. (Due to Pólya.)

7. Let a, b, c be integers such that $(a, b) = 1, c > 0$. Prove that there is an integer x such that $(a + bx, c) = 1$.

8. Show that there are infinitely many primes of the type $6n - 1$.

9. Show that product of three consecutive integers is divisible by 3 while the product of four consecutive integers is divisible by 4.

10. Suppose m, n are integers and $m = n^2 - n$. Then show that $m^2 - 2m$ is divisible by 24.

11. A printer numbers the pages of a book starting with 1 and uses 3189 digits in all. How many pages does the book have?

12. Show that any integer divisible by 3 can be written as a sum of cubes of four integers.

13. Let $p > 3$ be an odd prime. Suppose

$$\sum_{k=1}^{p-1} \frac{1}{k} = \frac{a}{b}$$

where $(a, b) = 1$. Prove that a is divisible by p.

14. Prove that if $n \geq 4$ then $n, n + 2, n + 4$ cannot all be primes.

15. If $2 = p_1 < p_2 < \cdots < p_n$ where p_i are primes, show that the number $p_1 p_2 \cdots p_n + 1$ can never be a perfect square.

16. Prove that, if $n > 4$, then the number $1! + 2! + 3! + \cdots + n!$ is never a square.

17. The gcd of two positive integers is 81 and their l.c.m. is 5103. Find the numbers.

18. Prove that there are infinitely many positive integers a such that $2a$ is a square, $3a$ is a cube and $5a$ is a fifth power.

19. Let p_1, p_2, p_3 be primes with $p_2 \neq p_3$ such that $4 + p_1 p_2$ and $4 + p_1 p_3$ are perfect squares. Find all possible values of p_1, p_2, p_3.

20. If $2^n - 1$ is a prime, show that n is a prime.

21. If $2^n + 1$ is a prime, show that n is a power of 2.

22.

(a)Prove that, for any odd integer n, n^4 when divided by 16 always leaves remainder 1.

(b) Hence or otherwise show that we cannot find integers $n_1, n_2, \ldots, n_8$ such that

$$n_1^4 + n_2^4 + \cdots + n_8^4 = 1993.$$

23. Suppose p is a prime number such that $(p-1)/4$ and $(p+1)/2$ are also primes. Show that $p = 13$.

24. Show that if a prime number p is divided by 30, then the remainder is either a prime or is 1.

25. Prove that among any five consecutive positive integers there is one integer which is relatively prime to the other four integers. (Hint: For any two positive integers $m < n$, any common divisor has to be less than or equal to $n - m$).

---

3 Congruences

3.1 An introduction to Congruences

A **congruence** is a convenient statement about divisibility. The notion of congruence was introduced by C. F. Gauss (1777-1855) in his famous book *Disquisitiones Arithmeticae*, written at age 24. It gained ready acceptance as a fundamental tool for the study of number theory.

Definition Let m be a non-zero integer. The integers a and b are said to be congruent modulo m if and only if $m \mid (a-b)$, and written $a \equiv b \pmod{m}$.

Since, $a-b$ is divisible by m if and only if $a-b$ is divisible by $-m$, we will confine our attention to a positive modulus.

For example, $19 \equiv 1 \pmod{6}$. We can also say that x is even if $x \equiv 0 \pmod{2}$ and x is odd if $x \equiv 1 \pmod{2}$. Further, if x is even then $x^2 \equiv 0 \pmod{4}$ and if x is odd then $x^2 \equiv 1 \pmod{4}$.

Theorem 1 Let a, b, c, d, x, y denote integers. Then,

1. $a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$, and $a - b \equiv 0 \pmod{m}$ are equivalent statements.
2. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.
3. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then
$$ax + cy \equiv bx + dy \pmod{m}.$$
4. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$. In particular, if $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$ for every positive integer k.
5. If $a \equiv b \pmod{m}$ and $d \mid m$, then $a \equiv b \pmod{d}$.

Proof:

1. Suppose $a \equiv b \pmod{m}$. Then, by definition, $m \mid (a-b)$. Now, $m \mid a-b$ if and only if $m \mid (b-a)$ if and only if $m \mid a-b \Rightarrow 0$. Hence, $a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$, and $a-b \equiv 0 \pmod{m}$ are equivalent statements.
2. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $m \mid (a-b)$ and $m \mid (b-c)$. Hence, $m \mid (a-c)$, i.e. $a \equiv c \pmod{m}$.
3. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $m \mid (a-b)$ and $m \mid (c-d)$. Hence, $m \mid ((a-b)x + (c-d)y)$. Hence, $m \mid (ax + cy - (bx + dy))$, i.e.
$$ax + cy \equiv bx + dy \pmod{m}.$$
4. $m \mid (a-b)$ and $m \mid (c-d) \Rightarrow m \mid ((a-b) + b \cdot (c-d)) \Rightarrow m \mid (ac - bd)$. Hence, $ac \equiv bd \pmod{m}$. Equivalently, we can take $x = c$ and $y = b$ in 3 above to get the same result.
5. If $a \equiv b \pmod{m}$, then $m \mid (a-b)$. But $d \mid m$, hence, $d \mid (a-b)$ i.e. $a \equiv b \pmod{d}$.

Theorem 2 Let $f(x)$ denote a polynomial with integral coefficients. If $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$.

Proof: Assume that $f(x) = c_0 + c_1 x + \cdots + c_n x^n$, where c_i's are integers. Since $a \equiv b \pmod{m}$, we get $a^2 \equiv b^2 \pmod{m}$, ..., $a^n \equiv b^n \pmod{m}$. Hence, for every $j, 0 \leq j \leq n$, we get $c_j a^j \equiv c_j b^j \pmod{m}$. Hence,
$$\sum_{j=0}^{n} c_j a^j \equiv \sum_{j=0}^{n} c_j b^j \pmod{m},$$
that is $f(a) \equiv f(b) \pmod{m}$.

Example 1: Find the remainder when $13^{73} + 14^3$ is divided by 11.

Solution: We note that $13 \equiv 2 \pmod{11}$ and $14 \equiv 3 \pmod{11}$. Hence we have

$$14^3 \equiv 3^3 \equiv 5 \pmod{11}$$

Also $2^5 \equiv -1 \pmod{11}$. Hence $2^{70} \equiv 1 \pmod{11}$. Thus we get

$$13^{73} \equiv 2^{73} \equiv 8 \pmod{11}$$

Adding the congruences we get that

$$13^{73} + 14^3 \equiv 8 + 5 \equiv 2 \pmod{11}$$

Hence the remainder we get when we divide $13^{73} + 14^3$ by 11 is 2

Example 2: Show that a number is divisible by 3 if and only if the sum of its digits is divisible by 3.

Solution: Let n be a given number. n can be written as

$$n = n_0 + 10n_1 + \ldots + 10^k n_k,$$

where $0 \leq n_0, n_1, \ldots, n_k \leq 9$. Note that $10 \equiv 1 \pmod 3$. Hence, for every positive integer m, $10^m \equiv 1 \pmod 3$. Hence, $n \equiv n_0 + n_1 + \ldots + n_k \pmod 3$. This implies that n is divisible by 3 if and only if the sum of its digits is divisible by 3.

The above argument also works if we replace 3 by 9, i.e., a number is divisible by 9 if and only if the sum of its digits is divisible by 9.

Example 3: If p and q are primes such that $p = q + 2$, prove that $p^p + q^q$ is a multiple of $p + q$.

Solution: We note that as p and q are primes such that $p = q + 2$, both p and q are odd primes. Hence, $q - 1$ is even. Consider

$$p^p + q^q = (p + q - q)^p + q^q \equiv (-q)^p + q^q \pmod{p+q} \equiv -q^p + q^q \pmod{p+q}.$$

Now $p + q = 2q + 2$ and $2 \mid q - 1$. Hence, $p + q = 2(q + 1)$ divides $q^2 - 1$. Hence, $p^p + q^q \equiv 0 \pmod{p+q}$, that is, $p^p + q^q$ is a multiple of $p + q$.

Example 4: Prove that $2^p + 3^p$ is not a perfect power (i.e. perfect square, cube etc.) if p is a prime number

Solution: If $p = 2$, then $2^2 + 3^2 = 13$ is not a perfect power.

Suppose that p is odd. Then $2^p + 3^p = (2 + 3) \sum_{k=0}^{p-1} (-1)^k 2^{p-1-k} 3^k$.

Now $3 \equiv -2 \pmod 5$. Hence, modulo 5, the sum

$$\sum_{k=0}^{p-1} (-1)^k 2^{p-1-k} 3^k \equiv \sum_{k=0}^{p-1} (-1)^k 2^{p-1-k} (-2)^k \equiv p2^{p-1} \pmod 5.$$

Hence, if $p \neq 5$, then $2^p + 3^p = 5n$, where $n \not\equiv 0 \pmod 5$, so that $2^p + 3^p$ is not a perfect power. Finally, $2^5 + 3^5 = 275$ is not a perfect power.

Example 5: Let $f(m, n) = 36^m - 5^n$, where m, n are natural numbers. Find the smallest value of $|f(m, n)|$. Justify your answer.

Solution. We note that $f(1, 2) = 11$. Further, $f(m, n)$ is odd, $f(m, n)$ is not a multiple of 3 and $f(m, n) \equiv 1 \pmod 5$. Thus, the only possible value less than 11 that $|f(m, n)|$ can take is 1. We now show that $|f(m, n)| \neq 1$. Now

$$|f(m, n)| = 1 \Rightarrow 36^m - 5^n = \pm 1 \Rightarrow 36^m \pm 1 = 5^n.$$

But modulo 5, $36^m \equiv 1 \pmod 5$ gives $2 \equiv 0 \pmod 5$, a contradiction, and going modulo 4, $36^m - 1 \equiv 5^n$ gives $-1 \equiv 1 \pmod 4$, a contradiction. Thus, the smallest value of $|f(m, n)|$ is 11.

3.2 Exercise 3.1

1. Show that the square of an odd integer is $\equiv 1 \pmod 8$.

2. Show that the square of an integer is $\equiv 0$ or $\equiv 1 \pmod 3$.

3. Find all primes p such that both p and $p^2 + 8$ are primes.

4. Show that the square of an integer is $\equiv 0, 1, -1 \pmod 5$.

5. Show that if $2n + 1$ and $3n + 1$ are both perfect squares then $40 \mid n$.

6. If an integer n is coprime to 6, then show that $n^2 \equiv 1 \pmod{24}$.

7. Let n be an integer. Show that if $2 + 2\sqrt{28n^2 + 1}$ is an integer, then it must be a perfect square.

8. If $a \equiv b \pmod{m^n}$, then prove that $a^m \equiv b^m \pmod{m^{n+1}}$.

9. If $(a, b) = 1$, then show that $\gcd\left(\frac{a^p - b^p}{a-b}, a - b\right) = 1$ or p.

3.3 Residue Systems: Fermat and Euler

Definition If $x \equiv y \pmod{m}$ then y is called a residue of x modulo m. A set $x_1, x_2, \ldots, x_m$ is called a *complete residue system* modulo m if for every integer y there exists a unique x_j such that $y \equiv x_j \pmod{m}$.

Definition A *reduced residue system* modulo m is a set of integers r_i such that $(r_i, m) = 1$, $r_i \not\equiv r_j \pmod{m}$ if $i \neq j$, and such that every x prime to m, is congruent to some member r_i of the set.

Example 1: Let m be any positive integer. Then $\{0, 1, 2, \ldots, m-1\}$ is a complete residue system modulo m. If $m = p$, a prime, then $\{1, 2, \ldots, p-1\}$ is a reduced residue system modulo p. $\{1, 5\}$ is a reduced residue system modulo 6 while $\{1, 3, 7, 9\}$ is a reduced residue system modulo 10. We also note that $\{1, 3, 3^3, 3^3\}$ is also a reduced residue system modulo 10.

Theorem 1: Let $(a, m) = 1$. Let $r_1, \ldots, r_n$ be a complete or reduced residue system modulo m. Then $ar_1, \ldots, ar_n$ is a complete or reduced residue system modulo m.

Definition The number $\phi(m)$ is the number of positive integers less than or equal to m and relatively prime to m.

Equivalently, $\phi(m)$ is the number of elements in a reduced residue system modulo m. For example, $\phi(6) = 2$, $\phi(8) = 4$, $\phi(11) = 10$ and $\phi(p) = p - 1$ if and only if p is a prime.

Theorem 2: For $n \geq 1$,

$$\sum_{d|n} \phi(d) = n.$$

Proof: Let $S = \{1, 2, \ldots, n\}$. For every positive divisor d of n, let

$$S_d = \{m \in S \mid \gcd(m, n) = d\}.$$

Then, clearly, these sets S_d are pairwise disjoint and their union is S. Also $\gcd(m, n) = d$ if and only if $\gcd(m/d, n/d) = 1$. Hence the number of integers in the set S_d is equal to the number of positive integers $\leq n/d$ which are relatively prime to n/d; i.e. equal to $\phi(n/d)$. Hence $n = \sum_{d|n} \phi\left(\frac{n}{d}\right)$. But as d runs through all positive divisors of n, so does n/d. Hence

$$\sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d) = n.$$

Theorem 3 (Euler's theorem) Let a, m be integers such that $(a, m) = 1$. Then

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

Proof: Let $r_1, r_2, \ldots, r_{\phi(m)}$ be a reduced residue system modulo m. Since $(a, m) = 1$, using Theorem 12, $ar_1, ar_2, \ldots, ar_{\phi(m)}$ is also a reduced residue system modulo m. Hence we get,

$$\prod_{i=1}^{\phi(m)} ar_i = a^{\phi(m)} \prod_{i=1}^{\phi(m)} r_i \equiv \prod_{i=1}^{\phi(m)} r_i \pmod{m}.$$

That is, $m \mid \prod_{i=1}^{\phi(m)} r_i (a^{\phi(m)} - 1)$. Since $\left(\prod_{i=1}^{\phi(m)} r_i, m\right) = 1$, using Euclid's lemma we get $m \mid a^{\phi(m)} - 1$. Hence, the theorem.

Theorem 4 (Fermat's theorem) Let p be a prime and a be an integer. Then

$$a^p \equiv a \pmod{p}$$

Proof: If $p \mid a$ then $a^p \equiv a \pmod{p}$. If $p \nmid a$ then $(a, p) = 1$. Since $\phi(p) = p - 1$, using (5) we get $a^{p-1} \equiv 1 \pmod{p}$, hence $a^p \equiv a \pmod{p}$.

Example 2: If $n \in \mathbb{N}$ such that $(n, 35) = 1$ then $n^{12} \equiv 1 \pmod{35}$

Solution: Since n and $35 = 5 \times 7$ have no common factor, we can say that $5 \nmid n$ and $7 \nmid n$. Hence by Euler's Theorem we have $n^4 \equiv 1 \pmod 5$ which implies that $n^{12} \equiv 1 \pmod 5$. Similarly $n^6 \equiv 1 \pmod 7$ which implies that $n^{12} \equiv 1 \pmod 7$. Combining these two we get that $n^{12} \equiv 1 \pmod{35}$

Example 3: If p, q are odd primes such that $2p = q + 1$, and a is relatively prime to 2, p and q, prove that $a^{2(p-1)} \equiv 1 \pmod{16pq}$.

Solution: Note that a is odd as a is relatively prime to 2. Now, $a^{2(p-1)} - 1 = (a^{p-1} - 1)(a^{p-1} + 1)$. Since, p is an odd prime, $p - 1$ is even and $a^{p-1} - 1$ is divisible by 8. Also, $a^{p-1} + 1$ is divisible by 2. Thus,

$$a^{2(p-1)} \equiv 1 \pmod{16} \quad (1).$$

Since, a is relatively prime to p, we get $a^{p-1} \equiv 1 \pmod p$. Hence,

$$a^{2(p-1)} \equiv 1 \pmod p \quad (2).$$

Since, a is relatively prime to q and $q - 1 = 2p - 2 = 2(p - 1)$, we get

$$a^{2(p-1)} \equiv 1 \pmod q \quad (3).$$

Using the fact that 2, p and q are relatively prime in pairs and combining (1), (2) and (3) we get $a^{2(p-1)} \equiv 1 \pmod{16pq}$.

Example 4: Prove that 504 divides $n^9 - n^3$, where n is an integer.

Solution: We note that $504 = 7 \times 8 \times 9$. If n is even then $8 \mid n^3$ while if n is odd then $8 \mid n^2 - 1$. Hence, for every n $8 \mid n^3(n^2 - 1)$. But $n^3(n^2 - 1) \mid n^3(n^6 - 1)$. Hence, $8 \mid n^9 - n^3$ for every integer n.

Now either $3 \mid n$ or $3 \nmid n$. If $3 \mid n$ then $9 \mid n^2$. Hence, $9 \mid n^3$. If $3 \nmid n$ then $(3, n) = 1$. This implies that $(9, n) = 1$. By Euler's theorem, we get $9 \mid n^6 - 1$. Thus, in either case $9 \mid n^9 - n^3$.

Similarly, either $7 \mid n$ or $7 \nmid n$. If $7 \mid n$ then $7 \mid n^3$. If $7 \nmid n$ then $(7, n) = 1$. By Euler's theorem, we get $7 \mid n^6 - 1$. Thus, in either case $7 \mid n^9 - n^3$.

Since, 7, 8 and 9 are relatively prime in pairs and each divides $n^9 - n^3$ we get that their product 504 divides $n^9 - n^3$.

Defintion Let $m \neq 0$. If $(a, m) = 1$, an integrer a' such that $aa' \equiv 1 \pmod m$ is called an inverse of a modulo m

Example 5: The following table shows the inverses of $1, \ldots, 12$ modulo 13.

number	1	2	3	4	5	6	7	8	9	10	11	12
inverse	1	7	9	10	8	11	2	5	3	4	6	12

Remark : Since $(a, m) = 1$, there exist integers b, c such that $ab + mc = 1$. Hence, $ab \equiv 1 \pmod m$. This shows that if $(a, m) = 1$, a has an inverse modulo m. Further, if b and c are inverses of $a \pmod m$ then $m \mid a(b - c)$. Using Euclid's lemma, we get $b \equiv c \pmod m$. Thus, the inverse is unique modulo m.

Let b and c be integers congruent $\pmod m$ and b' be the inverse of $b \pmod m$. Then $cb' \equiv bb' \equiv 1 \pmod m$. Hence, both b and c have the same inverse modulo m. Hence, the integers congruent modulo m have the same inverse modulo m.

Theorem 4 (Wilson's theorem) Let p be a prime. Then

$$(p - 1)! \equiv -1 \pmod p. \quad (7)$$

Proof. The result can easily be verified for $p = 2$ and $p = 3$. We assume that $p \geq 5$. Now, given an integer i such that $1 \leq i \leq p-1$ there exists a unique j such that $ij \equiv ji \equiv 1 \pmod{p}$, $1 \leq j \leq p-1$. Moreover $i = j$ if and only if $i = 1$ or $p-1$. Hence, $(p-2)! \equiv 1 \pmod{p}$. Hence,

$$(p-1)! \equiv p-1 \equiv -1 \pmod{p}.$$

Remark : Note that n is prime if and only if $(n-1)! \equiv -1 \pmod{n}$.

Theorem 5 Let p denote a prime. Then $x^2 \equiv -1 \pmod{p}$ has solutions if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.

Proof. If $p = 2$ we have the solution $x = 1$. For any odd prime we can write Wilson's theorem in the form

$$\prod_{j=1}^{(p-1)/2} j(p-j) \equiv -1 \pmod{p}.$$

But $j(p-j) \equiv -j^2 \pmod{p}$, and we get

$$(-1)^{(p-1)/2} \prod_{j=1}^{(p-1)/2} j^2 \equiv -1 \pmod{p}.$$

Hence for $p \equiv 1 \pmod{4}$, we get a solution of $x^2 \equiv -1 \pmod{p}$.

Suppose $p \neq 2$ or $p \not\equiv 1 \pmod{4}$ then $p \equiv 3 \pmod{4}$. In this case, if for some integer x, we have $x^2 \equiv -1 \pmod{p}$, then

$$(x^2)^{(p-1)/2} \equiv -1^{(p-1)/2} \pmod{p}.$$

Hence $x^{p-1} \equiv -1 \pmod{p}$. Since $(p, x) = 1$ we get $p \mid 2$, a contradiction.

Example 6: Let p be an odd prime. Prove that

$$1^2 \cdot 3^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$$

and

$$2^2 \cdot 4^2 \cdots (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

Solution. By Wilson's theorem,

$$(1 \cdot 3 \cdots (p-2))(2 \cdot 4 \cdots (p-1)) \equiv -1 \pmod{p}.$$

On the other hand,

$$1 \equiv -(p-1) \pmod{p}, \quad 3 \equiv -(p-3) \pmod{p}, \ldots, p-2 \equiv -(p-(p-2)) \pmod{p}.$$

Therefore,

$$1 \cdot 3 \cdots (p-2) \equiv (-1)^{\frac{p-1}{2}} (2 \cdot 4 \cdots (p-1)) \pmod{p}.$$

Multiplying the two congruences and canceling out the product $2 \cdot 4 \cdots (p-1)$, we obtain the first congruence from the statement. Switching the sides in the second and multiplying the congruences again, we obtain the second congruence from the statement.

3.4 Exercise 3.2

1. Let n be an even positive integer. Prove that $n^2 - 1$ divides $2^{n!} - 1$.

2. Let $a > 1$ be an integer. Show that the set

$$S = \{a^2 + a - 1, a^3 + a^2 - 1, a^4 + a^3 - 1, \ldots\}$$

contains an infinite subset whose elements are pairwise coprime.

3. Prove that the system

$$x^6 + x^3 + x^3y + y = 147^{157},$$
$$x^3 + x^3y + y^2 + y + z^9 = 157^{147}$$

has no solutions in integers x, y, and z.

4. Show that for every prime p there is an integer n such that $2^n + 3^n + 6^n - 1$ is divisible by p.

5.Show that if n has $p - 1$ digits all equal to 1, where p is a prime not equal to 2, 3, or 5, then n is divisible by p.

6.Prove that for any prime $p > 17$, the number

$$p^{32} - 1$$

is divisible by 16320.

7. Let p be an odd prime number. Show that if the equation $x^2 \equiv a \pmod{p}$ has a solution, then $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Conclude that there are infinitely many primes of the form $4m + 1$.

8. Prove that the equation $x^2 = y^3 + 7$ has no integer solutions.

9. Let $n > 1$ be a positive integer. Prove that the equation $(x + 1)^n - x^n = ny$ has no positive integer solutions.

3.5 Problems from contests

1. [RMO-24] Let $S = \{(a,b,c,d) \in \mathbb{N}^4 : a^2+b^2+c^2 = d^2\}$. Then find the largest $m \in \mathbb{N}$ such that m divides $abcd$ for all $(a,b,c,d) \in S$.

Solution: Observe that $d^2 \equiv 0,1 \pmod 4$. Thus out of a,b,c at most one of them can be odd. This follows beacause if two of them are odd then $d^2 \equiv 2 \pmod 4$ and if all of them are odd then $d^2 \equiv 3 \pmod 4$ both of which are not possible. Now since at least 2 of them are even, 4 divides the product $abcd$.

Now we know $n^2 \equiv 0,1 \pmod 3$. If three divides one of a,b,c then 3 divides the product $abcd$. If not then

$$d^2 \equiv a^2+b^2+c^2 \equiv 1+1+1 \equiv 0 \pmod 3$$

which means that 3 divides the product $abcd$ for all $(a,b,c,d) \in S$. Thus combining the two, we can say that 12 divides the product $abcd$ for all $(a,b,c,d) \in S$.

Now the question is "Is 12 the largest number that can divide this product in every case?". Assume that the largest m that divides the product is of the form $12k$ for some $k \in \mathbb{N}$. Since $(1,2,2,3) \in S$, for $12k$ to divide the product we would need $k = 1$. Hence 12 is indeed the largest number that will divides the product $abcd$ for all $(a,b,c,d) \in S$.

2. [ISI-18] Let $a,b,c \in \mathbb{N}$ such that $a^2+b^2 = c^2$ and $c - b = 1$. The show that

1. a is odd
2. b is divisible by 4
3. $a^b + b^a$ is divisible by c

Solution:

1. We know that $a^2+b^2 = c^2$. Now $c = b+1$. Substituting this we get that $a^2 = (b+1)^2 - b^2 = 2b+1$ which implies a is odd.
2. Form the first part, we get that a is odd which means that $a^2 \equiv 1 \pmod 8$ that is $8|(a^2-1)$. Thus we can write $a^2 - 1 = 8m$ for some $m \in \mathbb{Z}$. Now, we also have that $b = (a^2-1)/2$ which implies that $b = 4m$ and hence 4 divides b.
3. Showing that c divides $a^b + b^a$ is the same as showing that $(b+1)$ divides the sum. Now we can say that $b \equiv -1 \pmod{(b+1)}$ and since a is odd we have $b^a \equiv -1 \pmod{b+1}$. This means that $b+1$ divides b^a+1 which gives c divides b^a+1.

   Now, $a^2 = 2b+1$ which implies $a^2+1 = 2(b+1) = 2c$. Since b is a multiple of 4, a^4-1 divides a^b-1 which further implies that a^2-1 which is a factor of a^4-1 divides a^b-1. Thus c divides a^b-1. Now combing the two results, we can say that c divides $(a^b-1)+(b^a-1) = (a^b+b^a)$

3. [CMI-23] We want to find *odd* integers $n > 1$ for which n is a factor of $2023^n - 1$.

(a) Find the two smallest such integers.

(b) Prove that there are infinitely many such integers.

Solution: (a) 2023 is 1 mod 3, so $n = 3$ works. Similarly using modular arithmetic one checks that 5 and 7 do not work but 9 does. (b) If $n = k$ works so does $n = 3k$ by induction:

$$2023^{3k} - 1 = (2023^k - 1)(2023^{2k} + 2023^k + 1) = (\text{multiple of } k)(\text{multiple of } 3)$$

as each summand in the second factor is 1 mod 3. Thus all powers of 3 satisfy the required condition.

---

4 The Greatest Integer Function

4.1 The Box function

For real x, the symbol $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x. Thus, we note that $\lfloor \pi \rfloor = 3$, $\lfloor e \rfloor = 2$, $\lfloor -\pi \rfloor = -4$.

Theorem 1: Let x and y be real numbers. Then we have

1. $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$ and $x - 1 < \lfloor x \rfloor \leq x$, $0 \leq x - \lfloor x \rfloor < 1$.
2. If $x \geq 0$, $\lfloor x \rfloor = \sum_{1 \leq i \leq x} 1$.
3. $\lfloor x + m \rfloor = \lfloor x \rfloor + m$ if m is an integer.
4. $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$.
5. $\lfloor x \rfloor + \lfloor -x \rfloor = \begin{cases} 0 & \text{if } x \text{ is an integer,} \\ -1 & \text{otherwise.} \end{cases}$
6. $\left\lfloor \frac{\lfloor x \rfloor}{m} \right\rfloor = \left\lfloor \frac{x}{m} \right\rfloor$ if m is a positive integer.
7. $x - \lfloor x \rfloor$ is the fractional part of x and is denoted by $\{x\}$.
8. $-\lfloor -x \rfloor$ is the least integer $\geq x$.
9. $\lfloor x + 0.5 \rfloor$ is the nearest integer to x. If two integers are equally near to x, $\lfloor x + 0.5 \rfloor$ denotes the larger of the two.
10. If a and b are positive integers, $\left\lfloor \frac{b}{a} \right\rfloor$ is the number of integers among $1, 2, \ldots, n$ that are divisible by a. Thus, $b = aq + r, 0 \leq r < a$ can also be written as

$$b = a \left\lfloor \frac{b}{a} \right\rfloor + r.$$

Example 1: For every positive integer n, show that

$$\left\lfloor \sqrt{n} + \sqrt{n+1} \right\rfloor = \left\lfloor \sqrt{4n+1} \right\rfloor = \left\lfloor \sqrt{4n+2} \right\rfloor = \left\lfloor \sqrt{4n+3} \right\rfloor.$$

Solution: Note that $\left(\sqrt{n} + \sqrt{n+1}\right)^2 = 2n+1+2\sqrt{n(n+1)}$ and as $n \geq 1$, $n < \sqrt{n(n+1)} < n+1$. Consequently $4n+1 < \left(\sqrt{n} + \sqrt{n+1}\right)^2 < 4n+3$, which gives

$$\sqrt{4n+1} < \sqrt{n} + \sqrt{n+1} < \sqrt{4n+3}. \quad (1)$$

Also, there always exist an integer k such that

$$k^2 \leq 4n+1 < (k+1)^2.$$

Since a square cannot be congruent to 2 or 3 (mod 4), we have

$$k^2 \leq 4n+1 < 4n+2 < 4n+3 < (k+1)^2,$$

i.e.,

$$k \leq \sqrt{4n+1} < \sqrt{4n+2} < \sqrt{4n+3} < (k+1). \quad (2)$$

Combining (1) and (2), we get the required result.

Theorem 2 (Polignac's formula) If p is a prime number and n a positive integer, then the exponent of p in $n!$ is given by

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots .$$

Proof: Each multiple of p between 1 and n contributes a factor of p to $n!$. There are $\left\lfloor \frac{n}{p} \right\rfloor$ such factors. But the multiples of p^2 contribute yet another factor of p, so one should add $\left\lfloor \frac{n}{p^2} \right\rfloor$. And then come the multiples of p^3 and so on.

Example 2: Let m be an integer greater than 1. Prove that the product of m consecutive terms in an arithmetic progression is divisible by $m!$ if the ratio of the progression is coprime to m.

Solution: Let p be a prime that divides $n!$. The exponent of p in $n!$ is given by Polignac's formula. On the other hand, in the product $a(a+r)(a+2r)\cdots(a+(m-1)r)$ of m consecutive terms in a progression of ratio r, with $\gcd(r,m)=1$, at least $\left\lfloor \frac{m}{p^i} \right\rfloor$ terms are divisible by p^i. It follows that the power of p in this product is greater than or equal to the power of p in $m!$. Because this holds true for any prime factor in $m!$, the conclusion follows.

Example 3 [CMI-17] The domain of a function f is the set of natural numbers. The function is defined as follows:

$$f(n) = n + \lfloor \sqrt{n} \rfloor$$

where $\lfloor k \rfloor$ denotes the nearest integer smaller than or equal to k. For example, $\lfloor \pi \rfloor = 3$, $\lfloor 4 \rfloor = 4$. Prove that for every natural number m the following sequence contains at least one perfect square

$$m, f(m), f^2(m), f^3(m), \ldots$$

The notation f^k denotes the function obtained by composing f with itself k times, e.g., $f^2 = f \circ f$.

Solution: If m is itself a square then we are done. So assume that $m = k^2 + j$ for $1 \le j \le 2k$. Hence we have $f(m) = k^2 + j + k$. Consider the following two sets

$$A = \{m \text{ a natural number } \mid m = k^2 + j \text{ and } 0 \le j \le k\}.$$

$$B = \{m \text{ a natural number } \mid m = k^2 + j \text{ and } k+1 \le j \le 2k\}.$$

Suppose m is in the set B. Then

$$f(m) = k^2 + j + k = (k+1)^2 + (j-k-1).$$

Hence $f(m)$ is either a square or is in A. Thus it is enough to assume that $m \in A$. In that case $k^2 < f(m) < (k+1)^2$, so $\lfloor f(m) \rfloor = k$. Therefore

$$f^2(m) = (k+1)^2 + (j-1).$$

This clearly implies that $f^{2j}(m) = (k+j)^2$.

4.2 Exercise 4.1

1. For a positive integer n and a real number x, prove the identity

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{n} \right\rfloor + \cdots + \left\lfloor x + \frac{n-1}{n} \right\rfloor = \lfloor nx \rfloor .$$

2. For p and q coprime positive integers, prove the reciprocity law

$$\left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + \cdots + \left\lfloor \frac{(q-1)p}{q} \right\rfloor = \left\lfloor \frac{q}{p} \right\rfloor + \left\lfloor \frac{2q}{p} \right\rfloor + \cdots + \left\lfloor \frac{(p-1)q}{p} \right\rfloor .$$

3. Prove that for any real number x and for any positive integer n,

$$\lfloor nx \rfloor \geq \frac{\lfloor x \rfloor}{1} + \frac{\lfloor 2x \rfloor}{2} + \frac{\lfloor 3x \rfloor}{3} + \cdots + \frac{\lfloor nx \rfloor}{n}.$$

4. Find the locus of the points (x, y) that satisfy $\lfloor x \rfloor^2 + \lfloor y \rfloor^2 = 4$

5. Find all positive integers n such that $n!$ ends in exactly 1000 zeros.

6. Prove that $n!$ is not divisible by 2^n for any positive integer n.

7. Show that for each positive integer n,

$$n! = \prod_{i=1}^{n} \operatorname{lcm}\left(1, 2, \ldots, \left\lfloor \frac{n}{i} \right\rfloor\right),$$

---

5 Arithmetic Functions

5.1 No of divisors and Sum of divisors

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** (or **arithmetic**) function. Although the value of a number-theoretic function is not required to be a positive integer or, for that matter, even an integer, most of the number-theoretic functions that we shall encounter are integer-valued. Among the easiest to handle, and the most natural, are the functions τ and σ.

Definition: 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.

For an example of these notions, consider $n = 12$. Because 12 has the positive divisors 1, 2, 3, 4, 6, 12, we find that

$$\tau(12) = 6 \quad \text{and} \quad \sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28.$$

For the first few integers,

$$\tau(1) = 1 \quad \tau(2) = 2 \quad \tau(3) = 2 \quad \tau(4) = 3 \quad \tau(5) = 2 \quad \tau(6) = 4, \ldots$$

$$\sigma(1) = 1, \sigma(2) = 3, \sigma(3) = 4, \sigma(4) = 7, \sigma(5) = 6, \sigma(6) = 12, \ldots$$

It is not difficult to see that $\tau(n) = 2$ if and only if n is a prime number; also, $\sigma(n) = n + 1$ if and only if n is a prime.

Before studying the functions τ and σ in more detail, we wish to introduce notation that will clarify a number of situations later. It is customary to interpret the symbol

$$\sum_{d|n} f(d)$$

to mean, "Sum the values $f(d)$ as d runs over all the positive divisors of the positive integer n." For instance, we have

$$\sum_{d|20} f(d) = f(1) + f(2) + f(4) + f(5) + f(10) + f(20).$$

With this understanding, τ and σ may be expressed in the form

$$\tau(n) = \sum_{d|n} 1 \quad \sigma(n) = \sum_{d|n} d.$$

The notation $\sum_{d|n} 1$, in particular, says that we are to add together as many 1's as there are positive divisors of n. To illustrate: the integer 10 has the four positive divisors 1, 2, 5, 10, whence

$$\tau(10) = \sum_{d|10} 1 = 1 + 1 + 1 + 1 = 4$$

and

$$\sigma(10) = \sum_{d|10} d = 1 + 2 + 5 + 10 = 18.$$

Our first theorem makes it easy to obtain the positive divisors of a positive integer n once its prime factorization is known.

Theorem 1: If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then the positive divisors of n are precisely those integers d of the form

$$d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

where $0 \leq a_i \leq k_i$ $(i = 1, 2, \ldots, r)$.

Proof: Note that the divisor $d = 1$ is obtained when $a_1 = a_2 = \cdots = a_r = 0$, and n itself occurs when $a_1 = k_1, a_2 = k_2, \ldots, a_r = k_r$. Suppose that d divides n nontrivially; say, $n = dd'$, where $d > 1, d' > 1$. Express both d and d' as products of (not necessarily distinct) primes:

$$d = q_1 q_2 \cdots q_s \quad d' = t_1 t_2 \cdots t_u$$

with q_i, t_j prime. Then

$$p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = q_1 \cdots q_s t_1 \cdots t_u$$

are two prime factorizations of the positive integer n. By the uniqueness of the prime factorization, each prime q_i must be one of the p_j. Collecting the equal primes into a single integral power, we get

$$d = q_1 q_2 \cdots q_s = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

where the possibility that $a_i = 0$ is allowed.

Conversely, every number $d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ $(0 \leq a_i \leq k_i)$ turns out to be a divisor of n. For we can write

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = (p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r})(p_1^{k_1 - a_1} p_2^{k_2 - a_2} \cdots p_r^{k_r - a_r}) = dd'$$

with $d' = p_1^{k_1 - a_1} p_2^{k_2 - a_2} \cdots p_r^{k_r - a_r}$ and $k_i - a_i \geq 0$ for each i. Then $d' > 0$ and $d \mid n$.

We put this theorem to work at once.

Theorem 2: If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then

(a) $\tau(n) = (k_1+1)(k_2+1)\cdots(k_r+1)$, and

(b) $\sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1} \cdot \frac{p_2^{k_2+1}-1}{p_2-1} \cdot \ldots \cdot \frac{p_r^{k_r+1}-1}{p_r-1}$.

Proof: According to Theorem 6.1, the positive divisors of n are precisely those integers $d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ where $0 \leq a_i \leq k_i$. There are k_1+1 choices for the exponent a_1; k_2+1 choices for a_2; $\ldots$; and k_r+1 choices for a_r. Hence, there are

$$(k_1+1)(k_2+1)\cdots(k_r+1)$$

possible divisors of n.

To evaluate $\sigma(n)$, consider the product

$$(1 + p_1 + p_1^2 + \cdots + p_1^{k_1})(1 + p_2 + p_2^2 + \cdots + p_2^{k_2}) \cdots (1 + p_r + p_r^2 + \cdots + p_r^{k_r}).$$

Each positive divisor of n appears once and only once as a term in the expansion of this product, so that

$$\sigma(n) = (1 + p_1 + p_1^2 + \cdots + p_1^{k_1}) \cdots (1 + p_r + p_r^2 + \cdots + p_r^{k_r}).$$

Applying the formula for the sum of a finite geometric series to the i-th factor on the right-hand side, we get

$$1 + p_i + p_i^2 + \cdots + p_i^{k_i} = \frac{p_i^{k_i+1}-1}{p_i-1}.$$

It follows that

$$\sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1} \cdot \frac{p_2^{k_2+1}-1}{p_2-1} \cdot \ldots \cdot \frac{p_r^{k_r+1}-1}{p_r-1}.$$

Example 1: The number $180 = 2^2 \cdot 3^2 \cdot 5$ has

$$\tau(180) = (2+1)(2+1)(1+1) = 18$$

positive divisors. These are integers of the form

$$2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3}$$

where $a_1 = 0, 1, 2;$ $a_2 = 0, 1, 2;$ and $a_3 = 0, 1$. Specifically, we obtain

$$1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 30, 36, 45, 60, 90, 180.$$

The sum of these integers is

$$\sigma(180) = \frac{2^3-1}{2-1} \cdot \frac{3^3-1}{3-1} \cdot \frac{5^2-1}{5-1} = \frac{7}{1} \cdot \frac{26}{2} \cdot \frac{24}{4} = 7 \cdot 13 \cdot 6 = 546.$$

5.2 Multiplicative Functions

Definition: A number-theoretic function f is said to be *multiplicative* if

$$f(mn) = f(m)f(n)$$

whenever $\gcd(m, n) = 1$.

For simple illustrations of multiplicative functions, we need only consider the functions given by $f(n) = 1$ and $g(n) = n$ for all $n \geq 1$. It follows by induction that if f is multiplicative and $n_1, n_2, \ldots, n_r$ are positive integers that are pairwise relatively prime, then

$$f(n_1 n_2 \cdots n_r) = f(n_1)f(n_2)\cdots f(n_r).$$

Multiplicative functions have one big advantage for us: they are completely determined once their values at prime powers are known. Indeed, if $n > 1$ is a given positive integer, then we can write $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ in canonical form; because the $p_i^{k_i}$ are relatively prime in pairs, the multiplicative property ensures that

$$f(n) = f(p_1^{k_1}) f(p_2^{k_2}) \cdots f(p_r^{k_r}).$$

If f is a multiplicative function that does not vanish identically, then there exists an integer n such that $f(n) \neq 0$. But

$$f(n) = f(n \cdot 1) = f(n) f(1).$$

Being nonzero, $f(n)$ may be canceled from both sides of this equation to give $f(1) = 1$. The point to which we wish to call attention is that $f(1) = 1$ for any multiplicative function not identically zero.

We now establish that τ and σ have the multiplicative property.

Theorem 3: The functions τ and σ are both multiplicative functions.

Proof. Let m and n be relatively prime integers. Because the result is trivially true if either m or n is equal to 1, we may assume that $m > 1$ and $n > 1$. If

$$m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \quad \text{and} \quad n = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$$

are the prime factorizations of m and n, then because $\gcd(m, n) = 1$, no p_i can occur among the q_j. It follows that the prime factorization of the product mn is given by

$$mn = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} q_1^{j_1} \cdots q_s^{j_s}.$$

Appealing to Theorem 2, we obtain

$$\tau(mn) = [(k_1 + 1) \cdots (k_r + 1)][(j_1 + 1) \cdots (j_s + 1)] = \tau(m)\tau(n).$$

In a similar fashion, Theorem 2 gives

$$\sigma(mn) = \left[\frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1} \right] \left[\frac{q_1^{j_1+1} - 1}{q_1 - 1} \cdots \frac{q_s^{j_s+1} - 1}{q_s - 1} \right] = \sigma(m)\sigma(n).$$

Thus, τ and σ are multiplicative functions.

Lemma: If $\gcd(m, n) = 1$, then the set of positive divisors of mn consists of all products $d_1 d_2$, where $d_1 \mid m$, $d_2 \mid n$, and $\gcd(d_1, d_2) = 1$; furthermore, these products are all distinct.

Proof: It is harmless to assume that $m > 1$ and $n > 1$; let $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ and $n = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$ be their respective prime factorizations. Inasmuch as the primes $p_1, \ldots, p_r, q_1, \ldots, q_s$ are all distinct, the prime factorization of mn is

$$mn = p_1^{k_1} \cdots p_r^{k_r} q_1^{j_1} \cdots q_s^{j_s}.$$

Hence, any positive divisor d of mn will be uniquely representable in the form

$$d = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s} \quad \text{where} \quad 0 \leq a_i \leq k_i,\ 0 \leq b_i \leq j_i.$$

This allows us to write d as $d = d_1 d_2$, where $d_1 = p_1^{a_1} \cdots p_r^{a_r}$ divides m and $d_2 = q_1^{b_1} \cdots q_s^{b_s}$ divides n. Because no p_i is equal to any q_j, we surely must have $\gcd(d_1, d_2) = 1$.

Theorem 4: If f is a multiplicative function and F is defined by

$$F(n) = \sum_{d \mid n} f(d),$$

then F is also multiplicative.

Proof: Let m and n be relatively prime positive integers. Then

$$F(mn) = \sum_{d|mn} f(d) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2)$$

because every divisor d of mn can be uniquely written as a product of a divisor d_1 of m and a divisor d_2 of n, where $\gcd(d_1, d_2) = 1$. By the definition of a multiplicative function,

$$f(d_1 d_2) = f(d_1) f(d_2).$$

It follows that

$$F(mn) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1) f(d_2) = \left(\sum_{d_1|m} f(d_1) \right) \left(\sum_{d_2|n} f(d_2) \right) = F(m)F(n).$$

Corollary. The functions τ and σ are multiplicative functions.

Proof. We have mentioned that the constant function $f(n) = 1$ is multiplicative, as is the identity function $f(n) = n$. Because τ and σ may be represented in the form

$$\tau(n) = \sum_{d|n} 1 \quad \text{and} \quad \sigma(n) = \sum_{d|n} d,$$

the stated result follows immediately from Theorem 4.

5.3 Exercise 6.1

1. For any integer $n \geq 1$, establish the inequality $\tau(n) \leq 2n$.

2. Prove the following.

(a) $\tau(n)$ is an odd integer if and only if n is a perfect square.

(b) $\sigma(n)$ is an odd integer if and only if n is a perfect square or twice a perfect square.

3. Show that $\sum_{d|n} \frac{1}{d} = \frac{\sigma(n)}{n}$ for every positive integer n.

4. If n is a square-free integer, prove that $\tau(n) = 2^r$, where r is the number of prime divisors of n.

5. Establish the assertions below:

(a) If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then

$$1 > \frac{n}{\sigma(n)} > \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

(b) For any positive integer n,

$$\frac{\sigma(n!)}{n!} \geq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}.$$

(c) If $n > 1$ is a composite number, then $\sigma(n) > n + \sqrt{n}$.

6. Given a positive integer $k > 1$, show that there are infinitely many integers n for which $\tau(n) = k$, but at most finitely many n with $\sigma(n) = k$.

7. Prove the following

(a) Find the form of all positive integers n satisfying $\tau(n) = 10$. What is the smallest positive integer for which this is true?

(b) Show that there are no positive integers n satisfying $\sigma(n) = 10$.

8. Prove that there are infinitely many pairs of integers m and n with $\sigma(m^2) = \sigma(n^2)$.

9. For $k \geq 2$, show each of the following:

(a) $n = 2^{k-1}$ satisfies the equation $\sigma(n) = 2n - 1$.

(b) If $2^k - 1$ is prime, then $n = 2^{k-1}(2^k - 1)$ satisfies the equation $\sigma(n) = 2n$.

(c) If $2^k - 3$ is prime, then $n = 2^{k-1}(2^k - 3)$ satisfies $\sigma(n) = 2n + 2$.

(d) It is not known if there are any positive integers n for which $\sigma(n) = 2n + 1$.

---

6 Pythagorean Triplets and Representation of a numbers

6.1 Pythagorean Triplets

If (x_1, y_1, z_1) is a solution of $x^2 + y^2 = z^2$ in positive integers then the triple (x_1, y_1, z_1) is called a Pythagorean triple. If the gcd of x_1, y_1, z_1 is 1, then such a triple is called a primitive Pythagorean triple. For example, $(3, 4, 5)$, $(5, 12, 13)$, $(8, 15, 17)$ are primitive Pythagorean triples.

Theorem 1: A primitive Pythagorean triple (x_1, y_1, z_1) with y_1 even is given by $x_1 = r^2 - s^2, y_1 = 2rs, z_1 = r^2 + s^2$ where r and s are arbitrary positive integers of opposite parity with $r > s$ and $(r, s) = 1$.

Proof: Since the gcd of x_1, y_1, z_1 is 1, then x_1, y_1 cannot both be even. If x_1, y_1 are both odd then $x_1^2 \equiv 1 \pmod 4$ and $y_1^2 \equiv 1 \pmod 4$, so that $x_1^2 + y_1^2 = z_1^2 \equiv 2 \pmod 4$, a contradiction. Hence x_1, y_1 cannot both be odd. We assume that y_1 is even and x_1 is odd. Now, $y_1^2 = z_1^2 - x_1^2 = (z_1 + x_1)(z_1 - x_1)$. So $(y_1/2)^2 = y_1^2/4 = [(z_1 - x_1)/2][(z_1 + x_1)/2]$. Now since the g.c.d of x_1, y_1, z_1 is 1, we have $((z_1 - x_1)/2, (z_1 + x_1)/2) = 1$ and hence $(z_1 - x_1)/2 = s^2$ and $(z_1 + x_1)/2 = r^2$ for some positive integers r, s. Obviously $(r, s) = 1$; since the g.c.d of x_1, y_1, z_1 is 1, we get that one of r, s is odd and the other is even. Hence we get that the integers x_1, y_1, z_1 must be of the form $x_1 = r^2 - s^2, y_1 = 2rs, z_1 = r^2 + s^2$ with $r > s > 0, (r, s) = 1$ and r, s are of opposite parity. Conversely, if integers x_1, y_1, z_1 are of the above form, then (x_1, y_1, z_1) is a primitive Pythagorean triple.

Example 1: If (x, y, z) is a primitive Pythagorean triple then show that one of x, y is divisible by 3. Further, show that xyz is divisible by 60.

Solution: By the above theorem we have (assuming y even) $x = r^2 - s^2, y = 2rs, z = r^2 + s^2$. If $3|r$ or $3|s$ then $3|y$. If $3 \nmid r$ and $3 \nmid s$ then by Fermat's theorem $r^2 \equiv 1 \pmod 3$ and $s^2 \equiv 1 \pmod 3$. Thus $x = r^2 - s^2 \equiv 0 \pmod 3$ i.e. $3|x$. Since r and s are of opposite parity $4|y$. If $5|r$ then $5|y$. If $5 \nmid r$ then $r^4 \equiv 1 \pmod 5$ and $s^4 \equiv 1 \pmod 5$. Hence $xz = r^4 - s^4 \equiv 0 \pmod 5$. Since $3, 4, 5$ are pairwise coprime, their product i.e. 60 divides xyz.

Example 2: Let a, b, c be integer sides of a right-angled triangle, where $a < b < c$. Show that $ab(b^2 - a^2)$ is divisible by 84.

Solution: Let $a = xt, b = yt$ and $c = zt$ where (x, y, z) is a primitive Pythagorean triple and t is a positive integer. We may assume that y is even, hence we get $x = r^2 - s^2, y = 2rs, z = r^2 + s^2$ where r and s are arbitrary positive integers of opposite parity with $r > s$ and $(r, s) = 1$. Note that $84 = 4 \times 3 \times 7$. Hence,

$$xy(x^2 - y^2) = 2rs(r^2 - s^2)[(r^2 - s^2)^2 - (2rs)^2] = 2rs(r^2 - s^2)[r^4 + r^2s^2 + s^4 - 7r^2s^2].$$

is divisible by 4 as one of r and s is even. Either rs is divisible by 3 or otherwise $r^2 \equiv s^2 \equiv 1 \pmod 3$. Hence $3|r^2 - s^2$. If $7 \nmid rs$ then $r^6 \equiv s^6 \equiv 1 \pmod 7$. Hence $7|xy(x^2 - y^2)$. Since $3, 4 and 7$ are relatively prime pairs, we get the required result.

6.2 Representation of a positive integer

Let n be a positive integer, b be any positive integer > 1. Then n can be written uniquely as

$$n = n_k b^k + n_{k-1} b^{k-1} + \ldots + n_1 b + n_0 \quad (1)$$

where $0 \leq n_i < b, n_k \neq 0$. We also write (1) as

$$n = (n_k, n_{k-1}, \ldots, n_1, n_0)_b \quad (2)$$

(1) and (2) are called a digital representation of n in base b. The n_i are called the digits. The above n may also be written (for $k > s$) as

$$n = (n_k, n_{k-1}, \ldots, n_2, n_1, n_0)_b \quad (3)$$

We may thus write

$$n = (\ldots, n_i, \ldots, n_2, n_1, n_0)_b \text{ with } n_i = 0 \text{ for every } i > s.$$

We have the following conventions:

- Binary representation: base 2
- Ternary representation: base 3
- Octal representation: base 8
- Decimal representation: base 10
- Duodecimal representation: base 12
- Hexadecimal representation: base 16

Thus,

$$\begin{aligned} n = 210 &= 2 \times 10^2 + 1 \times 10^1 + 0 \times 10^0 = (210)_{10} \\ &= 1 \times 5^3 + 3 \times 5^2 + 2 \times 5 = (1320)_5 \end{aligned}$$

To convert $210 = (210)_{10}$ to base 2, we divide 210 by 2, and note the remainder, and repeat the process with 210 replaced by the quotient. Continue the process till we get the quotient to be zero. Then starting at the bottom, the remainders give us the binary digits for 210, read from left to right. Thus we have the following table.

divisor	quotient	remainder
2	105	0
2	52	1
2	26	0
2	13	0
2	6	1
2	3	0
2	1	1
2	0	1

Hence $(210)_{10} = (11010010)_2$. Check:

$$(11010010)_2 = 1 \times 2^7 + 1 \times 2^6 + 1 \times 2^4 + 1 \times 2^1 = 128 + 64 + 16 + 2 = 210.$$

The same procedure works for any base b. Note that for representation to base b, the 'digits' are the numbers 0, 1, $\ldots$, $b-1$. Thus in base 2 the digits are 0, 1 and in base 5 they are 0, 1, 2, 3, 4. If $b > 10$, then we have to use new symbols to designate the digits 10. E.g. if $b = 12$, the digits are 0, 1, $\ldots$, 10, 11. The new digits 10 and 11 may be designated by symbols such as as t and e or they may be underscored. Thus $(1\ t)_{12} = (2\ 2)_{10}$ or $(\underline{11}\ 1)_{12} = (1\ 3\ 3)_{10}$. When hexadecimal representation is used, we denote the numbers 10, 11, 12, 13, 14, and 15 by A, B, C, D, E, F respectively.

6.3 Exercise 7.1

1. Show that if $x_1^2 + y_1^2 = z_1^2$, then the following are equivalent:

(i) gcd of x_1, y_1, z_1 is 1

(ii) $(x_1, y_1) = 1$

(iii) $(y_1, z_1) = 1$

(iv) $(x_1, z_1) = 1$

(v) $(x_1, y_1, z_1) = 1$

2. If (x, y, z) is a Pythagorean triple such that each x, y, z can be written as sum of two squares then show that $180|xyz$.

3. Verify the following:

(i) $(556)_{10} = (4211)_5$

(ii) $(556)_9 = (456)_{10}$

(iii) $(1376)_8 = (53t)_{12}$

4. Show that every positive integer is congruent modulo $b - 1$ to sum of its digits in base b. Show further that if $n = (n_s, n_{s-1}, \ldots, n_1, n_0)_b$, then $n \equiv n_0 - n_1 + n_2 \ldots + (-1)^s n_s \pmod{(b+1)}$. Hence, derive a divisibility test for 11.

5. Noting that 37 divides 999, devise a test for divisibility by 37. Noting that $1001 = 7 \times 11 \times 13$, devise a test of divisibility by these primes.

---

7 Number Theory MCQ Questions

1. Suppose a, b and n are positive integers, all greater than one. If $a^n + b^n$ is prime, what can you say about n?

   (A) The integer n must be 2;

   (B) The integer n need not be 2, but must be a power of 2;

   (C) The integer n need not be a power of 2, but must be even;

   (D) None of the above is necessarily true.

2. Let x be an irrational number. If a, b, c and d are rational numbers such that

$$\frac{ax+b}{cx+d}$$

   is a rational number, which of the following must be true?

   (A) $ad = bc$ (B) $ac = bd$ (C) $ab = cd$ (D) $a = d = 0$

3. N is a 50 digit number. All the digits except the 26th from the right are 1. If N is divisible by 13, then the unknown digit is

   (A) 1 (B) 3 (C) 7 (D) 9

4. How many integers n are there such that $1 \leq n \leq 1000$ and the highest common factor of n and 36 is 1?

   (A) 333 (B) 667 (C) 166 (D) 361

5. The value of $\sum ij$, where the summation is over all i and j such that $1 \leq i, j \leq 10$, is

   (A) 1320 (B) 2640 (C) 3025 (D) none of the above

6. Let $d_1, d_2, \ldots, d_k$ be all the factors of a positive integer n including 1 and n. Suppose $d_1 + d_2 + \cdots + d_k = 72$. Then the value of

$$\frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_k}$$

   (A) is $\frac{k^2}{72}$;

   (B) is $\frac{72}{k}$;

   (C) is $\frac{72}{n}$;

   (D) cannot be computed.

7. If three prime numbers, all greater than 3, are in A.P., then their common difference

   (A) must be divisible by 2 but not necessarily by 3;

   (B) must be divisible by 3 but not necessarily by 2;

   (C) must be divisible by both 2 and 3;

   (D) must not be divisible by any of 2 and 3.

8. Let P denote the set of all positive integers and

$$S = \{(x, y) \in P \times P : x^2 - y^2 = 666\}.$$

   Then S

(A) is an empty set;

(B) contains exactly one element;

(C) contains exactly two elements;

(D) contains more than two elements.

9. The numbers $12n + 1$ and $30n + 2$ are relatively prime for

   (A) any positive integer n;

   (B) infinitely many, but not all, integers n;

   (C) for finitely many integers n;

   (D) no positive integer n.

10. How many possible values of (a, b, c, d), with a, b, c, d real, are there such that $abc = d$, $bcd = a$, $cda = b$, and $dab = c$?

    (A) 1 (B) 6 (C) 9 (D) 17

11. The digit at the unit place of $(1! - 2! + 3! - \cdots + 25!)^{(1!-2!+3!-\cdots+25!)}$ is

    (A) 0; (B) 1; (C) 5; (D) 9.

12. For every positive integer n, let $\langle n \rangle$ denote the integer closest to $\sqrt{n}$. Let $A_k = \{n > 0 : \langle n \rangle = k\}$. The number of elements in A_{49} is

    (A) 97 (B) 98 (C) 99 (D) 100.

13. The product of the first 100 positive integers ends with

    (A) 21 zeroes (B) 22 zeroes (C) 23 zeroes (D) 24 zeroes

14. Consider the following two statements about a positive integer n and choose the correct option below.

    (I) n is a perfect square.

    (II) The number of positive integer divisors of n is odd.

    (A) I and II are equivalent (B) I implies II but not conversely

    (C) II implies I but not conversely (D) Neither statement implies the other

15. If $x > y$ are positive integers such that $3x + 11y$ leaves a remainder 2 when divided by 7 and $9x + 5y$ leaves a remainder 3 when divided by 7, then the remainder when $x - y$ is divided by 7, equals

    (A) 3 (B) 4 (C) 5 (D) 6.

16. Let l, m, n be any three positive integers such that $l^2 + m^2 = n^2$. Then,

    (A) 3 always divides mn

    (B) 3 always divides lm

    (C) 3 always divides ln

    (D) 3 does not divide lmn

17. Consider the equation $x^2 + y^2 = 2007$. How many solutions (x, y) exist such that x and y are positive integers?

    (A) None

    (B) Exactly two

    (C) More than two but finitely many

    (D) Infinitely many

18. The last digit of $9! + 3^{9966}$ is

    (A) 3 (B) 9 (C) 7 (D) 1.

Answer Key

1	2	3	4	5	6	7	8	9
B	A	D	A	C	C	C	A	A
10	11	12	13	14	15	16	17	18
C	B	B	D	A	C	B	A	B

8 Some Harder Problems

Example 1. Let p be an odd prime number and a, b, c be integers so that the integers

$$a^{2023} + b^{2023}, \quad b^{2024} + c^{2024}, \quad c^{2025} + a^{2025}$$

are all divisible by p. Prove that p divides each of a, b, and c.

Solution: Set $k = 2023$. If one of a, b, c is divisible by p, then all of them are. Indeed, for example, if $p \mid a$, then $p \mid a^k + b^k$ implies $p \mid b$, and then $p \mid b^{k+1} + c^{k+1}$ implies $p \mid c$. The other cases follow similarly.

So for the sake of contradiction assume none of a, b, c is divisible by p. Then

$$a^{k(k+2)} \equiv (a^k)^{k+2} \equiv (-b^k)^{k+2} \equiv -b^{k(k+2)} \pmod p$$

and

$$a^{k(k+2)} \equiv (a^{k+2})^k \equiv (-c^{k+2})^k \equiv -c^{k(k+2)} \pmod p.$$

So $b^{k(k+2)} \equiv c^{k(k+2)} \pmod p$. But then

$$c^{k(k+2)} \cdot c \equiv c^{(k+1)^2} \equiv (-b^{k+1})^{k+1} \equiv b^{(k+1)^2} \equiv b^{k(k+2)} \cdot b \pmod p$$

which forces $b \equiv c \pmod p$. Thus

$$0 \equiv b^{k+1} + c^{k+1} = 2b^{k+1} \pmod p$$

implying $p \mid b$, a contradiction. Thus the proof is complete.

Example 2. Determine all integers $n \geq 1$ for which there exists a pair of positive integers (a, b) such that no cube of a prime divides $a^2 + b + 3$ and

$$\frac{ab + 3b + 8}{a^2 + b + 3} = n.$$

Solution. As $b \equiv -a^2 - 3 \pmod{a^2 + b + 3}$, the numerator of the given fraction satisfies

$$ab + 3b + 8 \equiv a(-a^2 - 3) + 3(-a^2 - 3) + 8 \equiv -(a+1)^3 \pmod{a^2 + b + 3}.$$

As $a^2 + b + 3$ is not divisible by p^3 for any prime p, if $a^2 + b + 3$ divides $(a+1)^3$ then it does also divide $(a+1)^2$. Since

$$0 < (a+1)^2 < 2(a^2 + b + 3),$$

we conclude $(a+1)^2 = a^2 + b + 3$. This yields $b = 2(a-1)$ and $n = 2$. The choice $(a, b) = (2, 2)$ with $a^2 + b + 3 = 9$ shows that $n = 2$ indeed is a solution.

Example 3: Solve the following equation in positive integers:

$$x^2 + y^2 = 1997(x - y).$$

Solution: Here is how to transform the equation from the statement into a Pythagorean equation:

$$\begin{aligned}
x^2 + y^2 &= 1997(x - y), \\
2(x^2 + y^2) &= 2 \cdot 1997(x - y), \\
(x+y)^2 + (x-y)^2 - 2 \cdot 1997(x - y) &= 0, \\
(x+y)^2 + (1997 - x + y)^2 &= 1997^2.
\end{aligned}$$

Because x and y are positive integers, $0 < x + y < 1997$, and for the same reason $0 < 1997 - x + y < 1997$. The problem reduces to solving the Pythagorean equation $a^2 + b^2 = 1997^2$ in positive integers. Since 1997 is prime, the greatest common divisor of a and b is 1. Hence there exist coprime positive integers $u > v$ with the greatest common divisor equal to 1 such that

$$1997 = u^2 + v^2, \quad a = 2uv, \quad b = u^2 - v^2.$$

Because u is the larger of the two numbers, $\frac{1997}{2} < u < 1997$; hence $33 \leq u \leq 44$. There are 12 cases to check. Our task is simplified if we look at the equality $1997 = u^2 + v^2$ and realize that neither u nor v can be divisible by 3. Moreover, looking at the same equality modulo 5, we find that u and v can only be 1 or -1 modulo 5. We are left with the cases $m = 34, 41$, or 44. The only solution is $(m, n) = (34, 29)$. Solving $x + y = 2 \cdot 34 \cdot 29$ and $1997 - x + y = 34^2 - 29^2$, we obtain $x = 1827$, $y = 145$. Solving $x + y = 34^2 - 29^2$, $1997 - x + y = 2 \cdot 34 \cdot 29$, we obtain $(x, y) = (170, 145)$. These are the two solutions to the equation.

Example 4: Let $X = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Let $S \subseteq X$ be such that any nonnegative integer n can be written as $p+q$ where the nonnegative integers p, q have all their digits in S. Find the smallest possible number of elements in S.

Solution: We show that 5 numbers will suffice. Take $S = \{0, 1, 3, 4, 6\}$. Observe the following splitting:

n	a	b
0	0	0
1	0	1
2	1	1
3	0	3
4	1	3
5	1	4
6	3	3
7	3	4
8	4	4
9	3	6

Thus each digit in a given nonnegative integer is split according to the above and can be written as a sum of two numbers each having digits in S.

We show that $|S| > 4$. Suppose $|S| \leq 4$. We may take $|S| = 4$ as adding extra numbers to S does not alter our argument. Let $S = \{a, b, c, d\}$. Since the last digit can be any one of the numbers 0, 1, 2, ..., 9, we must be able to write this as a sum of digits from S, modulo 10. Thus the collection

$$A = \{x + y \pmod{10} \mid x, y \in S\}$$

must contain $\{0, 1, 2, \ldots, 9\}$ as a subset. But A has at most 10 elements $\binom{4}{2} + 4$. Thus each element of the form $x + y \pmod{10}$, as x, y vary over S, must give different numbers from $\{0, 1, 2, \ldots, 9\}$.

Consider $a + a, b + b, c + c, d + d \pmod{10}$. They must give 4 even numbers. Hence the remaining even number must be from the remaining 6 elements obtained by adding two distinct members of S. We may assume that one even number is $a + b \pmod{10}$. Then a, b must have same parity. If any one of c, d has same parity as that of a, then its sum with a gives an even number, which is impossible. Hence c, d must have same parity, in which case $c + d \pmod{10}$ is even, which leads to a contradiction. We conclude that $|S| \geq 5$.

Example 5: Let n and M be positive integers such that $M > n^{n-1}$. Prove that there are n distinct primes $p_1, p_2, p_3, \ldots, p_n$ such that p_j divides $M + j$ for $1 \leq j \leq n$.

Solution: If some number $M + k$, $1 \leq k \leq n$, has at least n distinct prime factors, then we can associate a prime factor of $M + k$ with the number $M + k$ which is not associated with any of the remaining $n - 1$ numbers.

Suppose $M + j$ has less than n distinct prime factors. Write

$$M + j = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}, \quad r < n.$$

But $M+j > n^{n-1}$. Hence there exists t, $1 \le t \le r$ such that $p_t^{\alpha_t} > n$. Associate p_t with this $M+j$. Suppose p_t is associated with some $M+l$. Let $p_t^{\beta_t}$ be the largest power of p_t dividing $M+l$. Then $p_t^{\beta_t} > n$. Let $T = \gcd(p_t^{\alpha_t}, p_t^{\beta_t})$. Then $T > n$. Since $T \mid (M+j)$ and $T \mid (M+l)$, it follows that $T \mid |(j-l)|$. But $|j-l| < n$ and $T > n$, and we get a contradiction. This shows that p_t cannot be associated with any other $M+l$. Thus each $M+j$ is associated with different primes.

Example 6: From a set of 11 square integers, show that one can choose 6 numbers $a^2, b^2, c^2, d^2, e^2, f^2$ such that

$$a^2 + b^2 + c^2 \equiv d^2 + e^2 + f^2 \pmod{12}.$$

Solution: The first observation is that we can find 5 pairs of squares such that the two numbers in a pair have the same parity. We can see this as follows:

Odd numbers	Even numbers	Odd pairs	Even pairs	Total pairs
0	11	0	5	5
1	10	0	5	5
2	9	1	4	5
3	8	1	4	5
4	7	2	3	5
5	6	2	3	5
6	5	3	2	5
7	4	3	2	5
8	3	4	1	5
9	2	4	1	5
10	1	5	0	5
11	0	5	0	5

Let us take such 5 pairs: say $(x_1^2, y_1^2), (x_2^2, y_2^2), \ldots, (x_5^2, y_5^2)$. Then $x_j^2 - y_j^2$ is divisible by 4 for $1 \le j \le 5$. Let r_j be the remainder when $x_j^2 - y_j^2$ is divisible by 3, $1 \le j \le 3$. We have 5 remainders r_1, r_2, r_3, r_4, r_5. But these can be 0, 1 or 2. Hence either one of the remainders occurs 3 times or each of the remainders occurs once. If, for example $r_1 = r_2 = r_3$, then 3 divides $r_1 + r_2 + r_3$; if $r_1 = 0, r_2 = 1$ and $r_3 = 2$, then again 3 divides $r_1 + r_2 + r_3$. Thus we can always find three remainders whose sum is divisible by 3. This means we can find 3 pairs, say, $(x_1^2, y_1^2), (x_2^2, y_2^2), (x_3^2, y_3^2)$ such that 3 divides $(x_1^2 - y_1^2) + (x_2^2 - y_2^2) + (x_3^2 - y_3^2)$. Since each difference is divisible by 4, we conclude that we can find 6 numbers $a^2, b^2, c^2, d^2, e^2, f^2$ such that

$$a^2 + b^2 + c^2 \equiv d^2 + e^2 + f^2 \pmod{12}.$$

1. Find all non-negative integers x, y such that

$$x^3y + x + y = xy + 2xy^2$$

2. For any natural number $n > 1$, write the infinite decimal expansion of $\frac{1}{n}$ (for example, we write $\frac{1}{2} = 0.4\overline{9}$ as its infinite decimal expansion, not 0.5). Determine the length of the non-periodic part of the (infinite) decimal expansion of $\frac{1}{n}$.

3. For any natural number n, expressed in base 10, let $S(n)$ denote the sum of all digits of n. Find all natural numbers n such that $n = 2S(n)^2$.

4. Show that there are infinitely many triples (x, y, z) of integers such that

$$x^3 + y^4 = z^{31}$$

5. Show that there are infinitely many positive real numbers a which are not integers such that $a(a - 3\{a\})$ is an integer. (Here $\{a\}$ denotes the fractional part of a. For example $\{1.5\} = 0.5$; $\{-3.4\} = 0.6$.)

6. Find all integers a, b, c such that

$$a^2 = bc + 1, \quad b^2 = ca + 1.$$

7. For any positive integer $n > 1$, let $P(n)$ denote the largest prime not exceeding n. Let $N(n)$ denote the next prime larger than $P(n)$. (For example $P(10) = 7$ and $N(10) = 11$, while $P(11) = 11$ and $N(11) = 13$.) If $n + 1$ is a prime number, prove that the value of the sum

$$\frac{1}{P(2)N(2)} + \frac{1}{P(3)N(3)} + \frac{1}{P(4)N(4)} + \cdots + \frac{1}{P(n)N(n)} = \frac{n-1}{2n+2}.$$

8. Find all positive integers m, n, and primes $p \geq 5$ such that

$$m(4m^2 + m + 12) = 3(p^n - 1).$$

9. Let $p_1 < p_2 < p_3 < p_4$ and $q_1 < q_2 < q_3 < q_4$ be two sets of prime numbers such that $p_4 - p_1 = 8$ and $q_4 - q_1 = 8$. Suppose $p_1 > 5$ and $q_1 > 5$. Prove that 30 divides $p_1 - q_1$.

10. Find all non-zero real numbers x, y, z which satisfy the system of equations:

$$(x^2 + xy + y^2)(y^2 + yz + z^2)(z^2 + zx + x^2) = xyz,$$

$$(x^4 + x^2y^2 + y^4)(y^4 + y^2z^2 + z^4)(z^4 + z^2x^2 + x^4) = x^3y^3z^3.$$

11. Given a prime number p such that the number $2p$ is equal to the sum of the squares of some four consecutive positive integers. Prove that $p - 7$ is divisible by 36.

12. Suppose x is a nonzero real number such that both x^5 and $20x + \frac{19}{x}$ are rational numbers. Prove that x is a rational number.

13. Find all natural numbers n such that $1 + \lfloor \sqrt{2n} \rfloor$ divides $2n$. (For any real number x, $\lfloor x \rfloor$ denotes the largest integer not exceeding x.)

14. Show that there are infinitely many 4-tuples (a, b, c, d) of natural numbers such that $a^3 + b^4 + c^5 = d^7$.

15. Show that the equation

$$a^3 + (a+1)^3 + (a+2)^3 + (a+3)^3 + (a+4)^3 + (a+5)^3 + (a+6)^3 = b^4 + (b+1)^4$$

has no solutions in integers a, b.

16. A positive integer n is called *good* if there is a set of divisors of n whose members sum to n and include 1. Prove that every positive integer has a multiple which is good.

17. Let x and y be positive integers with no prime factors larger than 5. Find all such x and y which satisfy

$$x^2 - y^2 = 2^k$$

for some non-negative integer k.

18. Find all integers $n \geq 3$ such that the following property holds: if we list the divisors of $n!$ in increasing order as $1 = d_1 < d_2 < \cdots < d_k = n!$, then we have

$$d_2 - d_1 \leq d_3 - d_2 \leq \cdots \leq d_k - d_{k-1}.$$

19. Find all pairs of primes (p, q) for which $p - q$ and $pq - q$ are both perfect squares.

20. Given that $a_1, a_2, \ldots, a_{10}$ are positive real numbers, determine the smallest possible value of

$$\sum_{i=1}^{10} \left\lfloor \frac{7a_i}{a_i + a_{i+1}} \right\rfloor$$

where we define $a_{11} = a_1$.

---

9 Polynomials

9.1 Introduction: Remainder and Factor Theorem

We denote the set of rational numbers by $\mathbb{Q}$. Thus,

$$\mathbb{Q} = \left\{ \frac{m}{n} \middle| m, n \text{ are integers}, n \neq 0 \right\}.$$

Also, we denote the set of real numbers by $\mathbb{R}$ and the set of complex numbers by $\mathbb{C}$. Let $\mathbb{F}$ denote any one of the sets $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. If n is a non-negative integer, then an expression of the form

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n, \tag{1}$$

where $a_0, a_1, \ldots, a_n$ are in $\mathbb{F}$ (or in $\mathbb{Z}$), is called a **polynomial in** x **with coefficients** $a_0, \ldots, a_n$. We express this by saying that $f(x)$ is a **polynomial over** $\mathbb{F}$ (or $\mathbb{Z}$). If $f(x)$ is a polynomial over $\mathbb{Z}$ then $f(x)$ is called a polynomial with integer coefficients. Similarly, we can define a polynomial with real or rational coefficients. If all the coefficients are zero, then $f(x)$ is called the **zero polynomial** and is denoted by 0. If $a_0 \neq 0$, then $f(x)$ is called a **polynomial of degree** n and a_0 is called its **leading coefficient**. The polynomial is said to be **monic** if its leading coefficient is 1. If $n = 0$ and $a_0 \neq 0$, then $f(x) = a_0$ is a polynomial of degree zero. We do not define the degree of the zero polynomial. Two non-zero polynomials are called **(identically) equal** if the coefficients of respective powers of x in them are equal.

Theorem 1 (Division Algorithm) Let $f(x)$ and $g(x)$ be polynomials with coefficients in $\mathbb{F}$ and let $g(x)$ be non-zero. Then there exist **unique** polynomials $q(x)$ and $r(x)$ with coefficients in $\mathbb{F}$ such that,

$$f(x) = q(x)g(x) + r(x), \tag{2}$$

where $r(x)$ is either the zero polynomial or a non-zero polynomial of degree less than the degree of $g(x)$.

Here $q(x)$ is called the **quotient** and $r(x)$ the **remainder**, obtained on dividing $f(x)$ by $g(x)$. If $r(x)$ is the zero polynomial, we say that $f(x)$ is **divisible by** $g(x)$ over $\mathbb{F}$ or that $g(x)$ is a **factor of** $f(x)$ over $\mathbb{F}$.

We note that if $f(x)$ and $g(x)$ are over $\mathbb{Z}$ i.e. if they have integer coefficients, then $q(x)$ and $r(x)$ are, in general, over $\mathbb{Q}$. But if the leading coefficient of $g(x)$ is 1 or -1, then $q(x)$ and $r(x)$ also have integer coefficients.

Theorem 2 (Remainder Theorem) Let $a \in \mathbb{F}$. If $f(x)$ is a polynomial, then the remainder after dividing $f(x)$ by $x - a$ is $f(a)$.

Proof: Since the degree of $g(x) = x - a$ is 1, by (2) we get,

$$f(x) = (x - a)q(x) + r,$$

where r is **independent of** x. Hence putting $x = a$ we get $f(a) = r$.

Definition: Let $a \in \mathbb{F}$. Then a is said to be a **root** of a polynomial $f(x)$ (or of the polynomial equation $f(x) = 0$) if $f(a) = 0$.

Theorem 3 (Factor Theorem) A number a is a root of a polynomial $f(x)$ if and only if $x - a$ divides $f(x)$.

Proof: We have $f(x) = (x - a)q(x) + f(a)$. Hence a is a root of $f(x)$ if and only if $f(a) = 0$ if and only if $x - a$ divides $f(x)$ (by theorem 2).

We now state the following theorem without proof.

Theorem 4 (Fundamental Theorem of Algebra) If $f(x)$ is a polynomial of degree $n \geq 1$ with complex coefficients, then $f(x)$ has at least one complex root.

We can restate the Fundamental Theorem of Algebra as follows:

Theorem 5 If $f(x)$ is a polynomial of degree $n \geq 1$ with coefficients in $\mathbb{C}$, then $f(x)$ has exactly n roots, not necessarily distinct, in $\mathbb{C}$. Further, if these roots are $b_1, b_2, \ldots, b_n$, then $f(x)$ has the factorization

$$f(x) = a_0(x - b_1) \cdots (x - b_n), \tag{3}$$

where a_0 is the leading coefficient of $f(x)$.

Theorem 6 Let $f(x)$ be a polynomial, as in (1), having integer coefficients and degree $n \geq 1$ and $a_n \neq 0$. Let $p \neq 0$ and $q > 0$ be integers without a common factor. Then if $\frac{p}{q}$ is a rational root of $f(x)$, then p divides a_n and q divides a_0. If $a_0 = \pm 1$, then every rational root of $f(x)$ must be an integer and must divide a_n.

Proof: Let $\frac{p}{q}$ be a root of $f(x)$. Then $f\left(\frac{p}{q}\right) = 0$ i.e.

$$a_0 \left(\frac{p}{q}\right)^n + a_1 \left(\frac{p}{q}\right)^{n-1} + \cdots + a_n = 0$$

or

$$-p(a_0p^{n-1} + \cdots + a_{n-1}q^{n-1}) = a_nq^n \tag{4}$$

and

$$a_0p^n = -q(a_1p^{n-1} + \cdots + a_nq^{n-1}) \tag{5}$$

By (4), $p|a_nq^n$ and so $p|a_n$, since p and q are coprime. Similarly, (5) shows that $q|a_0$.

Note 1. If $f(x)$ has integer coefficients and a is an integer root of $f(x)$ and m is any integer different from a, then $a - m$ divides $f(m)$.

Proof: On dividing $f(x)$ by $x - m$ we get

$$f(x) = (x - m)q(x) + f(m),$$

where $q(x)$ has integer coefficients. So for $x = a$, we get

$$0 = f(a) = (a - m)q(a) + f(m) \quad \text{or} \quad f(m) = -(a - m)q(a).$$

Hence $(a - m)$ divides $f(m)$.

Example 1. Let $f(x)$ be a polynomial, as in (1), having integer coefficients and let $f(0) = 1989$ and $f(1) = 9891$. Prove that $f(x)$ has no integer roots.

Solution: If a is an integer root, then $a \neq 0$ as $f(0) \neq 0$. Also a must be odd since it must divide $f(0) = a_n = 1989$. But $a \neq 1$ as $f(1) \neq 0$. So taking $m = 1$ in Note 1, we see that the even number $(a - 1)$ divides the odd number $f(1) = 9891$, a contradiction.

Example 2. Find all polynomials p satisfying $p(x + 1) = p(x) + 2x + 1$.

Solution: Observe that $p(x) = x^2$ satisfies the given condition. We substitute $p(x) = f(x) + x^2$. Hence, the given condition gets transformed to

$$f(x + 1) = f(x).$$

Since, $p(x)$ and x^2 are polynomials, $f(x)$ is also a polynomial and since $f(x+1) = f(x)$ for all x, we get that $f(x)$ is a constant polynomial. Hence,

$$p(x) = x^2 + c.$$

Note 2. The roots of the equation $ax^2 + bx + c = 0$, $a \neq 0$ are given by

$$\alpha = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \quad \text{and} \quad \beta = \frac{-b - \sqrt{b^2 - 4ac}}{2a}.$$

Let us denote the expression $b^2 - 4ac$, i.e. the quantity under the radical sign, by the letter Δ (delta of the Greek alphabet). Then

$$\alpha = \frac{-b + \sqrt{\Delta}}{2a} \quad \text{and} \quad \beta = \frac{-b - \sqrt{\Delta}}{2a}.$$

We also note that

$$(\alpha-\beta)^2 = \frac{b^2-4ac}{a^2} = \frac{\Delta}{a^2}.$$

Hence, it is clear that whether the roots will be real or complex, equal or unequal, depends on Δ. Thus $\Delta = b^2-4ac$ discriminates the nature of the roots of the equation. Hence, Δ is called the *discriminant* of the equation.

The nature of the roots of the quadratic equation $ax^2+bx+c=0$, $a,b,c\in\mathbb{R}$ is decided as follows:

1. If $\Delta > 0$, $\sqrt{\Delta}$ is real and $\sqrt{\Delta}\neq 0$. Hence the roots $\frac{-b+\sqrt{\Delta}}{2a}$ and $\frac{-b-\sqrt{\Delta}}{2a}$ are real and distinct. Note that

$$(\alpha-\beta)^2 = \frac{b^2-4ac}{a^2} = \frac{\Delta}{a^2}.$$

Thus, conversely, if the roots are real and unequal, then $\Delta > 0$.

In particular, suppose $a,b,c\in\mathbb{Q}$ i.e. a,b,c are rational numbers, $a\neq 0$. Now, if Δ is a perfect square of a rational number, say $\Delta = k^2$, then the roots are rational, namely $\frac{-b\pm k}{2a}$. On the other hand, if Δ is not a perfect square of a rational number, then $\sqrt{\Delta}$ is irrational and so the roots are irrational and they are $\frac{-b+\sqrt{\Delta}}{2a}$ and $\frac{-b-\sqrt{\Delta}}{2a}$, i.e. they are always of the form $m+\sqrt{n}$ and $m-\sqrt{n}$, where $m=\frac{-b}{2a}$ and $n=\Delta\cdot 4a^2$ are rational numbers. Thus, if $a,b,c\in\mathbb{Q}$ then the roots $m+\sqrt{n}$ and $m-\sqrt{n}$ always occur in pairs.

2. If $\Delta = 0$ then the roots $\frac{-b\pm\sqrt{\Delta}}{2a} = \frac{-b}{2a}$ are real and equal. Conversely, it is easy to see that if the roots are real and equal, then $\Delta = 0$.

3. If $\Delta < 0$, $\sqrt{\Delta}$ is imaginary and the roots are complex numbers. Let $\Delta = -k^2$ where $k>0$. Hence the roots $\frac{-b}{2a}+\frac{k}{2a}i$ and $\frac{-b}{2a}-\frac{k}{2a}i$, i.e. they are complex conjugate numbers of the form $m+it$ and $m-it$, where

$$m=\frac{-b}{2a} \quad \text{and} \quad t=k\cdot 2a \quad \text{are real numbers.} \quad (\alpha-\beta)^2 = \frac{b^2-4ac}{a^2} = \frac{\Delta}{a^2}.$$

Thus, conversely, if the roots are non-real, then $\Delta < 0$.

Note 3. If $f(x)$ has real coefficients and if $c=a+ib$ (where $a,b\in\mathbb{R}$ and $b\neq 0$) is a complex root of $f(x)$, then the conjugate $\bar{c}=a-ib$ of c is also a root of $f(x)$.

Proof: On dividing $f(x)$ by $g(x)=(x-c)(x-\bar{c})=(x-a)^2+b^2$, we get

$$f(x)=(x-c)(x-\bar{c})q(x)+ex+d, \quad (6)$$

where $q(x)$ and $ex+d$ have real coefficients. Now

$$f(c)=0=e(a+ib)+d \quad \text{and so} \quad ea+d=0 \quad \text{and} \quad eb=0.$$

This gives $e=0$ as $b\neq 0$. Hence $d=0$. So by (6), $f(\bar{c})=0$.

Note 4. It can be shown that every polynomial of odd degree n with real coefficients has at least one real root.

Note 5. If a real quadratic surd $a+\sqrt{b}$ is a root of a polynomial $f(x)$ with rational coefficients, then $a-\sqrt{b}$ is also a root of $f(x)$.

An expression in variables $a,b,\ldots$ is said to be symmetric in $a,b,\ldots$ if it is unchanged under all permutations of $a,b,\ldots$.

Thus $a+b$ and $a/b+b/a$ are symmetric in a,b but $a-b$ is not symmetric. The simplest symmetric polynomials in a,b and c are the following: $a+b+c, ab+ac+bc, abc$. These are respectively the sum of products of a,b,c taken one at a time, two at a time and three at a time. The first two of these are usually denoted respectively by $\sum a, \sum ab$. These three polynomials are called *elementary symmetric polynomials* in a,b,c. Similarly the elementary symmetric polynomials in a,b,c,d are

$$\sum a = a+b+c+d, \quad \sum ab = ab+ac+ad+bc+bd+cd,$$

$$\sum abc = abc+abd+acd+bcd \quad \text{and} \quad abcd.$$

9.2 Vieta's Theorem

Let $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be any polynomial with complex coefficients with roots $r_1, r_2, \ldots, r_n$, and let s_j be the j^{th} elementary symmetric polynomial of the roots.

Vieta's formulas then state that

$$s_1 = r_1 + r_2 + \cdots + r_n = -\frac{a_{n-1}}{a_n}$$
$$s_2 = r_1 r_2 + r_2 r_3 + \cdots + r_{n-1} r_n = \frac{a_{n-2}}{a_n}$$
$$\vdots$$
$$s_n = r_1 r_2 r_3 \cdots r_n = (-1)^n \frac{a_0}{a_n}.$$

This can be compactly summarized as $s_j = (-1)^j \frac{a_{n-j}}{a_n}$ for some j such that $1 \leq j \leq n$.

Proof: Let all terms be defined as above. By the factor theorem, $P(x) = a_n(x - r_1)(x - r_2)\cdots(x - r_n)$. We will then prove Vieta's formulas by expanding this polynomial and comparing the resulting coefficients with the original polynomial's coefficients.

When expanding the factorization of $P(x)$, each term is generated by a series of n choices of whether to include x or the negative root $-r_i$ from every factor $(x - r_i)$. Consider all the expanded terms of the polynomial with degree $n - j$; they are formed by multiplying a choice of j negative roots, making the remaining $n - j$ choices in the product x, and finally multiplying by the constant a_n.

Note that adding together every multiplied choice of j negative roots yields $(-1)^j s_j$. Thus, when we expand $P(x)$, the coefficient of x_{n-j} is equal to $(-1)^j a_n s_j$. However, we defined the coefficient of x^{n-j} to be a_{n-j}. Thus, $(-1)^j a_n s_j = a_{n-j}$, or $s_j = (-1)^j a_{n-j}/a_n$, which completes the proof.

Theorem 7 (Newton) Every symmetric polynomial in $a_1, a_2, \ldots, a_n$ with integer coefficients (coefficients in $\mathbb{F}$) can be expressed as a polynomial in the elementary symmetric polynomials in $a_1, a_2, \ldots, a_n$ with integer coefficients (respectively with coefficients in $\mathbb{F}$).

For example,

$$a^2 + b^2 + c^2 = (a + b + c)^2 - 2(ab + bc + ca) = \left(\sum a\right)^2 - 2\sum ab$$

and

$$a^3 + b^3 + c^3 = (a + b + c)(a^2 + b^2 + c^2 - ab - bc - ca) + 3abc = (a + b + c)((a + b + c)^2 - 3(ab + bc + ca)) + 3abc$$

Now consider the cubic equation $f(x) = 0$, where

$$f(x) = a_0 x^3 + a_1 x^2 + a_2 x + a_3, \quad a_0 \neq 0.$$

Let α, β, γ be its roots. Then we have,

$$f(x) = a_0(x - \alpha)(x - \beta)(x - \gamma). \quad \text{Hence,}$$

$$a_0 x^3 + a_1 x^2 + a_2 x + a_3 = a_0[x^3 - \left(\sum \alpha\right) x^2 + \left(\sum \alpha\beta\right) x - \alpha\beta\gamma].$$

Hence equating coefficients of various powers of x on the two sides we obtain

$$\sum \alpha = -\frac{a_1}{a_0}, \quad \sum \alpha\beta = \frac{a_2}{a_0}, \quad \alpha\beta\gamma = -\frac{a_3}{a_0}.$$

These give the values of the elementary symmetric polynomials of the roots of $f(x)$ in terms of its coefficients. Similarly, for a fourth-degree polynomial $f(x)$ with roots $\alpha, \beta, \gamma, \delta$ we have

$$\sum \alpha = -\frac{a_1}{a_0}, \quad \sum \alpha\beta = \frac{a_2}{a_0}, \quad \sum \alpha\beta\gamma = -\frac{a_3}{a_0}, \quad \alpha\beta\gamma\delta = \frac{a_4}{a_0}.$$

Example 3: Find the roots of $4x^3 - 16x^2 - 9x + 36 = 0$, given that one root is the negative of another.

Solution. If the roots are a, b, c, we have $b = -a$, say. So by (7), $a - a + c = 4$,

$$-a^2 + ac - ac = -9/4 \quad \text{and} \quad -a^2c = -9.$$

Hence $c = 4$ and $a = 3/2$ as $-b$.

Hence, the roots are $\pm\frac{3}{2}, 4$.

9.3 Some solved examples

Example 4: Show that not all roots of the polynomial $P(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n$ can be real

Solution: Suppose that all its zeros $x_1, x_2, \ldots, x_n$ are real. They satisfy

$$\sum_i x_i = -2n, \quad \sum_{i<j} x_ix_j = 2n^2.$$

However, by the mean inequality we have

$$\sum_{i<j} x_ix_j = \frac{1}{2}\left(\sum_i x_i\right)^2 - \frac{1}{2}\sum_i x_i^2 \leq \frac{n-1}{2n}\left(\sum_i x_i\right)^2 = 2n(n-1),$$

a contradiction.

Example 5: Find all polynomials of the form $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ with $a_j \in \{-1, 1\}$ $j = 0, 1, \ldots, n$ whose all the roots are real

Solution: Let $x_1, \ldots, x_n$ be the roots of the given polynomial. Then

$$x_1^2 + x_2^2 + \cdots + x_n^2 = \left(\sum_i x_i\right)^2 - 2\left(\sum_{i<j} x_ix_j\right) = a_{n-1}^2 - 2a_{n-2} \leq 3;$$

$$x_1^2x_2^2 \cdots x_n^2 = 1.$$

By the mean inequality, the second equality implies $x_1^2 + \cdots + x_n^2 \geq n$; hence $n \leq 3$. The case $n = 3$ is only possible if $x_1, x_2, x_3 = \pm 1$. Now we can easily find all solutions: $x \pm 1, x^2 \pm x - 1, x^3 - x \pm (x^2 - 1)$.

Example 6: The quadratic equation $x^2 + mx + n$ has roots twice those of $x^2 + px + m$, and none of m, n, and p is zero. What is the value of n/p?

Solution: Let $x^2 + px + m = 0$ have roots a and b. Then

$$x^2 + px + m = (x - a)(x - b) = x^2 - (a + b)x + ab,$$

so $p = -(a + b)$ and $m = ab$. Also, $x^2 + mx + n = 0$ has roots $2a$ and $2b$, so

$$x^2 + mx + n = (x - 2a)(x - 2b) = x^2 - 2(a + b)x + 4ab,$$

and $m = -2(a + b)$ and $n = 4ab$. Thus

$$\frac{n}{p} = \frac{4ab}{-(a + b)} = \frac{4m}{m/2} = 8$$

9.4 Irreducible Polynomials

A polynomial is irreducible if it cannot be written as a product of two polynomials in a nontrivial manner. The question of irreducibility depends on the ring of coefficients. When the coefficients are complex numbers, only linear polynomials are irreducible. For real numbers, some quadratic polynomials are irreducible as well. Both these cases are rather dull. The interesting situations occur when the coefficients are rational or integer, in which case there is an interplay between polynomials and arithmetic. The cases of rational and integer coefficients are more or less equivalent, with minor differences such as the fact that $2x + 2$ is irreducible over $\mathbb{Q}[x]$ but reducible over $\mathbb{Z}[x]$. For matters of elegance, we focus on polynomials with integer coefficients. We will assume implicitly from now on that for any polynomial with integer coefficients, the greatest common divisor of its coefficients is 1.

Definition. A polynomial $P(x) \in \mathbb{Z}[x]$ is called irreducible over $\mathbb{Z}[x]$ if there do not exist polynomials $Q(x), R(x) \in \mathbb{Z}[x]$ different from ± 1 such that $P(x) = Q(x)R(x)$. Otherwise, $P(x)$ is called reducible.

We commence with an easy problem.

Example 7: Let $P(x)$ be an nth-degree polynomial with integer coefficients with the property that $|P(x)|$ is a prime number for $2n+1$ distinct integer values of the variable x. Prove that $P(x)$ is irreducible over $\mathbb{Z}[x]$.

Solution. Assume the contrary and let $P(x) = Q(x)R(x)$ with $Q(x), R(x) \in \mathbb{Z}[x]$, $Q(x), R(x) \neq \pm 1$. Let $k = \deg(Q(x))$. Then $Q(x) = 1$ at most k times and $Q(x) = -1$ at most k times. Also, $R(x) = 1$ at most $n-k$ times and $R(x) = -1$ at most $n-k$ times. Consequently, the product $|Q(x)R(x)|$ is composite except for at most $k + (n-k) + (n-k) + k = 2n$ values of x. This contradicts the hypothesis. Hence $P(x)$ is irreducible.

Theorem: Given a polynomial $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ with integer coefficients, suppose that there exists a prime number p such that a_n is not divisible by p, a_k is divisible by p for $k = 0, 1, \ldots, n-1$, and a_0 is not divisible by p^2. Then $P(x)$ is irreducible over $\mathbb{Z}[x]$.

Proof: We argue by contradiction. Suppose that $P(x) = Q(x)R(x)$, with $Q(x)$ and $R(x)$ not identically equal to ± 1. Let

$$Q(x) = b_k x^k + b_{k-1}x^{k-1} + \cdots + b_0,$$
$$R(x) = c_{n-k}x^{n-k} + c_{n-k-1}x^{n-k-1} + \cdots + c_0.$$

Let us look closely at the equalities

$$\sum_{j=0}^{i} b_j c_{i-j} = a_i, \quad i = 0, 1, \ldots, n,$$

obtained by identifying the coefficients. From the first of them, $b_0 c_0 = a_0$, and because a_0 is divisible by p but not by p^2, it follows that exactly one of b_0 and c_0 is divisible by p. Assume that b_0 is divisible by p and take the next equality $b_0 c_1 + b_1 c_0 = a_1$. The right-hand side is divisible by p, and the first term on the left is also divisible by p. Hence $b_1 c_0$ is divisible by p, and since c_0 is not, b_1 must be divisible by p.

This reasoning can be repeated to prove that all the b_i's are divisible by p. It is important that both $Q(x)$ and $R(x)$ have degrees greater than or equal to 1, for the fact that b_k is divisible by p follows from

$$b_k c_0 + b_{k-1}c_1 + \cdots = a_k,$$

where a_k is divisible by p for $k < n$. The contradiction arises in the equality $a_n = b_k c_{n-k}$, since the right-hand side is divisible by p, while the left-hand side is not. This proves the theorem.

Example 8: Prove that the polynomial

$$P(x) = x^{101} + 101x^{100} + 102$$

is irreducible over $\mathbb{Z}[x]$.

Solution: The number 101 is prime, yet we cannot apply Eisenstein's criterion because of the 102. The trick is to observe that the irreducibility of $P(x)$ is equivalent to the irreducibility of $P(x-1)$. Because the binomial coefficients $\binom{101}{k}$, $1 \leq k \leq 100$, are all divisible by 101, the polynomial $P(x-1)$ has all coefficients but the first divisible by 101, while the last coefficient is $(-1)^{101} + 101(-1)^{101} + 102 = 202$, which is divisible by 101 but not by 101^2. Eisenstein's criterion proves that $P(x-1)$ is irreducible; hence $P(x)$ is irreducible as well.

9.5 Exercise 1.1

1. Find numbers a, b such that the roots of $x^2 + ax + b = 0$ are a, b.

2. Suppose α, a, b are integers and $b \neq -1$. Show that if α satisfies the equation $x^2 + ax + b + 1 = 0$, then $a^2 + b^2$ is composite.

3. If $2(a + b + c) = \alpha^2 + \beta^2 + \gamma^2$, and the roots of $x^2 + \alpha x - a = 0$ are β, γ and the roots of $x^2 + \beta x - b = 0$ are γ, α, show that the equation whose roots are α, β is $x^2 + \gamma x - c = 0$.

4. Find the cubic in x which vanishes when $x = 1$ and $x = -2$ and has values 4 and 8 when $x = -1$ and $x = 2$ respectively.

5. Suppose $a_0, a_1, \cdots, a_n$ are integers and $a_0 \neq 0$ and $a_n \neq 0$. Consider the polynomial

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n.$$

If $p \neq 0, q > 0$ are coprime integers and p/q is a rational root of the equation $f(x) = 0$, then show that $p | a_n$ and $q | a_0$, and that if $q > 1$, then $p - mq$ divides $f(m)$ for any integer m.

6. Prove that a polynomial $f(x)$, with integral coefficients, has no integral roots if $f(0)$ and $f(1)$ are both odd integers.

7. Given that $x = 2$ is a root of $84x^3 - 157x^2 - kx + 78 = 0$, find the value of k and the other roots.

8. Find real numbers a, b if $x^2 + x + 1$ is a factor of $2x^6 - x^5 + ax^4 + x^3 + bx^2 - 4x - 3$.

9. If α, β are the roots of $2x^2 - 5x - 4 = 0$, find the simplest quadratic equation whose roots are $\alpha + \frac{1}{\alpha}, \beta + \frac{1}{\beta}$.

10. If α, β, γ are the roots of $x^3 + px - q = 0$, find the simplest cubic equation whose roots are $\alpha + \beta, \beta + \gamma, \gamma + \alpha$.

11. If α, β, γ are the roots of $x^3 - x^2 + 4x + 7 = 0$, find the simplest cubic equation whose roots are $\alpha + \beta, \beta + \gamma, \gamma + \alpha$.

12. Find the polynomial of degree 3 whose roots are the cubes of the roots of $x^3 - x - 1 = 0$.

13. Let $f(x)$ be a polynomial with integer coefficients. If a, b, c are distinct integers such that $f(a) = f(b) = f(c) = -1$, show that the equation $f(x) = 0$ has no integral roots.

14. For what integer a, does $x^2 - x + a$ divide $x^{13} + x + 90$?

15. Let $f(x), g(x)$ be polynomials with real coefficients. If $f(x)g(x) = f(x^2 + x + 1)$ for all $x \in \mathbb{R}$, show that $f(x)$ is of even degree.

16. A polynomial $f(x, y)$ is antisymmetric, if $f(x, y) = -f(y, x)$. Prove that every antisymmetric polynomial $f(x, y)$ has the form $f(x, y) = (x - y)g(x, y)$, where $g(x, y)$ is symmetric.

17. The polynomial $f(x, y, z)$ is antisymmetric if the sign changes on switching any two variables. Prove that every antisymmetric polynomial $f(x, y, z)$ can be written in the form $f(x, y, z) = (x - y)(x - z)(y - z)g(x, y, z)$, where $g(x, y, z)$ is symmetric.

18. If $f(x, y)$ is symmetric and $x - y \mid f(x, y)$, then $(x - y)^2 \mid f(x, y)$.

19. Show that $(x - 1)^2 \mid nx^{n+1} - (n + 1)x^n + 1$.

20. If x_1, x_2 are the zeros of the polynomial $x^2 - 6x + 1$, then for every nonnegative integer n, $x_1^n + x_2^n$ is an integer and not divisible by 5.

21. Given a monic polynomial $f(x)$ of degree n over $\mathbb{Z}$ and $k, p \in \mathbb{N}$, prove that if none of the numbers $f(k), f(k + 1), \ldots, f(k + p)$ is divisible by $p + 1$, then $f(x) = 0$ has no rational solution.

22. The polynomial $x^{2n} - 2x^{2n-1} + 3x^{2n-2} - \cdots - 2nx + 2n + 1$ has no real roots.

23. A polynomial $f(x) = x^4 + *x^3 + **x^2 + **x + 1$ has three undetermined coefficients denoted by stars. The players A and B move alternately, replacing a star by a real number until all stars are replaced. A wins if all zeros of the polynomial are complex. B wins if at least one zero is real. Show that B can win in spite of his only second move.

9.6 Some Harder Problems

Example 1: [ISI-17] Let k, n and r be positive integers.

(a) Let $Q(x) = x^k + a_1 x^{k+1} + \cdots + a_n x^{k+n}$ be a polynomial with real coefficients. Show that the function $\frac{Q(x)}{x^k}$ is strictly positive for all real x satisfying

$$0 < |x| < \frac{1}{1 + \sum_{i=1}^{n} |a_i|}.$$

(b) Let $P(x) = b_0 + b_1 x + \cdots + b_r x^r$ be a nonzero polynomial with real coefficients. Let m be the smallest number such that $b_m \neq 0$. Prove that the graph of $y = P(x)$ cuts the x-axis at the origin (i.e., P changes signs at $x = 0$) if and only if m is an odd integer.

Solution:

(a) For $0 < |x| < \frac{1}{1+\sum_{i=1}^{n}|a_i|} < 1$ the inequality $a_k x^k \geq -|a_k||x|^k$ holds true, thus

$$\frac{Q(x)}{x^k} = 1 + \sum_{i=1}^{n} a_k x^k \geq 1 - |x| \sum_{i=1}^{n} |a_i| > 1 - \frac{\sum_{i=1}^{n}|a_i|}{1 + \sum_{i=1}^{n}|a_i|} = \frac{1}{1 + \sum_{i=1}^{n}|a_i|} > 0$$

(b) We have $P(x) = x^m(H(x))$, where $H(x) := b_m + b_{m+1}x + \cdots + b_r x^{r-m}$, now $H(0) \neq 0$, and since $H(x)$ is continuous at 0, we have $H(x)$ has a fixed sign on $(-\delta, \delta)$ for some $\delta > 0$. But as $P(x)$ changes sign about 0, we must have x^m to change sign about 0 which implies that m must be odd.

Example 2: [ISI -13] Let $p(x)$ and $q(x)$ be two polynomials, both of which have their sum of coefficients equal to s. Let p, q satisfy $p(x)^3 - q(x)^3 = p(x^3) - q(x^3)$. Show that

(a) There exists an integer $a \geq 1$ and a polynomial $r(x)$ with $r(1) \neq 0$ such that

$$p(x) - q(x) = (x-1)^a r(x).$$

(b) Show that $s^2 = 3^{a-1}$, where a is described as above.

Solution:

(a) $p(1) = q(1) = s$. Then consider $h(x) = p(x) - q(x)$. Then $x = 1$ is a root of $h(x)$. So, there exists $a \in \mathbb{N}$ and a polynomial $r(x)$ with $r(1) \neq 0$ such that $h(x) = (x-1)^a \cdot r(x)$.

(b) $(p(x) - q(x))(p(x)^2 + p(x)q(x) + q(x)^2) = p(x^3) - q(x^3)$. So

$$(x-1)^a r(x)(p(x)^2 + p(x)q(x) + q(x)^2) = (x^3 - 1)^a r(x^3)$$

Plug $x = 1$ after cancelling $(x-1)^a$ and we are done.

Example 3: [INMO-23] Suppose $a_0, \ldots, a_{100}$ are positive reals. Consider the following polynomial for each k in $\{0, 1, \ldots, 100\}$:

$$a_{100+k}x^{100} + 100a_{99+k}x^{99} + a_{98+k}x^{98} + a_{97+k}x^{97} + \cdots + a_{2+k}x^2 + a_{1+k}x + a_k,$$

where indices are taken modulo 101, *i.e.*, $a_{100+i} = a_{i-1}$ for any i in $\{1, 2, \ldots, 100\}$. Show that it is impossible that each of these 101 polynomials has all its roots real.

Solution: Let $n = 50$. For the sake of contradiction, assume that each of these polynomials has all real roots; these roots must be negative. Let

$$-\alpha_{1,k}, -\alpha_{2,k}, \ldots, -\alpha_{2n,k}$$

be the roots of the polynomial

$$a_{2n+k}x^{2n} + 2na_{2n-1+k}x^{2n-1} + a_{2n-2+k}x^{2n-2} + a_{2n-3+k}x^{2n-3} + \cdots + a_{2+k}x^2 + a_{1+k}x + a_k.$$

Indices are taken modulo $2n+1$, so $a_{2n+k} = a_{k-1}$ and $a_{2n-1+k} = a_{k-2}$. Then

$$\sum_{j=1}^{2n} \alpha_{j,k} = 2n\left(\frac{a_{k-2}}{a_{k-1}}\right); \quad \prod_{j=1}^{2n} \alpha_{j,k} = \frac{a_k}{a_{k-1}}.$$

Since the $\alpha_{j,k}$'s are positive, AM-GM inequality can be applied and by virtue of it we are led to

$$\left(\frac{a_{k-2}}{a_{k-1}}\right)^{2n} \geq \frac{a_k}{a_{k-1}}.$$

for each k. As both sides of the inequalities are positive, multiplying them we obtain

$$\prod_{k=0}^{2n}\left(\frac{a_{k-2}}{a_{k-1}}\right)^{2n} \geq \prod_{k=0}^{2n} \frac{a_k}{a_{k-1}}.$$

But both sides are equal to 1. Therefore all the $2n+1$ A.M.-G.M. inequalities are equalities implying that for each k,

$$\alpha_{1,k} = \alpha_{2,k} = \cdots = \alpha_{2n,k} = \frac{a_{k-2}}{a_{k-1}}.$$

Since $n \geq 2$, using Vieta's relations gives

$$\frac{a_{k-3}}{a_{k-1}} = \sum_{1\leq i<j\leq 2n} \alpha_{i,k}\alpha_{j,k} = \binom{2n}{2}\left(\frac{a_{k-2}}{a_{k-1}}\right)^2.$$

Simplifying leads

$$\binom{2n}{2}\frac{a_{k-2}^2}{a_{k-1}^2} = a_{k-1}a_{k-3}$$

for each k. Multiplying all these equations yields

$$\left(\binom{2n}{2}\right)^{2n+1} - 1\left(\prod_{k=0}^{2n}\frac{a_{k-2}}{a_{k-1}}\right)^2 = 0,$$

which shows that at least one $a_k = 0$, a contradiction.

Example 4: [INMO-21] Find all pairs of integers (a, b) so that each of the two cubic polynomials

$$x^3 + ax + b \quad \text{and} \quad x^3 + bx + a$$

has all the roots to be integers.

Solution. The only such pair is $(0, 0)$, which clearly works. To prove this is the only one, let us prove an auxiliary result first.

Lemma. If α, β, γ are reals so that $\alpha + \beta + \gamma = 0$ and $|\alpha|, |\beta|, |\gamma| \geq 2$, then

$$|\alpha\beta + \beta\gamma + \gamma\alpha| < |\alpha\beta\gamma|.$$

Proof. Some two of these reals have the same sign; WLOG, suppose $\alpha\beta > 0$. Then $\gamma = -(\alpha + \beta)$, so by substituting this,

$$|\alpha\beta + \beta\gamma + \gamma\alpha| = |\alpha^2 + \beta^2 + \alpha\beta|, \quad |\alpha\beta\gamma| = |\alpha\beta(\alpha + \beta)|.$$

So we simply need to show $|\alpha\beta(\alpha + \beta)| > |\alpha^2 + \beta^2 + \alpha\beta|$. Since $|\alpha| \geq 2$ and $|\beta| \geq 2$, we have

$$|\alpha\beta(\alpha + \beta)| = |\alpha||\beta(\alpha + \beta)| \geq 2|\beta(\alpha + \beta)|,$$

$$|\alpha\beta(\alpha + \beta)| = |\beta||\alpha(\alpha + \beta)| \geq 2|\alpha(\alpha + \beta)|.$$

Adding these and using the triangle inequality,

$$\begin{aligned} 2|\alpha\beta(\alpha + \beta)| &\geq 2|\beta(\alpha + \beta)| + 2|\alpha(\alpha + \beta)| \\ &\geq 2|\beta(\alpha + \beta) + \alpha(\alpha + \beta)| \\ &\geq 2(|\alpha^2 + \beta^2 + 2\alpha\beta| \\ &> 2(|\alpha^2 + \beta^2 + \alpha\beta) \\ &= 2|\alpha^2 + \beta^2 + \alpha\beta|. \end{aligned}$$

Here we have used the fact that $\alpha^2 + \beta^2 + 2\alpha\beta = (\alpha + \beta)^2$ and $\alpha^2 + \beta^2 + \alpha\beta = \left(\frac{\alpha+\beta}{2}\right)^2 + \frac{3(\alpha^2)}{4}$ are both nonnegative. This proves our claim.

For our main problem, suppose the roots of $x^3 + ax + b$ are the integers r_1, r_2, r_3 and the roots of $x^3 + bx + a$ are the integers s_1, s_2, s_3. By Vieta's relations, we have

$$r_1 + r_2 + r_3 = 0 = s_1 + s_2 + s_3$$

$$r_1r_2 + r_2r_3 + r_3r_1 = a = -s_1s_2s_3$$

$$s_1s_2 + s_2s_3 + s_3s_1 = b = -r_1r_2r_3$$

If all six of these roots had an absolute value of at least 2, by our lemma, we would have

$$|b| = |s_1s_2 + s_2s_3 + s_3s_1| < |s_1s_2s_3| = |r_1r_2 + r_2r_3 + r_3r_1| < |r_1r_2r_3| = |b|,$$

which is absurd. Thus at least one of them is in the set $\{0, 1, -1\}$; WLOG, suppose it's r_1.

1. If $r_1 = 0$, then $r_2 = -r_3$, so $b = 0$. Then the roots of $x^3 + bx + a = x^3 + a$ are precisely the cube roots of $-a$, and these are all real only for $a = 0$. Thus $(a, b) = (0, 0)$, which is a solution.

2. If $r_1 = \pm 1$, then $\pm 1 + a + b = 0$, so a and b can't both be even. If $a = -s_1s_2s_3$ is odd, then s_1, s_2, s_3 are all odd, so $s_1 + s_2 + s_3$ cannot be zero. Similarly, if b is odd, we get a contradiction.

The proof is now complete.

Unsolved

1. Written on a blackboard is the polynomial $x^2 + x + 2014$. Calvin and Hobbes take turns alternatively (starting with Calvin) in the following game. During his turn, Calvin should either increase or decrease the coefficient of x by 1. And during his turn, Hobbes should either increase or decrease the constant coefficient by 1. Calvin wins if at any point of time the polynomial on the blackboard at that instant has integer roots. Prove that Calvin has a winning strategy.

2. Let a, b, c, d be positive integers such that $a \geq b \geq c \geq d$. Prove that the equation

$$x^4 - ax^3 - bx^2 - cx - d = 0$$

has no integer solution.

3. Consider two polynomials $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ and $Q(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$ with integer coefficients such that $a_n - b_n$ is a prime, $a_{n-1} = b_{n-1}$ and $a_n b_0 - a_0 b_n \neq 0$. Suppose there exists a rational number r such that $P(r) = Q(r) = 0$. Prove that r is an integer.

4. Let p, q, r be positive real numbers, not all equal, such that some two of the equations

$$px^2 + 2qx + r = 0, \quad qx^2 + 2rx + p = 0, \quad rx^2 + 2px + q = 0,$$

have a common root, say α. Prove that

(a) α is real and negative; and

(b) the third equation has non-real roots.

5. If α is a real root of the equation $x^5 - x^3 + x - 2 = 0$, prove that $\lfloor \alpha^6 \rfloor = 3$. (For any real number a, we denote by $\lfloor a \rfloor$ the greatest integer not exceeding a.)

6. Let a, b, c be three real numbers such that $1 \geq a \geq b \geq c \geq 0$. Prove that if λ is a root of the cubic equation $x^3 + ax^2 + bx + c = 0$ (real or complex), then $|\lambda| \leq 1$.

7. If $P(x), Q(x), R(x)$, and $S(x)$ are all polynomials such that

$$P(x^5) + xQ(x^5) + x^2 R(x^5) = (x^4 + x^3 + x^2 + x + 1)S(x),$$

prove that $x - 1$ is a factor of $P(x)$.

8. If $P(x)$ denotes a polynomial of degree n such that

$$P(k) = \frac{k}{k+1}$$

for $k = 0, 1, 2, \ldots, n$, determine $P(n+1)$.

9.7 Polynomials MCQ

1. For how many real values of p do the equations $x^2 + px + 1 = 0$ and $x^2 + x + p = 0$ have exactly one common root?

(A) 0 (B) 1 (C) 2 (D) 3

2. Let $f(x)$ be a degree five polynomial with real coefficients. Then the number of real roots of f must be

(A) 1 (B) 2 or 4 (C) 1 or 3 or 5 (D) none of the above

3. The number of rational roots of the polynomial $x^3 - 3x - 1$ is

(A) 0 (B) 1 (C) 2 (D) 3

4. Suppose a, b, and c are three numbers in G.P. If the equations $ax^2 + 2bx + c = 0$ and $dx^2 + 2ex + f = 0$ have a common root, then $\frac{d}{a}$, $\frac{e}{b}$, and $\frac{f}{c}$ are in

(A) A.P. (B) G.P. (C) H.P. (D) none of the above.

5. Suppose $x^2 + px + q = 0$ has two real roots α and β with $|\alpha| \neq |\beta|$. If α^4 and β^4 are the roots of $x^2 + rx + s = 0$, then the equation $x^2 - 4qx + 2q^2 + r = 0$ has

(A) one positive and one negative root (B) two distinct positive roots (C) two distinct negative roots (D) no real roots

6. The number of polynomials of the form $x^3 + ax^2 + bx + c$ which are divisible by $x^2 + 1$ and where a, b, and c belong to $\{1, 2, \ldots, 10\}$, is

(A) 1 (B) 10 (C) 11 (D) 100

7. The remainder $R(x)$ obtained by dividing the polynomial x^{100} by the polynomial $x^2 - 3x + 2$ is

(A) $2^{100} - 1$

(B) $(2^{100} - 1)x - 2(2^{99} - 1)$

(C) $2^{100}x - 3 \cdot 2^{100}$

(D) $(2^{100} - 1)x + 2(2^{99} - 1)$

8. The equations $x^3 + 2x^2 + 2x + 1 = 0$ and $x^{200} + x^{130} + 1 = 0$ have

(A) exactly one common root (B) no common root

(C) exactly three common roots (D) exactly two common roots

9. The sum of the coefficients of the polynomial $(x - 1)^2(x - 2)^4(x - 3)^6$ is

(A) 6 (B) 0 (C) 28 (D) 18

10. The polynomial $p(x) = x^4 - 4x^2 + 1$ has

(A) no roots in the interval $[0, 3]$

(B) exactly one root in the interval $[0, 3]$

(C) exactly two roots in the interval $[0, 3]$

(D) more than two roots in the interval $[0, 3]$

11. Let $f(x)$ be a real-valued function satisfying $af(x) + bf(-x) = px^2 + qx + r$, where a and b are distinct real numbers and p, q, and r are non-zero real numbers. Then $f(x) = 0$ will have real solution when

(A) $\left(\frac{a+b}{a-b}\right)^2 \leq \frac{q^2}{4pr}$ (B) $\left(\frac{a+b}{a-b}\right)^2 \leq \frac{4pr}{q^2}$

(C) $\left(\frac{a+b}{a-b}\right)^2 \geq \frac{q^2}{4pr}$ (D) $\left(\frac{a+b}{a-b}\right)^2 \geq \frac{4pr}{q^2}$

12. Let a and b be real numbers satisfying $a^2 + b^2 \neq 0$. Then the set of real numbers c, such that the equations $al + bm = c$ and $l^2 + m^2 = 1$ have real solutions for l and m is

(A) $[-\sqrt{a^2+b^2}, \sqrt{a^2+b^2}]$ (B) $[-|a+b|, |a+b|]$ (C) $[0, a^2+b^2]$ (D) $(-\infty, \infty)$

13. If $P(x) = ax^2 + bx + c$ and $Q(x) = -ax^2 + bx + c$, where $ac \neq 0$, then the equation $P(x)Q(x) = 0$ has:

(A) only real roots (B) no real root

(C) at least two real roots (D) exactly two real roots

14. Let $p_n(x)$, $n \geq 0$ be polynomials defined by $p_0(x) = 1$, $p_1(x) = x$, and $p_n(x) = xp_{n-1}(x) - p_{n-2}(x)$ for $n \geq 2$. Then $p_{10}(0)$ equals

(A) 0 (B) 10 (C) 1 (D) -1

15. If a, b, c are real numbers so that $x^3 + ax^2 + bx + c = (x^2+1)g(x)$ for some polynomial g, then

(A) $b = 1, a = c$ (B) $b = 0 = c$ (C) $a = 0$ (D) none of the above

16. The roots of the equation $x^4 + x^2 = 1$ are

(A) all real and positive (B) never real

(C) 2 positive and 2 negative (D) 1 positive, 1 negative and 2 non-real

17. If the roots of the equation $x^4 + ax^3 + bx^2 + cx + d = 0$ are in geometric progression then

(A) $b^2 = ac$ (B) $a^2 = b$ (C) $a^2b^2 = c^2$ (D) $c^2 = a^2d$

18. If all the roots of the equation $x^4 - 8x^3 + ax^2 + bx + 16 = 0$ are positive, then $a + b$

(A) must be -8

(B) can be any number strictly between -16 and -8

(C) must be -16

(D) can be any number strictly between -8 and 0

19. The polynomial $x^7 + x^2 + 1$ is divisible by

(A) $x^5 - x^4 + x^2 - x + 1$ (B) $x^5 + x^4 + 1$ (C) $x^5 + x^4 + x^2 + x + 1$ (D) $x^5 - x^4 + x^2 + x + 1$

20. Suppose that both the roots of the equation $x^2 + ax + 2016 = 0$ are positive even integers. The number of possible values of a is

(A) 6 (B) 12 (C) 18 (D) 24

ANSWER KEY

1	2	3	4	5	6	7	8	9	10
B	C	A	A	A	B	B	D	B	C
11	12	13	14	15	16	17	18	19	20
D	A	C	D	A	D	D	A	A	B

10 Inequalities

10.1 Some basic Identities

Among the basic properties of order relation in $\mathbb{R}$, we have the following:

For all $a, b, c \in \mathbb{R}$,

(I) Exactly one of the following is true: $a < b$, $a = b$, $a > b$.

(II) If $a < b$ and $b < c$ then $a < c$.

(III) If $a < b$ then $a + c < b + c$.

(IV) If $a < b$ and $c > 0$ then $ac < bc$.

These properties imply the following important results.

1. $a > 0$ and $b > 0 \Rightarrow ab > 0$.

2. $a < b$ and $c < 0 \Rightarrow ac > bc$.

3. For every $a \in \mathbb{R}$, $a^2 \geq 0$, and equality occurs if and only if $a = 0$. This is equivalent to the following: (i) $a \neq 0 \Rightarrow a^2 > 0$, and (ii) $a = 0 \Rightarrow a^2 = 0$.

4. If a, b, c, d are all positive, and if $a > b$ and $c > d$, then, (i) $ac > bd$, (ii) $(a/d) > (b/c)$.

5. Let $a > 0$, $b > 0$ and $m \in \mathbb{N}$. Then $a > b \Leftrightarrow a^m > b^m$.

6. Let $a > 0$. Then $f(x) = ax^2 + bx + c \geq 0$, for all $x \in \mathbb{R}$ if and only if $b^2 - 4ac \leq 0$.

We note that

$$f(x) = a\left[\left(x + \frac{b}{2a}\right)^2 + \frac{4ac - b^2}{4a^2}\right].$$

Example 1: If $a > 0$ then show that $a + \frac{1}{a} \geq 2$, with equality if and only if $a = 1$.

Solution: This follows because the inequality is equivalent to $(a-1)^2 \geq 0$.

Example 2: If a, b, c, d are positive, then show that

$$\sqrt{(a+c)(b+d)} \geq \sqrt{ab} + \sqrt{cd}.$$

Solution: Since all terms are positive, the inequality is equivalent to that obtained by squaring both sides. Hence (1) is equivalent to $(a+c)(b+d) \geq ab + cd + 2\sqrt{abcd}$ i.e. to $ad + bc \geq 2\sqrt{abcd}$.

Example 3: If $a, b, c > 0$ and $a + b + c = 1$, then show that $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} \geq 9$.

Solution: For, on dividing $a + b + c = 1$ by a, b, c in turn, we get

$$1 + \frac{b}{a} + \frac{c}{a} = \frac{1}{a}, \quad \frac{a}{b} + 1 + \frac{c}{b} = \frac{1}{b}, \quad \frac{a}{c} + \frac{b}{c} + 1 = \frac{1}{c}.$$

Adding,

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 3 + \left(\frac{a}{b} + \frac{b}{a}\right) + \left(\frac{b}{c} + \frac{c}{b}\right) + \left(\frac{a}{c} + \frac{c}{a}\right) \geq 3 + 2 + 2 + 2 = 9, \text{ by Ex. 1.}$$

Note that equality occurs if and only if $a = b = c$.

Example 4: If a, b, c are positive, then show that $(a+b)(b+c)(c+a) \geq 8abc$.

Solution: By Example. 1, $\frac{\sqrt{a}}{\sqrt{b}} + \frac{\sqrt{b}}{\sqrt{a}} \geq 2$ or $\frac{a+b}{\sqrt{ab}} \geq 2$. Similarly, $\frac{b+c}{\sqrt{bc}} \geq 2$ and $\frac{c+a}{\sqrt{ca}} \geq 2$. Multiplying these three inequalities the result follows.

10.2 The three mean inequality

The Three Means: If a, b are positive real numbers, we define their arithmetic mean (A.M.), geometric mean (G.M.) and harmonic mean (H.M.) as follows

$$\text{A.M.} = A = \frac{a+b}{2}, \quad \text{G.M.} = G = \sqrt{ab}, \quad \text{H.M.} = H = \left(\frac{1}{a} + \frac{1}{b}\right)^{-1}.$$

Remark 2.1 Note that the H.M. is the reciprocal of the A.M. of the reciprocals of the given numbers. Further, H.M. of a and b is $\frac{2ab}{a+b}$. We also note that the A.M. can be defined for any real numbers (not necessarily positive) but to define G.M. and H.M. we require necessarily positive real numbers.

Theorem 1 If a, b are positive, then $A \geq G \geq H$. Also, equality occurs if and only if $a = b$.

Proof: First let $a \neq b$. Then $\sqrt{a}$ and $\sqrt{b}$ are unequal and so $(\sqrt{a} - \sqrt{b})^2 \geq 0$. Hence the identities $A - G = \frac{a+b}{2} - \sqrt{ab} = \frac{1}{2}(\sqrt{a} - \sqrt{b})^2$, $G - H = \frac{\sqrt{ab} - \frac{2ab}{a+b}}{a+b} = \frac{\sqrt{ab}(\sqrt{a}-\sqrt{b})^2}{a+b}$ respectively show that $A > G$ and $G > H$. If $a = b$, it is clear that $A = G = H = a$.

Corollary: If $a > b > 0$, then $a > A > G > H > b$.

Example 5 If $a_1, a_2, \ldots, a_n$ are all positive, then show that

$$\sqrt{a_1 a_2} + \sqrt{a_1 a_3} + \ldots + \sqrt{a_{n-1} a_n} \leq \frac{n-1}{2}(a_1 + a_2 + \ldots + a_n).$$

Solution: Add the $n(n-1)/2$ inequalities

$$\sqrt{a_1 a_2} \leq \frac{a_1 + a_2}{2}, \sqrt{a_1 a_3} \leq \frac{a_1 + a_3}{2}, \ldots, \sqrt{a_{n-1} a_n} \leq \frac{a_{n-1} + a_n}{2},$$

and note that in the sum on the right each a_i occurs $n-1$ times. [**For example, for** $n = 4$**, we have to consider 6 terms:** $\sqrt{a_1 a_2}, \sqrt{a_1 a_3}, \sqrt{a_1 a_4}, \sqrt{a_2 a_3}, \sqrt{a_2 a_4}, \sqrt{a_3 a_4}$.

If $a_1, \ldots, a_n$ are n positive real numbers, we define their arithmetic mean A_n, geometric mean G_n and harmonic mean H_n as follows:

$$A_n = \frac{a_1 + \ldots + a_n}{n}, \quad G_n = (a_1 a_2 \ldots a_n)^{1/n}, \quad H_n = \frac{n}{\frac{1}{a_1} + \ldots + \frac{1}{a_n}}.$$

We observe that one can have a remark similar to Remark 2.1 here. We also have the following generalization of theorem 9.

Theorem 2 If $a_1, \ldots, a_n$ are positive real numbers, then

$$A_n \geq G_n \geq H_n,$$

and equality occurs if and only if $a_1 = a_2 = \ldots = a_n$.

Proof: First we prove by induction on n that $A_n \geq G_n$ with equality if and only if all the n numbers are equal. The result is true for $n = 2$. Assume the result for $n = m - 1$. Suppose $0 < a_1 \leq a_2 \leq \ldots \leq a_m$. We note that the result is true if $a_1 = a_m$. Suppose $a_1 < a_m$. Then clearly

$$m a_1 < a_1 + a_2 + \ldots + a_m < m a_m,$$

so that $a_1 < A_m < a_m$. Hence

$$A_m(a_1 + a_m - A_m) - a_1 a_m = (a_1 - A_m)(A_m - a_m) > 0$$

and so

$$a_1 + a_m - A_m > \frac{a_1 a_m}{A_m} \tag{3}$$

Now since the A.M. of the $m-1$ numbers $a_2, \ldots, a_{m-1}, a_1+a_m-A_m$ is A_m, we have by induction hypothesis,

$$A_{m-1} \geq \frac{a_2 \cdots a_{m-1}(a_1 + a_m - A_m)}{m} > \frac{a_2 \cdots a_{m-1} \frac{a_1 a_m}{A_m}}{m} \quad \text{[by (3)]}$$

Hence $A_m > a_1 a_2 \cdots a_m$ i.e. $A_m > G_m$.
Thus the result is true for $n = m$ and the induction is complete. We also observe that when the a_i's are unequal, the arithmetic mean is strictly greater than the geometric mean. Hence, if the arithmetic mean and the geometric mean are equal then all the a_i's must be equal.

Finally, applying this result to the n positive numbers $\frac{1}{a_1}, \ldots, \frac{1}{a_n}$ we see that $G_n \geq H_n$, with equality if and only if $a_1 = \ldots = a_n$.

Example 6 If $b_1, \ldots, b_n$ is a permutation of the n positive numbers $a_1, \ldots, a_n$, then

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} + \cdots + \frac{a_n}{b_n} \geq n.$$

Solution. Using AM-GM inequality for the numbers $\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}$, we get

$$\frac{1}{n}\left(\frac{a_1}{b_1} + \frac{a_2}{b_2} + \cdots + \frac{a_n}{b_n}\right) \geq \left(\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} \cdots \frac{a_n}{b_n}\right)^{1/n} = 1.$$

Example 7 Let x, y, z be positive real numbers satisfying $x + y + z = 1$. Prove that

$$xy(x+y)^2 + yz(y+z)^2 + zx(z+x)^2 \geq 4xyz.$$

Solution. As $x + y + z = 1$, the given inequality holds if and only if

$$xy(1-z)^2 + yz(1-x)^2 + zx(1-y)^2 \geq 4xyz$$

if and only if

$$xy + yz + zx - 6xyz + xy^2 + yz^2 + zx^2 \geq 4xyz$$

if and only if

$$\frac{1}{z} + \frac{1}{x} + \frac{1}{y} + x + y + z \geq 10$$

if and only if

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} \geq 9 \quad \text{or} \quad \frac{1}{3} \geq \frac{3}{1 + \frac{1}{x} + \frac{1}{y} + \frac{1}{z}}.$$

whihc is true as $x + y + z = 1$ and AM$\geq$HM applies.

10.3 Exercise 10.1

1. For $a, b, c > 0$, prove that

$$\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} \geq \frac{3}{2}$$

2. Let a, b, c be side-lengths of a triangle. Prove that,

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} \leq \frac{1}{b+c-a} + \frac{1}{c+a-b} + \frac{1}{a+b-c}.$$

3. For $a_1, \ldots, a_n > 0$ with $a_1 + \cdots + a_n = s$ prove that

$$\frac{a_1}{s-a_1} + \frac{a_2}{s-a_2} + \cdots + \frac{a_n}{s-a_n} \geq \frac{n}{n-1}.$$

4. For $a, b, c > 0$ show that,

$$\frac{ab}{a+b+2c} + \frac{bc}{b+c+2a} + \frac{ca}{c+a+2b} \leq \frac{a+b+c}{4}.$$

5. Let $a, b, c \in \mathbb{R}^+$. Prove the inequalities

$$\frac{9abc}{2(a+b+c)} \leq \frac{ab^2}{a+b} + \frac{bc^2}{b+c} + \frac{ca^2}{c+a} \leq \frac{a^2+b^2+c^2}{2}.$$

10.4 Cauchy-Schwarz Inequality

Another inequality which is useful in applications is the Cauchy-Schwarz inequality. We express this as a theorem.

Theorem 1. Let $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ be two sets of real numbers.

Then

$$\left(\sum_{i=1}^{n} a_i b_i\right)^2 \leq \left(\sum_{i=1}^{n} a_i^2\right)\left(\sum_{i=1}^{n} b_i^2\right) \tag{1}$$

and equality holds in (1) if and only if

$$\frac{a_1}{b_1} = \frac{a_2}{b_2} = \cdots = \frac{a_n}{b_n}. \tag{2}$$

Proof. Let us put

$$A = \sum_{i=1}^{n} a_i^2, \quad B = \sum_{i=1}^{n} b_i^2, \quad C = \sum_{i=1}^{n} a_i b_i.$$

Then (1) is equivalent to

$$C^2 \leq AB. \tag{3}$$

If $B = 0$, then $b_i = 0$ for $i = 1, 2, \ldots, n$. Hence $C = 0$ and (3) is true. Therefore it is sufficient to consider the case $B \neq 0$. This implies that $B > 0$. We now have

$$0 \leq \sum_{i=1}^{n}(Ba_i - Cb_i)^2 = \sum_{i=1}^{n}\left(B^2 a_i^2 - 2BCa_i b_i + C^2 b_i^2\right) = B^2 \sum_{i=1}^{n} a_i^2 - 2BC \sum_{i=1}^{n} a_i b_i + C^2 \sum_{i=1}^{n} b_i^2 = B(AB - C^2).$$

Since $B > 0$, we get $AB - C^2 \geq 0$ which is the required inequality (3). Moreover, equality holds if and only if

$$\sum_{i=1}^{n}(Ba_i - Cb_i)^2 = 0.$$

This is equivalent to

$$\frac{a_i}{b_i} = \frac{C}{B} \quad \text{for } i = 1, 2, \ldots, n.$$

Remark. The Cauchy-Schwarz inequality is also true for complex numbers with a little modification. If $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ are two sets of complex numbers, then

$$\left|\sum_{i=1}^{n} a_i b_i\right|^2 \leq \left(\sum_{i=1}^{n} |a_i|^2\right)\left(\sum_{i=1}^{n} |b_i|^2\right) \tag{4}$$

with equality in (4) if and only if $a_i = \lambda b_i$ for some constant λ, $i = 1, 2, \ldots, n$. The proof of this inequality is left to the problems at the end of the chapter.

Example 1. If $a_1, a_2, \ldots, a_n$ are real numbers such that $a_1 + a_2 + \ldots + a_n = 1$, prove that

$$a_1^2 + a_2^2 + \ldots + a_n^2 \geq \frac{1}{n}.$$

Solution. We have

$$1 = (a_1 + a_2 + \ldots + a_n)^2 = (a_1 \cdot 1 + a_2 \cdot 1 + \ldots + a_n \cdot 1)^2 \leq (a_1^2 + a_2^2 + \ldots + a_n^2)(1 + 1 + \ldots + 1) = n(a_1^2 + a_2^2 + \ldots + a_n^2).$$

Therefore,

$$a_1^2 + a_2^2 + \ldots + a_n^2 \geq \frac{1}{n}.$$

Example 2. If a, b, c, d are positive real numbers such that $c^2 + d^2 = (a^2 + b^2)^3$, prove that

$$\frac{a^3}{c} + \frac{b^3}{d} \geq 1,$$

with equality iff $ad = bc$.

Solution: Using Cauchy-Schwarz inequality, we get

$$\begin{aligned}(a^2+b^2)^2 &= \left(\sqrt{\frac{a^3}{c}} \cdot \sqrt{ac} + \sqrt{\frac{b^3}{d}} \cdot \sqrt{bd}\right)^2 \\ &\leq \left(\frac{a^3}{c} + \frac{b^3}{d}\right)(ac+bd)\end{aligned}$$

where equality holds iff $a^2d^2 = b^2c^2$.

Thus

$$\begin{aligned}\left(\frac{a^3}{c} + \frac{b^3}{d}\right)(ac+bd) &\leq (a^2+b^2)^2 \\ &= (a^2+b^2)^{1/2}(a^2+b^2)^{3/2} \\ &= (a^2+b^2)^{1/2}(c^2+d^2)^{1/2} \\ &\geq ac+bd\end{aligned}$$

again by another application of Cauchy-Schwarz inequality. Equality holds in the last step iff $\frac{a}{c} = \frac{b}{d}$.

Combining both, we get

$$\frac{a^3}{c} = \frac{b^3}{d} \geq 1$$

and equality holds iff $ad = bc$.

10.5 Exercise 2.2

1. Find the maximum value of $2x + 5y + 4z$ where x, y, z are real numbers (not necessarily positive) satisfying $x^2 + 5y^2 + z^2 = 1$.

2. Find the minimum value of $2x^2 + 3y^2 + 6z^2$ where x, y, z are real numbers (not necessarily positive) satisfying $x + y + z = 7$.

3. For $x, y, z \in \mathbb{R}$, show that,

$$\left(\frac{x}{2} + \frac{y}{3} + \frac{z}{6}\right)^2 \leq \left(\frac{x^2}{2} + \frac{y^2}{3} + \frac{z^2}{6}\right)$$

4. Suppose $P(x) = a_0 + a_1x + \cdots + a_nx^n$ with $a_k \geq 0$ for each $k = 0, 1, \ldots, n$. Show that if $P(x)P(1/x) \geq 1$ holds for $x = 1$ then it holds for every non-zero $x \in \mathbb{R}$.

5. For $x, y, z \geq 0$, prove that,

$$\sqrt{x(3x + y)} + \sqrt{y(3y + z)} + \sqrt{z(3z + x)} \leq 2(x + y + z).$$

6. Suppose $x, y, z > 1$ satisfy $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 2$. Prove that,

$$\sqrt{x + y + z} \geq \sqrt{x - 1} + \sqrt{y - 1} + \sqrt{z - 1}.$$

7. Let $a, b, c \in \mathbb{R}^+$ such that,

$$\frac{1}{a + b + 1} + \frac{1}{b + c + 1} + \frac{1}{c + a + 1} \geq 1.$$

Prove that, $a + b + c \geq ab + bc + ca$.

8. Let a, b, c be positive real numbers with $abc = 1$. Prove that

$$\frac{a}{a + b^4 + c^4} + \frac{b}{b + c^4 + a^4} + \frac{c}{c + a^4 + b^4}$$

10.6 Rearrangement and Chebycheff

Theorem (Rearrangement inequality) If $x_1, x_2, \ldots, x_n$ and $y_1, y_2, \ldots, y_n$ are two non-decreasing sequences of real numbers, and if $\sigma_1, \sigma_2, \ldots, \sigma_n$ is any permutation of $\{1, 2, \ldots, n\}$, then the following inequality holds:

$$x_1y_n + x_2y_{n-1} + \cdots + x_ny_1 \leq x_1y_{\sigma_1} + x_2y_{\sigma_2} + \cdots + x_ny_{\sigma_n} \leq x_1y_1 + x_2y_2 + \cdots + x_ny_n.$$

Proof: Let us prove the right inequality. The left one will follow by applying the right one to the sequences $x_1, x_2, \ldots, x_n$ and $-y_n, -y_{n-1}, \ldots, -y_1$.

We will prove the right inequality by induction on n. For $n = 2$, the statement can be easily proved. Assume that the statement holds for all pairs of sequences of lengths $1, 2, \ldots, n$. Let $x_1 \leq x_2 \leq \cdots \leq x_{n+1}$ and $y_1 \leq y_2 \leq \cdots \leq y_{n+1}$ be two sequences of real numbers, and let $\sigma_1, \sigma_2, \ldots, \sigma_{n+1}$ be a permutation of $\{1, 2, \ldots, n+1\}$. Let i be the integer such that $\sigma_i = n + 1$.

Then we have

$$\begin{gathered} x_1y_{\sigma_1} + x_2y_{\sigma_2} + \cdots + (x_iy_{\sigma_i} + x_{i+1}y_{\sigma_{i+1}}) + \cdots + x_{n+1}y_{n+1} \leq \\ x_1y_{\sigma_1} + x_2y_{\sigma_2} + \cdots + (x_iy_{\sigma_{i+1}} + x_{i+1}y_{\sigma_i}) + \cdots + x_{n+1}y_{n+1}. \end{gathered}$$

The last inequality holds because we applied the case $n = 2$ for the non-decreasing sequences (x_i, x_{i+1}) and $(y_{\sigma_{i+1}}, y_{\sigma_i})$. The previous inequality can be now written as

$$\sum_{j=1}^{n+1} x_jy_{\sigma_j} \leq \sum_{j=1}^{n+1} x_jy_{\tau_j^1},$$

where $\tau_1^1, \tau_2^1, \ldots, \tau_{n+1}^1$ is the permutation obtained from $\sigma_1, \sigma_2, \ldots, \sigma_{n+1}$ by transposing the term $n + 1$ with the one that is adjacent and to the right. Repeating this procedure we obtain the inequality

$$\sum_{i=j}^{n+1} x_jy_{\sigma_j} \leq \sum_{j=1}^{n+1} x_jy_{\tau_j^{n+1-i}}.$$

We now have $\tau_{n+1-i}^{n+1} = n + 1$ and we can apply inductive hypothesis to obtain

$$\sum_{j=1}^{n} x_jy_{\tau_j^{n+1-i}} \leq \sum_{j=1}^{n} x_jy_j \Rightarrow \sum_{j=1}^{n+1} x_jy_{\tau_j^{n+1-i}} \leq \sum_{j=1}^{n+1} x_jy_j.$$

Example 1: Suppose a, b, c are side-lengths of a triangle. Prove that,

$$a^2(b + c - a) + b^2(c + a - b) + c^2(a + b - c) \leq 3abc.$$

Solution: First note that,

$$a(b + c - a) \leq b(c + a - b) \iff 0 \leq (a - b)(a + b - c) \iff a \leq b.$$

Thus, $a(b + c - a), b(c + a - b), c(a + b - c)$ and a, b, c are ordered oppositely. Hence,

$$\sum_{\text{cyc}} a^2(b + c - a) \leq \sum_{\text{cyc}} b \cdot a(b + c - a), \quad \sum_{\text{cyc}} a^2(b + c - a) \leq \sum_{\text{cyc}} c \cdot a(b + c - a).$$

Just adding these two inequalities and collecting terms on the RHS,

$$2\sum_{\text{cyc}} a^2(b + c - a) \leq \sum_{\text{cyc}} ba(b + c - a + c + a - b) = 6abc.$$

Theorem (Chebyshev)
Let $a_1 \geq a_2 \geq \cdots \geq a_n$ and $b_1 \geq b_2 \geq \cdots \geq b_n$ be real numbers. Then

$$n \sum_{i=1}^{n} a_i b_i \geq \left(\sum_{i=1}^{n} a_i \right) \left(\sum_{i=1}^{n} b_i \right) \geq n \sum_{i=1}^{n} a_i b_{n+1-i}. \tag{1}$$

The two inequalities become equalities at the same time when $a_1 = a_2 = \cdots = a_n$ or $b_1 = b_2 = \cdots = b_n$.

Proof
According to rearrangement inequality we have the following relations:

$$\begin{aligned} a_1b_1 + a_2b_2 + a_3b_3 + \cdots + a_nb_n &\geq a_1b_1 + a_2b_2 + a_3b_3 + \cdots + a_nb_n \\ &\geq a_1b_2 + a_2b_3 + a_3b_4 + \cdots + a_nb_1 \\ &\geq a_1b_3 + a_2b_4 + a_3b_5 + \cdots + a_nb_2 \\ &\vdots \\ &\geq a_1b_n + a_2b_{n-1} + \cdots + a_nb_1. \end{aligned}$$

Summing up these n inequalities we obtain (1).

Example 2: Let a, b, c be side-lengths of a triangle. Prove that,

$$a^2b(a-b) + b^2c(b-c) + c^2a(c-a) \geq 0.$$

Solution: From last solution, we see that, $a(b+c-a), b(c+a-b), c(a+b-c)$ and a, b, c are oppositely ordered. (and so the first three are similarly ordered as $1/a, 1/b, 1/c$.

$$\sum_{\text{cyc}} \frac{1}{a} \cdot a(b+c-a) \geq \sum_{\text{cyc}} \frac{1}{c} \cdot a(b+c-a)$$

$$\begin{aligned} &\Rightarrow a+b+c \geq a+b+c + \frac{a(b-a)}{c} + \frac{b(c-b)}{a} + \frac{c(a-c)}{b} \\ &\Rightarrow a^2b(a-b) + b^2c(b-c) + c^2a(c-a) \geq 0. \end{aligned}$$

Example 3: Let x, y, z be real numbers, each greater than 1. Prove that

$$\frac{x+1}{y+1} + \frac{y+1}{z+1} + \frac{z+1}{x+1} \leq \frac{x-1}{y-1} + \frac{y-1}{z-1} + \frac{z-1}{x-1}.$$

Solution: RHS - LHS is sum of terms like $\frac{x-1}{y-1} - \frac{x+1}{y+1} = \frac{2(x-y)}{y^2-1}$, so it suffices to show that

$$\frac{x}{x^2-1} + \frac{y}{y^2-1} + \frac{z}{z^2-1} \leq \frac{x}{y^2-1} + \frac{y}{z^2-1} + \frac{z}{x^2-1}$$

which follows from rearrangement inequality as x, y, z and $\frac{1}{x^2-1}, \frac{1}{y^2-1}, \frac{1}{z^2-1}$ are oppositely sorted.

10.7 Exercise

1. If $a, b, c, d > 0$, then show that at least one of the following inequalities is wrong:

$$a + b < c + d, \quad (a + b)(c + d) < ab + cd, \quad (a + b)cd < ab(c + d).$$

2. For any $n \in \mathbb{N}$, prove that,

$$\frac{1}{2} \le \frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n} \le \frac{3}{4}.$$

3. Let $a, b, c, d \in \mathbb{R}^+$ such that $abcd = 1$. Prove that,

$$\frac{1}{a+b+2} + \frac{1}{b+c+2} + \frac{1}{c+d+2} + \frac{1}{d+a+2} \le 1.$$

4. Let $a, b, c, d \in \mathbb{R}^+$ such that $abcd = 1$. Prove that,

$$a^4(1+a) + b^4(1+b) + c^4(1+c) + d^4(1+d) \ge \frac{1}{2}(1+a)(1+b)(1+c)(1+d).$$

5. For $a, b, c > 0$, prove that,

$$\left(\frac{a}{b} + \frac{b}{c} + \frac{c}{a}\right) + \left(\frac{b}{a} + \frac{c}{b} + \frac{a}{c}\right) \ge 6,$$

$$\left(\frac{a}{b} + \frac{b}{c} + \frac{c}{a}\right) + \left(\frac{b}{a} + \frac{c}{b} + \frac{a}{c}\right) \ge 3 + x, \quad \text{where } 3 \ge x.$$

6. For any $a, b, c \in \mathbb{R}^+$, prove that,

$$ab(a+b) + bc(b+c) + ca(c+a) \ge \sum_{\text{cyc}} \sqrt{\frac{a}{b}(b+c)(c+a)}.$$

7. Let $a_1, a_2, \ldots, a_n$ and $b_1, \ldots, b_n$ be real numbers and let $A, B > 0$ such that $A^2 \ge a_1^2 + a_2^2 + \cdots + a_n^2$ and $B^2 \ge b_1^2 + b_2^2 + \cdots + b_n^2$. Prove that,

$$(A^2 - a_1^2 - a_2^2 - \cdots - a_n^2)(B^2 - b_1^2 - b_2^2 - \cdots - b_n^2) \le (AB - a_1b_1 - a_2b_2 - \cdots - a_nb_n)^2.$$

8. Let a, b, c be positive real numbers. Find the extreme values of the expression

$$\sqrt{a^2x^2 + b^2y^2 + c^2z^2} + \sqrt{b^2x^2 + c^2y^2 + a^2z^2} + \sqrt{c^2x^2 + a^2y^2 + b^2z^2},$$

where x, y, z are real numbers such that $x^2 + y^2 + z^2 = 1$.

9. For $a, b, c \ge 1$, prove that

$$\sqrt{a-1} + \sqrt{b-1} + \sqrt{c-1} \le \sqrt{a(bc+1)}.$$

10. For $a, b, c > 0$, prove that

$$\frac{1}{\sqrt{a^3+1}} + \frac{1}{\sqrt{b^3+1}} + \frac{1}{\sqrt{c^3+1}} \le 1.$$

11. Prove that,

$$a^2 + b^2 + c^2 \ge 12.$$

12. Let a, b, c be positive real numbers with $abc = 1$. Prove that,

$$\left(a - 1 + \frac{1}{b}\right)\left(b - 1 + \frac{1}{c}\right)\left(c - 1 + \frac{1}{a}\right) \le 1.$$

13. If x, y, z be positive real numbers, prove that,

$$3(x^2+xy+y^2)(y^2+yz+z^2)(z^2+zx+x^2) \geq (x+y+z)^2(xy+yz+zx)^2.$$

14. Let a, b, c, d be positive real numbers with sum 4. Prove that,

$$\frac{a}{1+b^2c}+\frac{b}{1+c^2d}+\frac{c}{1+d^2a}+\frac{d}{1+a^2b} \geq 2.$$

15. Let $x, y \in \mathbb{R}^+$ such that $x+y=2$. Prove that,

$$x^3y^3(x^3+y^3) \leq 2.$$

16. Prove that,

$$\prod_{k=1}^{n} k^k = 1^1 \cdot 2^2 \cdot 3^3 \cdots n^n > \left(\frac{n+1}{2}\right)^{n(n+1)/2}.$$

17. Suppose a, b, c are side lengths of a triangle. Prove that,

$$\left(1+\frac{b-c}{a}\right)^a \left(1+\frac{c-a}{b}\right)^b \left(1+\frac{a-b}{c}\right)^c \leq 1.$$

18. Let $a, b, c > 0$ such that $a+b+c=1$. Prove that,

$$a^a b^b c^c + a^b b^c c^a + a^c b^a c^b \leq 1.$$

19. Let a, b, c be positive reals such that $a+b+c=\sqrt{a}+\sqrt{b}+\sqrt{c}$. Prove that, $a^a b^b c^c \geq 1$.

20. For $a, b, c > 0$, prove that,

$$\frac{a+b+c}{\sqrt[3]{abc}}+\frac{8abc}{(a+b)(b+c)(c+a)} \geq 4.$$

21. Let $a, b, c \in \mathbb{R}^+$. Prove that,

$$\frac{1}{\sqrt{a^3+b}}+\frac{1}{\sqrt{b^3+c}}+\frac{1}{\sqrt{c^3+a}} \leq \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{a}}+\frac{1}{\sqrt{b}}+\frac{1}{\sqrt{c}}\right).$$

22. For $0<x<1$ prove that,

$$x+\frac{1}{x^x}<2.$$

23. For $n \geq 3$, suppose $a_2, a_3, \ldots, a_n \in \mathbb{R}^+$ such that $a_2a_3\cdots a_n=1$. Prove that,

$$(1+a_2)^2(1+a_3)^3\cdots(1+a_n)^n > n^n.$$

24. Suppose $a, b, c, d \in \mathbb{R}^+$ such that $abcd=1$ and

$$a+b+c+d > \frac{a}{b}+\frac{b}{c}+\frac{c}{d}+\frac{d}{a}. \quad \text{Prove that,} \quad a+b+c+d < \frac{b}{a}+\frac{c}{b}+\frac{d}{c}+\frac{a}{d}.$$

10.8 Some Harder Problems

Example 1: Let x, y, z be real numbers, each greater than 1. Prove that

$$\frac{x+1}{y+1}+\frac{y+1}{z+1}+\frac{z+1}{x+1} \leq \frac{x-1}{y-1}+\frac{y-1}{z-1}+\frac{z-1}{x-1}.$$

Solution: We may assume that $x=\max\{x, y, z\}$. There are two cases: $x \geq y \geq z$ and $x \geq z \geq y$. We consider both these cases. The inequality is equivalent to

$$\left\{\frac{x-1}{y-1}+\frac{x+1}{y+1}\right\}+\left\{\frac{y-1}{z-1}+\frac{y+1}{z+1}\right\}+\left\{\frac{z-1}{x-1}+\frac{z+1}{x+1}\right\} \geq 0.$$

This is further equivalent to

$$\frac{x-y}{y^2-1}+\frac{y-z}{z^2-1}+\frac{z-x}{x^2-1} \geq 0.$$

Suppose $x \geq y \geq z$. We write

$$\frac{x-y}{y^2-1}+\frac{y-z}{z^2-1}+\frac{z-x}{x^2-1}=\frac{x-y}{y^2-1}+\frac{y-z}{z^2-1}+\frac{z-x}{x^2-1}.$$

This reduces to

$$(x-y)\left(\frac{x^2-y^2}{(x^2-1)(y^2-1)}\right)+(y-z)\left(\frac{y^2-z^2}{(y^2-1)(z^2-1)}\right).$$

Since $x \geq y$ and $x \geq z$, this sum is nonnegative.

Suppose $x \geq z \geq y$. We write

$$\frac{x-y}{y^2-1}+\frac{y-z}{z^2-1}+\frac{z-x}{x^2-1}=\frac{x-z+z-y}{y^2-1}+\frac{y-z}{z^2-1}+\frac{z-x}{x^2-1}.$$

This reduces to

$$(x-z)\left(\frac{x^2-y^2}{(x^2-1)(y^2-1)}\right)+(z-y)\left(\frac{z^2-y^2}{(y^2-1)(z^2-1)}\right).$$

Since $x \geq z$ and $z \geq y$, this sum is nonnegative.

Thus

$$\frac{x-y}{y^2-1}+\frac{y-z}{z^2-1}+\frac{z-x}{x^2-1} \geq 0$$

in both the cases. This completes the proof.

Example 2: Let a, b, c be positive real numbers such that

$$\frac{a}{1+a}+\frac{b}{1+b}+\frac{c}{1+c}=1.$$

Prove that $abc \leq 1/8$.

Solution: This is equivalent to

$$\sum a(1+b)(1+c)=(1+a)(1+b)(1+c).$$

This simplifies to

$$ab+bc+ca+2abc=1.$$

Using AM-GM inequality, we have

$$1=ab+bc+ca+2abc \geq 4(ab \cdot bc \cdot ca \cdot 2abc)^{1/4}.$$

Simplification gives

$$abc \leq \frac{1}{8}.$$

Example 3: Let a, b, c be positive real numbers such that $abc = 1$. Prove that

$$\frac{a^3}{(a-b)(a-c)} + \frac{b^3}{(b-c)(b-a)} + \frac{c^3}{(c-a)(c-b)} \geq 3.$$

Solution: Observe that

$$\frac{1}{(a-b)(a-c)} = \frac{(b-c)}{(a-b)(b-c)(a-c)} = \frac{(a-c)-(a-b)}{(a-b)(b-c)(a-c)} = \frac{1}{(a-b)(b-c)} - \frac{1}{(b-c)(a-c)}.$$

Hence

$$\begin{aligned}
\frac{a^3}{(a-b)(a-c)} + \frac{b^3}{(b-c)(b-a)} + \frac{c^3}{(c-a)(c-b)} &= \frac{a^3-b^3}{(a-b)(b-c)} + \frac{c^3-a^3}{(c-a)(c-b)} \\
&= \frac{a^2+ab+b^2}{b-c} - \frac{c^2+ca+a^2}{b-c} \\
&= \frac{ab+b^2-c^2-ca}{b-c} \\
&= \frac{(a+b+c)(b-c)}{b-c} = a+b+c.
\end{aligned}$$

Therefore

$$\frac{a^3}{(a-b)(a-c)} + \frac{b^3}{(b-c)(b-a)} + \frac{c^3}{(c-a)(c-b)} = a+b+c \geq 3(abc)^{1/3} = 3.$$

Example 4: Let a, b, c be positive real numbers such that

$$\frac{ab}{1+bc} + \frac{bc}{1+ca} + \frac{ca}{1+ab} = 1.$$

Prove that

$$\frac{1}{a^3} + \frac{1}{b^3} + \frac{1}{c^3} \geq 6\sqrt{2}.$$

Solution: The given condition is equivalent to

$$\sum ab(1+ca)(1+ab) = (1+ab)(1+bc)(1+ca).$$

This gives

$$\sum ab + \sum a^2b^2 + abc\sum a + abc\sum a + a^2b^2c^2 = 1 + \sum ab + abc\sum a + a^2b^2c^2.$$

Hence

$$a^2b^2c^2 + 1 = \sum a^2b^2 + abc\sum a^2b.$$

Using

$$\sum a^2b^2 \geq 3(abc)^{4/3}, \quad \sum a^2b \geq 3abc,$$

we get

$$a^2b^2c^2 + 1 \geq 3(abc)^{4/3} + 3(abc)^2.$$

Taking $x = (abc)^{2/3}$, this reduces to $2x^3 + 3x^2 - 1 \leq 0$. This gives $(x+1)^2(2x-1) \leq 0$. Hence $x \leq 1/2$. Therefore $abc \leq \frac{1}{2}\sqrt{2}$. Finally,

$$\frac{1}{a^3} + \frac{1}{b^3} + \frac{1}{c^3} \geq \frac{3}{abc} \geq 6\sqrt{2}.$$

Example 5: Let $x_1, x_2, \dots, x_{2014}$ be positive real numbers such that $\sum_{j=1}^{2014} x_j = 1$. Determine with proof the smallest constant K such that

$$K \sum_{j=1}^{2014} \frac{x_j^2}{1-x_j} \geq 1.$$

Solution: Let us take the general case: $\{x_1, x_2, \dots, x_n\}$ are positive real numbers such that $\sum_{k=1}^{n} x_k = 1$. Then

$$\sum_{k=1}^{n} \frac{x_k^2}{1-x_k} = \sum_{k=1}^{n} \frac{x_k^2-1}{1-x_k} + \sum_{k=1}^{n} \frac{1}{1-x_k} = \sum_{k=1}^{n} \frac{-(1-x_k)}{1-x_k} + \sum_{k=1}^{n} \frac{1}{1-x_k}.$$

Now the first sum is $-n-1$. We can estimate the second sum using AM-HM inequality:

$$\sum_{k=1}^{n} \frac{1}{1-x_k} \geq \frac{n^2}{\sum_{k=1}^{n}(1-x_k)} = \frac{n^2}{n-1}.$$

Thus we obtain

$$\sum_{k=1}^{n} \frac{x_k^2}{1-x_k} \geq -(1+n) + \frac{n^2}{n-1} = \frac{1}{n-1}.$$

Here equality holds if and only if all x_j's are equal. Thus we get the smallest constant K such that

$$K \sum_{j=1}^{2014} \frac{x_j^2}{1-x_j} \geq 1$$

to be $2014 - 1 = 2013$.

Example 6: Let x, y, z be positive real numbers. Prove that

$$\frac{y^2+z^2}{x} + \frac{z^2+x^2}{y} + \frac{x^2+y^2}{z} \geq 2(x+y+z).$$

Solution: We write the inequality in the form

$$\frac{x^2}{y} + \frac{y^2}{x} + \frac{y^2}{z} + \frac{z^2}{y} + \frac{z^2}{x} + \frac{x^2}{z} \geq 2(x+y+z).$$

We observe that $x^2 + y^2 \geq 2xy$. Hence $x^2 + y^2 - xy \geq xy$. Multiplying both sides by $(x+y)$, we get

$$x^3 + y^3 = (x+y)(x^2 - xy + y^2) \geq (x+y)xy.$$

Thus

$$\frac{x^2}{y} + \frac{y^2}{x} \geq x + y.$$

Similarly, we obtain

$$\frac{y^2}{z} + \frac{z^2}{y} \geq y + z, \quad \frac{z^2}{x} + \frac{x^2}{z} \geq x + y.$$

Adding three inequalities, we get the required result.

Example 7: Find all real numbers x and y such that

$$x^2 + 2y^2 + \frac{1}{2} \leq x(2y+1).$$

Solution: We write the inequality in the form

$$2x^2 + 4y^2 + 1 - 4xy - 2x \leq 0.$$

Thus $(x^2 - 4xy + 4y^2) + (x^2 - 2x + 1) \leq 0$. Hence

$$(x - 2y)^2 + (x - 1)^2 \leq 0.$$

Since x, y are real, we know that $(x - 2y)^2 \geq 0$ and $(x - 1)^2 \geq 0$. Hence it follows that $(x - 2y)^2 = 0$ and $(x - 1)^2 = 0$. Therefore $x = 1$ and $y = 1/2$.

Example 8: If x and y are positive real numbers, prove that

$$4x^4 + 4y^3 + 5x^2 + y + 1 \geq 12xy.$$

Solution: We have from AM-GM inequality,

$$4x^4 + 1 \geq 4x^2, \quad 4y^3 + y = y(4y^2 + 1) \geq 4y^2.$$

Hence

$$4x^4 + 4y^3 + 5x^2 + y + 1 \geq 4x^2 + 4y^2 + 5x^2 = 9x^2 + 4y^2 \geq 2(\sqrt{9 \times 4})xy = 12xy.$$

---

1. Let a, b, c be positive numbers such that

$$\frac{1}{1+a} + \frac{1}{1+b} + \frac{1}{1+c} \leq 1.$$

Prove that $(1+a^2)(1+b^2)(1+c^2) \geq 125$. When does the equality hold?

2. Let a and b be positive real numbers such that $a + b = 1$. Prove that

$$a^a b^b + a^b b^a \leq 1.$$

3. If a, b, c are three positive real numbers, prove that

$$\frac{a^2+1}{b+c} + \frac{b^2+1}{c+a} + \frac{c^2+1}{a+b} \geq 3.$$

4. Prove that:

(a) $5 < \sqrt{5} + \sqrt[3]{5} + \sqrt[4]{5}$;

(b) $8 > \sqrt{8} + \sqrt[3]{8} + \sqrt[4]{8}$;

(c) $n > \sqrt{n} + \sqrt[3]{n} + \sqrt[4]{n}$ for all integers $n \geq 9$.

5. Let a, b, c be three positive real numbers such that $a + b + c = 1$. Let

$$\lambda = \min\{a^3 + a^2bc, b^3 + ab^2c, c^3 + abc^2\}.$$

Prove that the roots of the equation $x^2 + x + 4\lambda = 0$ are real.

6. Let x and y be positive real numbers such that $y^3 + y \leq x - x^3$. Prove that

(a) $y < x < 1$; and

(b) $x^2 + y^2 < 1$.

7. Let $n \geq 3$ be an integer and let $1 < a_1 \leq a_2 \leq a_3 \leq \cdots \leq a_n$ be n real numbers such that $a_1 + a_2 + a_3 + \cdots + a_n = 2n$. Prove that

$$a_1a_2 \cdots a_{n-1} + a_1a_2 \cdots a_{n-2} + \cdots + a_1a_2 + a_1 + 2 \leq a_1a_2 \cdots a_n.$$

8. Let a, b, c be positive real numbers such that $a^3 + b^3 = c^3$. Prove that

$$a^2 + b^2 - c^2 > 6(c-a)(c-b).$$

9. If x, y, z are positive real numbers, prove that

$$(x+y+z)^2(yz+zx+xy)^2 \leq 3(y^2+yz+z^2)(z^2+zx+x^2)(x^2+xy+y^2).$$

10. Let x, y be positive reals such that $x + y = 2$. Prove that

$$x^3y^3(x^3+y^3) \leq 2.$$

10.9 Inequalities MCQ

1. Given a and b are positive numbers and c and d are real numbers, positive or negative, then $a^c \leq b^d$:

(A) if $a \leq b$ and $c \leq d$;

(B) if either $a \leq b$ or $c \leq d$;

(C) if $a \geq 1$, $b \geq 1$, $d \geq c$;

(D) is not implied by any of the foregoing conditions.

2. For all x such that $1 \leq x \leq 3$, the inequality $(x - 3a)(x - a - 3) < 0$ holds for:

(A) no value of a;

(B) all a satisfying $\frac{2}{3} < a < 1$;

(C) all a satisfying $0 < a < \frac{1}{3}$;

(D) all a satisfying $\frac{1}{3} < a < \frac{2}{3}$.

3. Given that x is a real number satisfying:

$$(3x^2 - 10x + 3)(2x^2 - 5x + 2) < 0,$$

it follows that:

(A) $x < \frac{1}{3}$;

(B) $\frac{1}{3} < x < \frac{1}{2}$;

(C) $2 < x < 3$;

(D) $\frac{1}{3} < x < \frac{1}{2}$ or $2 < x < 3$.

4. If x, y, z are arbitrary real numbers satisfying the condition $xy + yz + zx < 0$, and if

$$u = \frac{x^2 + y^2 + z^2}{xy + yz + zx},$$

then only one of the following statements is always correct. Which one is it?

(A) $-1 \leq u < 0$;

(B) u takes all negative real values;

(C) $-2 < u \leq -1$;

(D) $u \leq -2$.

5. The inequality

$$\frac{|x|^2 - |x| - 2}{2|x| - |x|^2 - 2} > 2$$

holds if and only if:

(A) $1 < x < -\frac{2}{3}$ or $\frac{2}{3} < x < 1$;

(B) $1 < x < 1$;

(C) $\frac{2}{3} < x < 1$;

(D) $x > 1$ or $x < -1$ or $-\frac{2}{3} < x < \frac{2}{3}$.

6. The set of all real numbers x satisfying the inequality $|x^2 + 3x| + x^2 - 2 \geq 0$ is:

(A) all the real numbers x with either $x \leq -3$ or $x \geq 2$;

(B) all the real numbers x with either $x \leq -\frac{3}{2}$ or $x \geq \frac{1}{2}$;

(C) all the real numbers x with either $x \leq -2$ or $x \geq \frac{1}{2}$;

(D) described by none of the foregoing statements.

7. The least value of $\frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ for positive x, y, z satisfying the condition $x + y + z = 9$ is:

(A) $\frac{15}{7}$;

(B) $\frac{1}{9}$;

(C) 3;

(D) 1.

8. The smallest value of α satisfying the conditions that α is a positive integer and that $\frac{\alpha}{540}$ is the square of a rational number is:

(A) 15;

(B) 5;

(C) 6;

(D) 3.

9. The set of all values of x satisfying the inequality $\frac{6x^2+5x+3}{x^2+2x+3} > 2$ is:

(A) $x > \frac{3}{4}$;

(B) $|x| > 1$;

(C) either $x > \frac{3}{4}$ or $x < -1$;

(D) $|x| > \frac{3}{4}$.

10. The set of all x satisfying $|x^2 - 4| \leq 4x$ is:

(A) $x < 2(\sqrt{2} - 1)$ or $x > 2(\sqrt{2} + 1)$;

(B) $x > 2(\sqrt{2} + 1)$;

(C) $x < -2(\sqrt{2} - 1)$ or $x > 2(\sqrt{2} + 1)$;

(D) none of the foregoing sets.

11. If a, b, c are positive real numbers and

$$\alpha = \frac{b^2 + c^2}{b + c} + \frac{c^2 + a^2}{c + a} + \frac{a^2 + b^2}{a + b},$$

then only one of the following statements is always true. Which one is it?

(A) $0 \leq \alpha < a$;

(B) $a \leq \alpha < a + b$;

(C) $a + b \leq \alpha < a + b + c$;

(D) $a + b + c \leq \alpha < 2(a + b + c)$.

12. Suppose a, b, c are real numbers such that $a^2b^2 + b^2c^2 + c^2a^2 = k$, where k is a constant. Then the set of all possible values of $abc(a + b + c)$ is precisely the interval:

(A) $[-k, k]$

(B) $\left[-\frac{k}{2}, \frac{k}{2}\right]$

(C) $\left[-\frac{k}{2}, k\right]$

(D) $\left[-k, \frac{k}{2}\right]$

13. If a, b, c, d are real numbers such that $b > 0$, $d > 0$ and $\frac{a}{b} < \frac{c}{d}$, then only one of the following statements is always true. Which one is it?

(A) $\frac{a}{b} < \frac{a-c}{b-d} < \frac{c}{d}$;

(B) $\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$;

(C) $\frac{a}{b} < \frac{a-c}{b+d} < \frac{c}{d}$;

(D) $\frac{a}{b} < \frac{a+c}{b-d} < \frac{c}{d}$.

14. If x, y, z are arbitrary positive real numbers satisfying the equation

$$4xy + 6yz + 8zx = 9,$$

then the maximum possible value of the product xyz is:

(A) $\frac{1}{2\sqrt{2}}$;

(B) $\frac{\sqrt{3}}{4}$;

(C) $\frac{3}{8}$;

(D) none of the foregoing values.

15. Let P and Q be the subsets of the X-Y plane defined as:

$$P = \{(x, y) : x > 0, y > 0 \text{ and } x^2 + y^2 = 1\},$$

and

$$Q = \{(x, y) : x > 0, y > 0 \text{ and } x^8 + y^8 < 1\}.$$

Then, $P \cap Q$ is

(A) the empty set $\emptyset$;

(B) P;

(C) Q;

(D) none of the foregoing sets.

16. The minimum value of the quantity

$$\frac{(a^2 + 3a + 1)(b^2 + 3b + 1)(c^2 + 3c + 1)}{abc},$$

where a, b and c are positive real numbers, is

(A) $\frac{11^3}{2^3}$;

(B) 125;

(C) 25;

(D) 27.

17. The smallest integer greater than the real number $(\sqrt{5}+\sqrt{3})^{2n}$ (for nonnegative integer n) is

(A) 8^n;

(B) 4^{2n};

(C) $(\sqrt{5}+\sqrt{3})^{2n}+(\sqrt{5}-\sqrt{3})^{2n}-1$;

(D) $(\sqrt{5}+\sqrt{3})^{2n}+(\sqrt{5}-\sqrt{3})^{2n}$.

18. The set of all values of m for which $mx^2-6mx+5m+1>0$ for all real x is

(A) $0 \le m \le \frac{1}{4}$;

(B) $m < \frac{1}{4}$;

(C) $m \ge 0$;

(D) $0 \le m < \frac{1}{4}$.

ANSWER KEY

1	2	3	4	5	6	7	8	9
D	C	D	D	A	B	D	A	C
10	11	12	13	14	15	16	17	18
A	D	C	B	C	B	B	D	D

11 Complex Numbers

11.1 Algebraic Representation of Complex Numbers

In what follows we assume that the definition and basic properties of the set of real numbers $\mathbb{R}$ are known.

Let us consider the set $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$. Two elements (x_1, y_1) and (x_2, y_2) of $\mathbb{R}^2$ are equal if and only if $x_1 = x_2$ and $y_1 = y_2$. The operations of addition and multiplication are defined on the set $\mathbb{R}^2$ as follows:

$$z_1 + z_2 = (x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2) \in \mathbb{R}^2$$

and

$$z_1 \cdot z_2 = (x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1) \in \mathbb{R}^2,$$

for all $z_1 = (x_1, y_1) \in \mathbb{R}^2$ and $z_2 = (x_2, y_2) \in \mathbb{R}^2$.

The element $z_1 + z_2 \in \mathbb{R}^2$ is called the *sum* of z_1 and z_2 and the element $z_1 \cdot z_2 \in \mathbb{R}^2$ is called the *product* of z_1 and z_2.

Definition. The set $\mathbb{R}^2$, together with the addition and multiplication operations, is called the *set of complex numbers*, denoted by $\mathbb{C}$. Any element $z = (x, y) \in \mathbb{C}$ is called a *complex number.*

The notation $\mathbb{C}^*$ is used to indicate the set $\mathbb{C} \setminus \{(0, 0)\}$.

Properties concerning addition

The addition of complex numbers satisfies the following properties:

(a) **Commutative law**

$$z_1 + z_2 = z_2 + z_1 \text{ for all } z_1, z_2 \in \mathbb{C}.$$

(b) **Associative law**

$$(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3) \text{ for all } z_1, z_2, z_3 \in \mathbb{C}.$$

Indeed, if $z_1 = (x_1, y_1) \in \mathbb{C}$, $z_2 = (x_2, y_2) \in \mathbb{C}$, $z_3 = (x_3, y_3) \in \mathbb{C}$, then

$$(z_1 + z_2) + z_3 = [(x_1, y_1) + (x_2, y_2)] + (x_3, y_3)$$

$$= (x_1 + x_2, y_1 + y_2) + (x_3, y_3) = ((x_1 + x_2) + x_3, (y_1 + y_2) + y_3),$$

and

$$z_1 + (z_2 + z_3) = (x_1, y_1) + [(x_2, y_2) + (x_3, y_3)]$$

$$= (x_1, y_1) + (x_2 + x_3, y_2 + y_3) = (x_1 + (x_2 + x_3), y_1 + (y_2 + y_3)).$$

The claim holds due to the associativity of the addition of real numbers.

(c) **Additive identity** There is a unique complex number $0 = (0, 0)$ such that

$$z + 0 = 0 + z = z \text{ for all } z = (x, y) \in \mathbb{C}.$$

(d) **Additive inverse** For any complex number $z = (x, y)$ there is a unique $-z = (-x, -y) \in \mathbb{C}$ such that

$$z + (-z) = (-z) + z = 0.$$

Properties concerning multiplication

The multiplication of complex numbers satisfies the following properties:

(a) **Commutative law**

$$z_1 \cdot z_2 = z_2 \cdot z_1 \text{ for all } z_1, z_2 \in \mathbb{C}.$$

(b) **Associative law**

$$(z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 \cdot z_3) \text{ for all } z_1, z_2, z_3 \in \mathbb{C}.$$

(c) **Multiplicative identity** There is a unique complex number $1 = (1, 0) \in \mathbb{C}$ such that

$$z \cdot 1 = 1 \cdot z = z \text{ for all } z \in \mathbb{C}.$$

A simple algebraic manipulation is all that is needed to verify these equalities:

$$z \cdot 1 = (x, y) \cdot (1, 0) = (x \cdot 1 - y \cdot 0, x \cdot 0 + y \cdot 1) = (x, y) = z$$

and

$$1 \cdot z = (1, 0) \cdot (x, y) = (1 \cdot x - 0 \cdot y, 1 \cdot y + 0 \cdot x) = (x, y) = z.$$

(d) **Multiplicative inverse** For any complex number $z = (x, y) \in \mathbb{C}^*$ there is a unique number $z^{-1} = (x', y') \in \mathbb{C}$ such that

$$z \cdot z^{-1} = z^{-1} \cdot z = 1.$$

To find $z^{-1} = (x', y')$, observe that $(x, y) \neq (0, 0)$ implies $x \neq 0$ or $y \neq 0$ and consequently $x^2 + y^2 \neq 0$. The relation $z \cdot z^{-1} = 1$ gives $(x, y) \cdot (x', y') = (1, 0)$, or equivalently

$$\begin{cases} xx' - yy' = 1 \\ yx' + xy' = 0 \end{cases}$$

Solving this system with respect to x' and y', one obtains

$$x' = \frac{x}{x^2 + y^2} \quad \text{and} \quad y' = \frac{-y}{x^2 + y^2},$$

hence the multiplicative inverse of the complex number $z = (x, y) \in \mathbb{C}^*$ is

$$z^{-1} = \frac{1}{z} = \left(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2} \right) \in \mathbb{C}^*.$$

By the commutative law we also have $z^{-1} \cdot z = 1$.

Two complex numbers $z_1 = (x_1, y_1) \in \mathbb{C}$ and $z = (x, y) \in \mathbb{C}^*$ uniquely determine a third number called their *quotient*, denoted by $\frac{z_1}{z}$ and defined by

$$\frac{z_1}{z} = z_1 \cdot z^{-1} = (x_1, y_1) \cdot \left(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2} \right) = \left(\frac{x_1 x + y_1 y}{x^2 + y^2}, \frac{-x_1 y + y_1 x}{x^2 + y^2} \right) \in \mathbb{C}.$$

11.1.1 Complex numbers in algebraic form

For algebraic manipulation it is not convenient to represent a complex number as an ordered pair. For this reason another form of writing is preferred.

To introduce this new algebraic representation, consider the set $\mathbb{R} \times \{0\}$, together with the addition and multiplication operations defined on $\mathbb{R}^2$. The function

$$f : \mathbb{R} \to \mathbb{R} \times \{0\}, \quad f(x) = (x, 0)$$

is bijective and moreover,

$$(x, 0) + (y, 0) = (x + y, 0) \quad \text{and} \quad (x, 0) \cdot (y, 0) = (xy, 0).$$

The reader will not fail to notice that the algebraic operations on $\mathbb{R} \times \{0\}$ are similar to the operations on $\mathbb{R}$; therefore we can identify the ordered pair $(x, 0)$ with the number x for all $x \in \mathbb{R}$. Hence we can use, by the above bijection f, the notation $(x, 0) = x$.

Setting $i = (0, 1)$ we obtain

$$z = (x, y) = (x, 0) + (0, y) = (x, 0) + (y, 0) \cdot (0, 1) = x + yi = (x, 0) + (0, 1) \cdot (y, 0).$$

In this way we obtain

Proposition. Any complex number $z = (x, y)$ can be uniquely represented in the form

$$z = x + yi,$$

where x, y are real numbers. The relation $i^2 = -1$ holds.

The formula $i^2 = -1$ follows directly from the definition of multiplication: $i^2 = i \cdot i = (0, 1) \cdot (0, 1) = (-1, 0) = -1$.

The expression $x + yi$ is called the *algebraic representation (form)* of the complex number $z = (x, y)$, so we can write $\mathbb{C} = \{x + yi \mid x \in \mathbb{R}, y \in \mathbb{R}, i^2 = -1\}$. From now on we will denote the complex number $z = (x, y)$ by $x + iy$. The real number $x = \operatorname{Re}(z)$ is called the *real part* of the complex number z and similarly, $y = \operatorname{Im}(z)$ is called the *imaginary part* of z. Complex numbers of the form $iy, y \in \mathbb{R}$—in other words, complex numbers whose real part is 0—are called *imaginary.* On the other hand, complex numbers of the form $iy, y \in \mathbb{R}^*$ are called *purely imaginary* and the number y is called the *imaginary unit.*

Powers of the number i

The formulas for the powers of a complex number with integer exponents are preserved for the algebraic form $z = x + iy$. Setting $z = i$, we obtain

$$\begin{aligned} &i^0 = 1; \quad i^1 = i; \quad i^2 = -1; \quad i^3 = i^2 \cdot i = -i; \\ &i^4 = i^3 \cdot i = 1; \quad i^5 = i^4 \cdot i = i; \quad i^6 = i^5 \cdot i = -1; \quad i^7 = i^6 \cdot i = -i. \end{aligned}$$

One can prove by induction that for any positive integer n,

$$i^{4n} = 1; \quad i^{4n+1} = i; \quad i^{4n+2} = -1; \quad i^{4n+3} = -i.$$

Hence $i^n \in \{-1, 1, -i, i\}$ for all integers $n \geq 0$. If n is a negative integer, we have

$$i^n = (i^{-1})^{-n} = \left(\frac{1}{i}\right)^{-n} = (-i)^{-n}.$$

Example 1: We have

$$i^{105} + i^{23} + i^{20} - i^{34} = i^{4 \cdot 26+1} + i^{4 \cdot 5+3} + i^{4 \cdot 5} - i^{4 \cdot 8+2} = i - i + 1 + 1 = 2.$$

Example 2: Let us solve the equation $z^3 = 18 + 26i$, where $z = x + yi$ and x, y are integers. We can write

$$\begin{aligned} (x + yi)^3 &= (x + yi)^2(x + yi) = (x^2 - y^2 + 2xyi)(x + yi) \\ &= (x^3 - 3xy^2) + (3x^2y - y^3)i = 18 + 26i. \end{aligned}$$

Using the definition of equality of complex numbers, we obtain

$$\begin{cases} x^3 - 3xy^2 = 18 \\ 3x^2y - y^3 = 26 \end{cases}$$

Setting $y = tx$ in the equality $18(3x^2y - y^3) = 26(x^3 - 3xy^2)$, let us observe that $x \neq 0$ and $y \neq 0$ implies $18(3t - t^3) = 26(1 - 3t^2)$. The last relation is equivalent to $(3t - 1)(3t^2 - 12t - 13) = 0$.

The only rational solution of this equation is $t = \frac{1}{3}$; hence,

$$x = 3, \quad y = 1 \quad \text{and} \quad z = 3 + i.$$

Conjugate of a complex number: For a complex number $z = x + yi$ the number $\overline{z} = x - yi$ is called the *complex conjugate* or the *conjugate complex* of z.

Proposition.

1) The relation $z = \overline{z}$ holds if and only if $z \in \mathbb{R}$.

2) For any complex number z the relation $\overline{\overline{z}} = z$ holds.

3) For any complex number z the number $z \cdot \overline{z} \in \mathbb{R}$ is a nonnegative real number.

4) $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ (the conjugate of a sum is the sum of the conjugates).

5) $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$ (the conjugate of a product is the product of the conjugates).

6) For any nonzero complex number z the relation $\overline{z^{-1}} = (\overline{z})^{-1}$ holds.

7) $\overline{\left(\frac{z_1}{z_2}\right)} = \frac{\overline{z_1}}{\overline{z_2}}, z_2 \neq 0$ (the conjugate of a quotient is the quotient of the conjugates).

8) The formulas

$$\mathrm{Re}(z) = \frac{z + \overline{z}}{2} \quad \text{and} \quad \mathrm{Im}(z) = \frac{z - \overline{z}}{2i}$$

are valid for all $z \in \mathbb{C}$.

Modulus of a complex number The number $|z| = \sqrt{x^2 + y^2}$ is called the *modulus* or the *absolute value* of the complex number $z = x + yi$. For example, the complex numbers

$$z_1 = 4 + 3i, \quad z_2 = -3i, \quad z_3 = 2$$

have the moduli

$$|z_1| = \sqrt{4^2 + 3^2} = 5, \quad |z_2| = \sqrt{0^2 + (-3)^2} = 3, \quad |z_3| = \sqrt{2^2} = 2.$$

Proposition. The following properties are satisfied:

1) $-|z| \leq \mathrm{Re}(z) \leq |z|$ and $-|z| \leq \mathrm{Im}(z) \leq |z|$.

2) $|z| \geq 0$ for all $z \in \mathbb{C}$. Moreover, we have $|z| = 0$ if and only if $z = 0$.

3) $|z| = |-z| = |\overline{z}|$.

4) $z \cdot \overline{z} = |z|^2$.

5) $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$

6) $|z_1| - |z_2| \leq |z_1 + z_2| \leq |z_1| + |z_2|$.

7) $|z^{-1}| = |z|^{-1}$, $z \neq 0$.

8) $\left|\frac{z_1}{z_2}\right| = \frac{|z_1|}{|z_2|}$, $z_2 \neq 0$

9) $|z_1| - |z_2| \leq |z_1 - z_2| \leq |z_1| + |z_2|$.

Example 3: Prove the identity

$$|z_1 + z_2|^2 + |z_1 - z_2|^2 = 2(|z_1|^2 + |z_2|^2)$$

for all complex numbers z_1, z_2.

Solution. Using property 4 in the proposition above, we obtain

$$\begin{aligned}|z_1+z_2|^2+|z_1-z_2|^2 &= (z_1+z_2)(\overline{z_1+z_2})+(z_1-z_2)(\overline{z_1-z_2})\\ &= |z_1|^2+z_1\cdot\overline{z_2}+z_2\cdot\overline{z_1}+|z_2|^2+|z_1|^2-z_1\cdot\overline{z_2}-z_2\cdot\overline{z_1}+|z_2|^2\\ &= 2(|z_1|^2+|z_2|^2).\end{aligned}$$

Example 4: Prove that if $|z_1|=|z_2|=1$ and $z_1z_2\neq -1$, then $\frac{z_1+z_2}{1+z_1z_2}$ is a real number.

Solution. Using again property 4 in the above proposition, we have

$$z_1\cdot\overline{z_1}=|z_1|^2=1 \quad\text{and}\quad \overline{z_1}=\frac{1}{z_1}.$$

Likewise, $\overline{z_2}=\frac{1}{z_2}$. Hence denoting by A the number in the problem we have

$$\overline{A}=\frac{\overline{z_1}+\overline{z_2}}{1+\overline{z_1}\cdot\overline{z_2}}=\frac{\frac{1}{z_1}+\frac{1}{z_2}}{1+\frac{1}{z_1}\cdot\frac{1}{z_2}}=\frac{\frac{z_1+z_2}{z_1z_2}}{\frac{z_1z_2+1}{z_1z_2}}=\frac{z_1+z_2}{1+z_1z_2}=A,$$

so A is a real number.

Example 5: Solve, in complex numbers, the quadratic equation

$$z^2-8(1-i)z+63-16i=0.$$

Solution. We have

$$\Delta'=(4-4i)^2-(63-16i)=-63-16i$$

and

$$r=|\Delta'|=\sqrt{63^2+16^2}=65,$$

where $\Delta'=\left(\frac{b}{2}\right)^2-ac$.

The equation

$$y^2=-63-16i$$

has the solution $y_{1,2}=\pm\left(\sqrt{\frac{65-63}{2}}+i\sqrt{\frac{65+63}{2}}\right)=\pm(1-8i)$. It follows that

$$z_{1,2}=4-4i\pm(1-8i).$$

Hence

$$z_1=5-12i \quad\text{and}\quad z_2=3+4i.$$

Example 6: Let p and q be complex numbers with $q\neq 0$. Prove that if the roots of the quadratic equation $x^2+px+q^2=0$ have the same absolute value, then $\frac{p}{q}$ is a real number.

Solution. Let x_1 and x_2 be the roots of the equation and let $r=|x_1|=|x_2|$. Then

$$\frac{p^2}{q^2}=\frac{(x_1+x_2)^2}{x_1x_2}=\frac{x_1}{x_2}+\frac{x_2}{x_1}+2=\frac{x_1\overline{x_2}}{r^2}+\frac{x_2\overline{x_1}}{r^2}+2=2+\frac{2}{r^2}\mathrm{Re}(x_1\overline{x_2})$$

is a real number. Moreover,

$$\mathrm{Re}(x_1\overline{x_2})\geq -|x_1\overline{x_2}|=-r^2, \quad\text{so}\quad \frac{p^2}{q^2}\geq 0.$$

Therefore $\frac{p}{q}$ is a real number, as claimed.

11.2 Exercise 3.1

1. Find all complex numbers z such that
$$4z^2 + 8|z|^2 = 8.$$

2. Find all complex numbers z such that $z^3 = \overline{z}$.

3. Consider $z \in \mathbb{C}$ with $\mathrm{Re}(z) > 1$. Prove that
$$\left|\frac{1}{z} - \frac{1}{2}\right| < \frac{1}{2}.$$

4. Find all complex numbers z such that
$$z' = (z-2)(\overline{z} + i)$$
is a real number.

5. Find all complex numbers z such that $|z| = \left|\frac{1}{z}\right|$.

6. Let $z_1, z_2 \in \mathbb{C}$ be complex numbers such that $|z_1 + z_2| = \sqrt{3}$ and $|z_1| = |z_2| = 1$. Compute $|z_1 - z_2|$.

7. Let $n > 2$ be an integer. Find the number of solutions to the equation
$$z^{n-1} = i\overline{z}.$$

8. Let z_1, z_2, z_3 be complex numbers with
$$|z_1| = |z_2| = |z_3| = R > 0.$$
Prove that
$$|z_1 - z_2| \cdot |z_2 - z_3| + |z_3 - z_1| \cdot |z_1 - z_2| + |z_2 - z_3| \cdot |z_3 - z_1| \leq 9R^2.$$

9. Let u, v, w, z be complex numbers such that $|u| < 1$, $|v| = 1$ and
$$w = \frac{v(u-z)}{\overline{u} \cdot z - 1}.$$
Prove that $|w| \leq 1$ if and only if $|z| \leq 1$.

10. Let z_1, z_2, z_3 be complex numbers such that
$$z_1 + z_2 + z_3 = 0 \quad \text{and} \quad |z_1| = |z_2| = |z_3| = 1.$$
Prove that
$$z_1^2 + z_2^2 + z_3^2 = 0.$$

11. Consider the complex numbers $z_1, z_2, \ldots, z_n$ with
$$|z_1| = |z_2| = \cdots = |z_n| = r > 0.$$
Prove that the number
$$E = \frac{(z_1 + z_2)(z_2 + z_3)\cdots(z_{n-1} + z_n)(z_n + z_1)}{z_1 \cdot z_2 \cdot \cdots \cdot z_n}$$
is real.

12. Let a, b, c be distinct nonzero complex numbers with $|a| = |b| = |c|$.

(a) Prove that if a root of the equation $az^2 + bz + c = 0$ has modulus equal to 1, then $b^2 = ac$.

(b) If each of the equations
$$az^2 + bz + c = 0 \quad \text{and} \quad bz^2 + cz + a = 0$$
has a root having modulus 1, then $|a - b| = |b - c| = |c - a|$.

11.3 Complex Numbers in Trigonometric Form

Let us consider a point $P(x, y)$ on the plane, one that is not the origin. Then the number

$$r = \sqrt{x^2 + y^2}$$

is called the polar radius of the point P and the directed angle $\phi \in [0, 2\pi)$ between the positive x-sxis and the vector $\overrightarrow{OP}$ is called the polar argument of the point P. Thus we can denote any point in $\mathbb{R}^2$ uniquely as $P(r, \phi)$

Observe that we look at the point $P(x, y)$ in its complex form we have $P = x + iy$ and plotting it we can conclude that

$$x = r\cos\phi \text{ and } y = r\sin\phi$$

Example 1: Find the polar representation of the complex number

$$z = 1 + \cos a + i\sin a, \quad a \in (0, 2\pi).$$

Solution. The modulus is

$$|z| = \sqrt{(1+\cos a)^2 + \sin^2 a} = \sqrt{2(1+\cos a)} = \sqrt{4\cos^2\frac{a}{2}} = 2\left|\cos\frac{a}{2}\right|.$$

The argument of z is determined as follows:

(a) If $a \in (0, \pi)$, then $\frac{a}{2} \in \left(0, \frac{\pi}{2}\right)$ and the point $P(1 + \cos a, \sin a)$ lies on the first quadrant. Hence

$$t^* = \arctan\frac{\sin a}{1+\cos a} = \arctan\left(\tan\frac{a}{2}\right) = \frac{a}{2},$$

and in this case

$$z = 2\cos\frac{a}{2}\left(\cos\frac{a}{2} + i\sin\frac{a}{2}\right).$$

(b) If $a \in (\pi, 2\pi)$, then $\frac{a}{2} \in \left(\frac{\pi}{2}, \pi\right)$ and the point $P(1 + \cos a, \sin a)$ lies on the fourth quadrant. Hence

$$t^* = \arctan\left(\tan\frac{a}{2}\right) + 2\pi = \frac{a}{2} - \pi + 2\pi = \frac{a}{2} + \pi$$

and

$$z = -2\cos\frac{a}{2}\left(\cos\left(\frac{a}{2}+\pi\right) + i\sin\left(\frac{a}{2}+\pi\right)\right).$$

(c) If $a = \pi$, then $z = 0$.

Example 2: Find all complex numbers z such that $|z| = 1$ and

$$\left|\frac{z}{\overline{z}} + \frac{\overline{z}}{z}\right| = 1.$$

Solution. Let $z = \cos x + i \sin x$, $x \in [0, 2\pi)$. Then

$$1 = \left|\frac{z}{\overline{z}} + \frac{\overline{z}}{z}\right| = \left|\frac{z^2 + \overline{z}^2}{|z|^2}\right| = |\cos 2x + i \sin 2x + \cos 2x - i \sin 2x| = 2|\cos 2x|.$$

Hence

$$\cos 2x = \frac{1}{2} \quad \text{or} \quad \cos 2x = -\frac{1}{2}.$$

If $\cos 2x = \frac{1}{2}$, then

$$x_1 = \frac{\pi}{6}, \quad x_2 = \frac{5\pi}{6}, \quad x_3 = \frac{7\pi}{6}, \quad x_4 = \frac{11\pi}{6}.$$

If $\cos 2x = -\frac{1}{2}$, then

$$x_5 = \frac{\pi}{3}, \quad x_6 = \frac{2\pi}{3}, \quad x_7 = \frac{4\pi}{3}, \quad x_8 = \frac{5\pi}{3}.$$

Hence there are eight solutions

$$z_k = \cos x_k + i \sin x_k, \quad k = 1, 2, \ldots, 8.$$

Proposition: Observe that multiplication becomes easier when we consider the polar form of complex numbers. The following holds

$$z_1 = r_1(\cos t_1 + i \sin t_1) \quad \text{and} \quad z_2 = r_2(\cos t_2 + i \sin t_2).$$

then we have

$$z_1 z_2 = r_1 r_2(\cos(t_1 + t_2) + i \sin(t_1 + t_2))$$

Proof. Indeed,

$$\begin{aligned}
z_1 z_2 &= r_1 r_2(\cos t_1 + i \sin t_1)(\cos t_2 + i \sin t_2) \\
&= r_1 r_2((\cos t_1 \cos t_2 - \sin t_1 \sin t_2) + i(\sin t_1 \cos t_2 + \sin t_2 \cos t_1)) \\
&= r_1 r_2(\cos(t_1 + t_2) + i \sin(t_1 + t_2)).
\end{aligned}$$

We can extend this to multiplication of n complex numbers. If we have

$$x_k = r_k(\cos \alpha_k + \sin \alpha_k) \quad 1 \leq k \leq n$$

$$\prod_{k=1}^{n} z_k = \prod_{k=1}^{n} r_k \left(\cos \sum_{k=1}^{n} \alpha_k + i \sin \sum_{k=1}^{n} \cos \alpha_k \right)$$

Example 3: Let $z_1 = 1 - i$ and $z_2 = \sqrt{3} + i$. Then

$$z_1 = \sqrt{2}\left(\cos \frac{7\pi}{4} + i \sin \frac{7\pi}{4}\right), \quad z_2 = 2\left(\cos \frac{\pi}{6} + i \sin \frac{\pi}{6}\right)$$

and

$$\begin{aligned}
z_1 z_2 &= 2\sqrt{2}\left[\cos\left(\frac{7\pi}{4} + \frac{\pi}{6}\right) + i \sin\left(\frac{7\pi}{4} + \frac{\pi}{6}\right)\right] \\
&= 2\sqrt{2}\left(\cos \frac{23\pi}{12} + i \sin \frac{23\pi}{12}\right).
\end{aligned}$$

Proposition: Finding powers of a complex Number also becomes easier using the polar form of a complex number. We have for $z = r(\cos t + i \sin t)$ and $n \in \mathbb{N}$, we have

$$z^n = r^n(\cos nt + i \sin nt).$$

Proof. Apply the multiplication formula for $z = z_1 = z_2 = \cdots = z_n$ we obtain

$$\begin{aligned} z^n &= \underbrace{r \cdot r \cdots r}_{n \text{ times}}(\cos \underbrace{(t + t + \cdots + t)}_{n \text{ times}} + i \sin \underbrace{(t + t + \cdots + t)}_{n \text{ times}}) \\ &= r^n(\cos nt + i \sin nt). \end{aligned}$$

Example 4: Prove that

$$\sin 5t = 16 \sin^5 t - 20 \sin^3 t + 5 \sin t;$$

$$\cos 5t = 16 \cos^5 t - 20 \cos^3 t + 5 \cos t.$$

Example 4: Compute

$$z = \frac{(1-i)^{10}(\sqrt{3}+i)^5}{(-1-i\sqrt{3})^{10}}.$$

Solution. We can write

$$\begin{aligned} z &= \frac{(\sqrt{2})^{10}\left(\cos\frac{7\pi}{4} + i\sin\frac{7\pi}{4}\right)^{10} \cdot 2^5\left(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}\right)^5}{2^{10}\left(\cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}\right)^{10}} \\ &= \frac{2^{10}\left(\cos\frac{35\pi}{2} + i\sin\frac{35\pi}{2}\right)\left(\cos\frac{5\pi}{6} + i\sin\frac{5\pi}{6}\right)}{2^{10}\left(\cos\frac{40\pi}{3} + i\sin\frac{40\pi}{3}\right)} \\ &= \frac{\cos\frac{55\pi}{3} + i\sin\frac{55\pi}{3}}{\cos\frac{40\pi}{3} + i\sin\frac{40\pi}{3}} \\ &= \cos 5\pi + i\sin 5\pi \\ &= -1. \end{aligned}$$

11.4 nth roots of unity

Consider a positive integer $n \geq 2$ and a complex number $z_0 \neq 0$. As in the field of real numbers, the equation

$$Z^n - z_0 = 0 \tag{1}$$

is used for defining the n-th roots of number z_0. Hence we call any solution Z of the equation (1) an n-th root of the complex number z_0.

Theorem. *Let $z_0 = r(\cos t^* + i \sin t^*)$ be a complex number with $r > 0$ and $t^* \in [0, 2\pi)$.*

The number z_0 has n distinct n-th roots, given by the formulas

$$Z_k = \sqrt[n]{r}\left(\cos\frac{t^* + 2k\pi}{n} + i \sin\frac{t^* + 2k\pi}{n}\right),$$

for $k = 0, 1, \ldots, n-1$.

Proof. We use the polar representation of the complex number Z with the extended argument

$$Z = \rho(\cos\varphi + i \sin\varphi).$$

By definition, we have $Z^n = z_0$ or equivalently

$$\rho^n(\cos n\varphi + i \sin n\varphi) = r(\cos t^* + i \sin t^*).$$

We obtain $\rho^n = r$ and $n\varphi = t^* + 2k\pi$ for $k \in \mathbb{Z}$; hence $\rho = \sqrt[n]{r}$ and $\varphi_k = \frac{t^*}{n} + k \cdot \frac{2\pi}{n}$ for $k \in \mathbb{Z}$.

So far the roots of equation (1) are

$$Z_k = \sqrt[n]{r}(\cos\varphi_k + i \sin\varphi_k) \quad \text{for } k \in \mathbb{Z}.$$

Now observe that $0 \leq \varphi_0 < \varphi_1 < \cdots < \varphi_{n-1} < 2\pi$, so the numbers φ_k, $k \in \{0, 1, \ldots, n-1\}$, are reduced arguments, i.e., $\varphi_k^* = \varphi_k$. Until now we had n distinct roots of z_0:

$$Z_0, Z_1, \ldots, Z_{n-1}.$$

Consider some integer k and let $r \in \{0, 1, \ldots, n-1\}$ be the residue of k modulo n. Then $k = nq + r$ for $q \in \mathbb{Z}$, and

$$\varphi_k = \frac{t^*}{n} + (nq + r)\frac{2\pi}{n} = \frac{t^*}{n} + r\frac{2\pi}{n} + 2q\pi = \varphi_r + 2q\pi.$$

It is clear that $Z_k = Z_r$. Hence

$$\{Z_k : k \in \mathbb{Z}\} = \{Z_0, Z_1, \ldots, Z_{n-1}\}.$$

In other words, there are exactly n distinct n-th roots of z_0, as claimed.

The roots of the equation $Z^n - 1 = 0$ are called the n^{th} *roots of unity.* Since $1 = \cos 0 + i \sin 0$, from the formulas for the n^{th} roots of a complex number we derive that the n^{th} roots of unity are

$$\alpha_k = \cos\frac{2k\pi}{n} + i \sin\frac{2k\pi}{n}, \quad k \in \{0, 1, 2, \ldots, n-1\}.$$

11.5 Some Harder Problems

1. Let $z_1, z_2, z_3, \ldots, z_{12}$ be the 12 zeroes of the polynomial $z^{12} - 2^{36}$. For each j, let w_j be one of z_j or iz_j. Then find the maximum possible value of the real part of

$$X = \sum_{j=1}^{12} w_j$$

2. Let k be a positive integer, let $m = 2^k + 1$, and let $r \neq 1$ be a complex root of $z^m - 1 = 0$. Prove that there exist polynomials $P(z)$ and $Q(z)$ with integer coefficients such that

$$(P(r))^2 + (Q(r))^2 = -1.$$

3. Find the number of ordered pairs (a, b) of real numbers such that

$$(a + bi)^{2002} = a - bi.$$

4. Let α be a primitive root of unity and let z be a complex number such that

$$|z - \alpha^k| \leq 1 \quad \text{for all } k = 0, 1, \ldots, n-1.$$

Prove that $z = 0$.

5. Let z_1, z_2, z_3 be complex numbers such that

$$|z_1| = |z_2| = |z_3| = r > 0$$

and $z_1 + z_2 + z_3 \neq 0$. Prove that

$$\left| \frac{z_1 z_2 + z_2 z_3 + z_3 z_1}{z_1 + z_2 + z_3} \right| = r.$$

6. Let z_1, z_2 be complex numbers such that

$$|z_1| = |z_2| = r > 0.$$

Prove that

$$\left(\frac{z_1 + z_2}{r^2 + z_1 z_2} \right)^2 + \left(\frac{z_1 - z_2}{r^2 - z_1 z_2} \right)^2 \geq \frac{1}{r^2}.$$

7. Let z_1, z_2, z_3 be complex numbers such that

$$|z_1| = |z_2| = |z_3| = 1$$

and

$$\frac{z_1^2}{z_2 z_3} + \frac{z_2^2}{z_1 z_3} + \frac{z_3^2}{z_1 z_2} + 1 = 0.$$

Prove that

$$|z_1 + z_2 + z_3| \in \{1, 2\}.$$

11.6 Complex Numbers MCQ

1. The value of $\left(\frac{\sqrt{3}}{2} + i \cdot \frac{1}{2}\right)^{165}$ is

(A) -1 (B) $\frac{\sqrt{3}}{2} - i \cdot \frac{1}{2}$ (C) i (D) $-i$

2. The value of the expression

$$\left(\frac{-1+\sqrt{-3}}{2}\right)^n + \left(\frac{-1-\sqrt{-3}}{2}\right)^n$$

is

(A) 3 when n is a positive multiple of 3, and 0 when n is any other positive integer

(B) 2 when n is a positive multiple of 3, and -1 when n is any other positive integer

(C) 1 when n is a positive multiple of 3, and -2 when n is any other positive integer

(D) none of the foregoing numbers

3. How many integers k are there for which $(1-i)^k = 2^k$? (Here $i = \sqrt{-1}$)

(A) one (B) none (C) two (D) more than two

4. If n is a multiple of 4, the sum $S = 1 + 2i + 3i^2 + \ldots + (n+1)i^n$, where $i = \sqrt{-1}$, is

(A) $1-i$ (B) $\frac{n+2}{2}$ (C) $\frac{n^2+8-4ni}{8}$ (D) $\frac{n+2-ni}{2}$

5. If $a_0, a_1, \ldots, a_n$ are real numbers such that

$$(1+z)^n = a_0 + a_1 z + a_2 z^2 + \ldots + a_n z^n,$$

for all complex numbers z, then the value of

$$(a_0 - a_2 + a_4 - a_6 + \ldots)^2 + (a_1 - a_3 + a_5 - a_7 + \ldots)^2$$

equals

(A) $2n$ (B) $a_0^2 + a_1^2 + \ldots + a_n^2$ (C) $2n^2$ (D) $2n^2$

6. If $t_k = \binom{100}{k} x^{100-k}$ for $k = 0, 1, \ldots, 100$, then

$$(t_0 - t_2 + t_4 - \ldots + t_{100})^2 + (t_1 - t_3 + t_5 - \ldots - t_{99})^2$$

equals

(A) $(x^2-1)^{100}$ (B) $(x+1)^{100}$ (C) $(x^2+1)^{100}$ (D) $(x-1)^{100}$

7. The expression $\left(\frac{1+i}{1-i}\right)^n$ equals

(A) $-i^{n+1}$ (B) i^{n+1} (C) $-2i^{n+1}$ (D) 1

8. The value of the sum

$$\cos\frac{\pi}{1000} + \cos\frac{2\pi}{1000} + \ldots + \cos\frac{999\pi}{1000}$$

is

(A) 0 (B) 1 (C) $\frac{1}{1000}$ (D) an irrational number

9. The sum

$$1 + \binom{n}{1}\cos\theta + \binom{n}{2}\cos 2\theta + \ldots + \binom{n}{n}\cos n\theta$$

equals

(A) $(2\cos\frac{\theta}{2})^n \cos n\theta$ (B) $(2\cos^2\frac{\theta}{2})^n$ (C) $(2\cos^2\frac{n\theta}{2})^n$ (D) none of the foregoing quantities

10. Let $i = \sqrt{-1}$. Then

(A) i and $-i$ each has exactly one square root

(B) i has two square roots but $-i$ does not have any

(C) neither i nor $-i$ has any square root

(D) i and $-i$ each has exactly two square roots

11. If the complex numbers w and z represent two diagonally opposite vertices of a square, then the other two vertices are given by the complex numbers

(A) $w + iz$ and $w - iz$

(B) $\frac{1}{2}(w+z) + \frac{1}{2}i(w+z)$ and $\frac{1}{2}(w+z) - \frac{1}{2}i(w+z)$

(C) $\frac{1}{2}(w-z) + \frac{1}{2}i(w-z)$ and $\frac{1}{2}(w-z) - \frac{1}{2}i(w-z)$

(D) $\frac{1}{2}(w+z) + \frac{1}{2}i(w-z)$ and $\frac{1}{2}(w+z) - \frac{1}{2}i(w-z)$

12. Let

$$A = \{a + b\sqrt{-1} \mid a, b \text{ are integers}\}$$

and

$$U = \{x \in A \mid \frac{1}{x} \in A\}.$$

Then the number of elements in U is

(A) 2 (B) 4 (C) 6 (D) 8

13. Let $i = \sqrt{-1}$. Then the number of distinct elements in the set

$$S = \{i^n + i^{-n} : n \text{ an integer}\}$$

is

(A) 3 (B) 4 (C) greater than 4 but finite (D) infinite

14. Let $i = \sqrt{-1}$ and p be a positive integer. A necessary and sufficient condition for $(-i)^p = i$ is

(A) p is one of $3, 11, 19, 27, \ldots$ (B) p is an odd integer

(C) p is not divisible by 4 (D) none of the foregoing conditions

15. Suppose z_1, z_2 are complex numbers satisfying $z_2 \neq 0$, $z_1 \neq z_2$ and

$$\left|\frac{z_1 + z_2}{z_1 - z_2}\right| = 1.$$

Then $\frac{z_1}{z_2}$ is

(A) real and negative (B) real and positive

(C) purely imaginary (D) not necessarily any of these

16. The modulus of the complex number

$$\left(\frac{2 + i\sqrt{5}}{2 - i\sqrt{5}}\right)^{10} + \left(\frac{2 - i\sqrt{5}}{2 + i\sqrt{5}}\right)^{10}$$

is

(A) $2\cos\left(20\cos^{-1}\frac{3}{\sqrt{3}}\right)$ (B) $2\sin\left(10\cos^{-1}\frac{3}{\sqrt{3}}\right)$ (C) $2\cos\left(10\cos^{-1}\frac{3}{\sqrt{3}}\right)$ (D) $2\sin\left(20\cos^{-1}\frac{3}{\sqrt{3}}\right)$

17. . For any complex number $z = x + iy$ with x and y real, define $\langle z\rangle = |x| + |y|$. Let z_1 and z_2 be any two complex numbers. Then

(A) $\langle z_1 + z_2\rangle \leq \langle z_1\rangle + \langle z_2\rangle$ (B) $\langle z_1 + z_2\rangle \geq \langle z_1\rangle + \langle z_2\rangle$

(C) $\langle z_1 + z_2\rangle > \langle z_1\rangle + \langle z_2\rangle$ (D) none of the foregoing statements need always be true

18. Recall that for a complex number $z = x+iy$, where $i = \sqrt{-1}$, $|z| = (x^2+y^2)^{1/2}$ and $\arg(z) =$ principal value of $\tan^{-1}\left(\frac{y}{x}\right)$ Given complex numbers $z_1 = a + ib$, $z_2 = \frac{a}{\sqrt{2}}(1-i) + \frac{b}{\sqrt{2}}(1+i)$, $z_3 = \frac{a}{\sqrt{2}}(i-1) - \frac{b}{\sqrt{2}}(i+1)$, where a and b are real numbers, only one of the following statements is true. Which one is it?

(A) $|z_1| = |z_2|$ and $|z_2| > |z_3|$ (B) $|z_1| = |z_3|$ and $|z_1| < |z_2|$

(C) $\arg z_1 = \arg z_2$ and $\arg z_1 - \arg z_3 = \frac{\pi}{4}$ (D) $\arg z_2 - \arg z_1 = -\frac{\pi}{4}$ and $\arg z_3 - \arg z_2 = \pm\pi$

19. If $a_0, a_1, \ldots, a_{2n}$ are real numbers such that

$$(1 + z)^{2n} = a_0 + a_1 z + a_2 z^2 + \ldots + a_{2n} z^{2n},$$

for all complex numbers z, then

(A) $a_0 + a_1 + a_2 + \ldots + a_{2n} = 2^n$ (B) $(a_0 - a_2 + a_4 - \ldots)^2 + (a_1 - a_3 + a_5 - \ldots)^2 = 2^{2n}$

(C) $a_0^2 + a_1^2 + a_2^2 + \ldots + a_{2n}^2 = 2^{2n}$ (D) $(a_0 + a_2 + a_4 + \ldots)^2 + (a_1 + a_3 + a_5 + \ldots)^2 = 2^{2n}$

20. If z is a nonzero complex number and $\frac{z}{1+z}$ is purely imaginary, then z

(A) can be neither real nor purely imaginary (B) is real

(C) is purely imaginary (D) satisfies none of the above properties

ANSWER KEY

1	2	3	4	5	6	7	8	9	10
D	B	A	D	A	C	C	A	A	D
11	12	13	14	15	16	17	18	19	20
D	B	A	D	C	A	A	D	B	A

12 Geometry: Triangles

12.1 Congruence of Triangles

Definition 3. If two triangles have two sides of the one equal to two sides of the other, each to each, and also the angles contained by those sides equal, then the two triangles are **congruent**.

In other words, two triangles $A_1B_1C_1$ and $A_2B_2C_2$ are congruent if $A_1B_1 = A_2B_2$, $B_1C_1 = B_2C_2$, $C_1A_1 = C_2A_2$, $\angle A_1 = \angle A_2$, $\angle B_1 = \angle B_2$, and $\angle C_1 = \angle C_2$. We write $\Delta A_1B_1C_1 \equiv \Delta A_2B_2C_2$ to mean that the two triangles are congruent. We observe that:

1. $\Delta ABC = \Delta ABC$ for any triangle ABC
2. If $\Delta A_1B_1C_1 \equiv \Delta A_2B_2C_2$, then $\Delta A_2B_2C_2 \equiv \Delta A_1B_1C_1$
3. If $\Delta A_1B_1C_1 \equiv \Delta A_2B_2C_2$ and $\Delta A_2B_2C_2 \equiv \Delta A_3B_3C_3$, then $\Delta A_1B_1C_1 \equiv \Delta A_3B_3C_3$

We take the following test for congruence of two triangles as an axiom.

SAS test: Two triangles are congruent if two sides and the included angle of one triangle are respectively equal to two sides and the included angle of the other.

This says that, if in two triangles, $A_1B_1C_1$ and $A_2B_2C_2$, $A_1B_1 = A_2B_2$, $A_1C_1 = A_2C_2$ and $\angle A_1 = \angle A_2$, then the two triangles are congruent. This is known as the **"Side Angle Side" test**.

Theorem 1: The sum of any two angles of a triangle is less than a straight angle.

Proof. Let D be the midpoint of the side BC of a triangle ABC. Produce AD to E such that $AD = DE$ (Fig. 1). Then by the SAS test the triangles ADB and EDC are congruent. Therefore, $\angle ABC = \angle ECD$ and hence $\angle ABC + \angle BCA = \angle ECD + \angle BCA = \angle ECA < 180°$ (note that E cannot lie on AC since the two distinct lines AD and AC have only one common point, namely A). Thus, the sum $\angle ABC + \angle BCA$ is less than two right angles. Similar arguments show that $\angle C + \angle A$ and $\angle A + \angle B$ are also each less than $180°$.

Corollary 1. Any exterior angle of a triangle is greater than any of the two non-adjacent interior angles.

Proof. Let ABC be any triangle and D be a point on BC produced as shown in Fig. 2. We want to prove that the exterior angle DCA is bigger than each of the non-adjacent interior angles A and B. By Theorem 1, $\angle DCA + \angle ACB = 180°$. By the theorem (Theorem 4) $\angle BCA + \angle CAB < 180° = \angle DCA + \angle BCA$. Therefore $\angle CAB < \angle DCA$. Again $\angle ABC + \angle BCA < 180° = \angle DCA + \angle BCA$ implies that $\angle ABC < \angle DCA$. Thus the exterior angle DCA is bigger than each of $\angle A$ and $\angle B$ of $\triangle ABC$. □

Corollary 2. In any triangle ABC, at most one of the angles A, B, C can be obtuse.

Proof. Immediate from Theorem 1.

Theorem 5. (ASA theorem) Two triangles are congruent if two angles and a side of one triangle are respectively equal to two angles and the corresponding side of the other.

Proof. Case (i) Suppose in triangles $A_1B_1C_1$ and $A_2B_2C_2$ we have $\angle B_1 = \angle B_2$, $\angle C_1 = \angle C_2$ and $B_1C_1 = B_2C_2$. Take D_1 on B_1A_1 such that $B_1D_1 = B_2A_2$ (we may assume without loss of generality $A_2B_2 \le A_1B_1$) (Fig. 3). Then in the two triangles $B_1C_1D_1$ and $B_2C_2A_2$, we have, the two sides B_1C_1 and B_1D_1 of $\Delta B_1C_1D_1$ equal in length to the two sides B_2C_2 and B_2A_2 respectively of $\Delta B_2C_2A_2$. Further the included angles B_1 and B_2 are equal. Therefore by SAS test, the two triangles are congruent. This means that $\angle B_1C_1D_1 = \angle B_2C_2A_2$. But $\angle B_2C_2A_2 = \angle B_1C_1A_1$ by our assumption. Therefore $\angle B_1C_1D_1 = \angle B_1C_1A_1$ and hence by our fundamental principle of measuring angles, the ray C_1D_1 coincides with the ray C_1A_1. This in turn implies D_1 coincides with A_1. Thus $\Delta A_1B_1C_1 \equiv \Delta A_2B_2C_2$.

Case (ii) $\angle B_1 = \angle B_2, \angle C_1 = \angle C_2$ and the side A_1B_1 of $\Delta A_1B_1C_1$ = side A_2B_2 of $\Delta A_2B_2C_2$. Take E_1 on B_1C_1 such that $B_1E_1 = B_2C_2$ (as in Fig. 3.21; again without loss of generality we may assume that $B_1C_1 > B_2C_2$). Then the two triangles $B_1E_1A_1$ and $B_2C_2A_2$ are congruent by the SAS test. Now, for $\Delta A_1E_1C_1$, the exterior

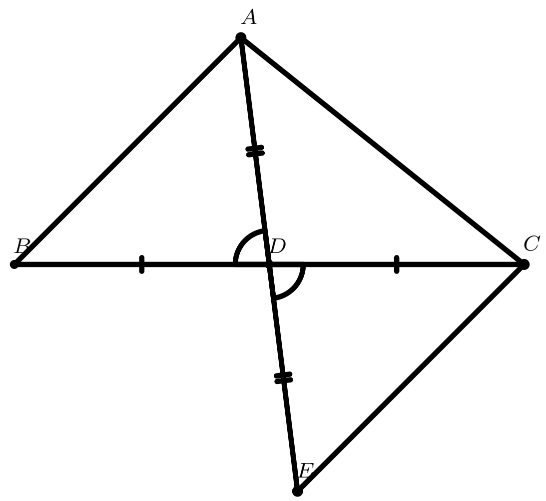


Figure 1:

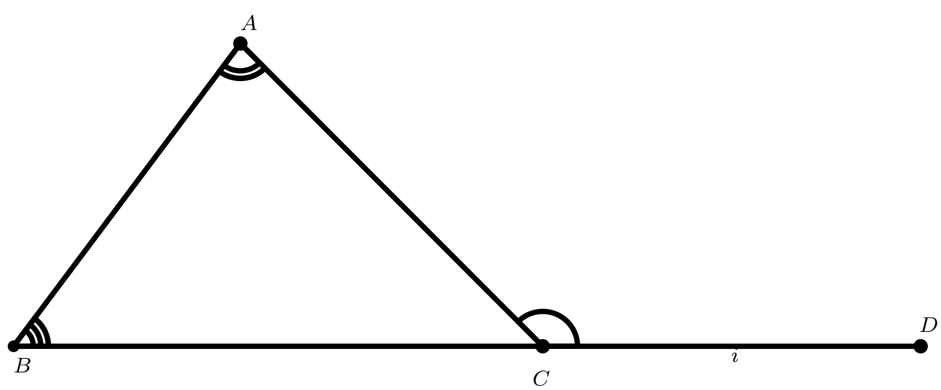


Figure 2:

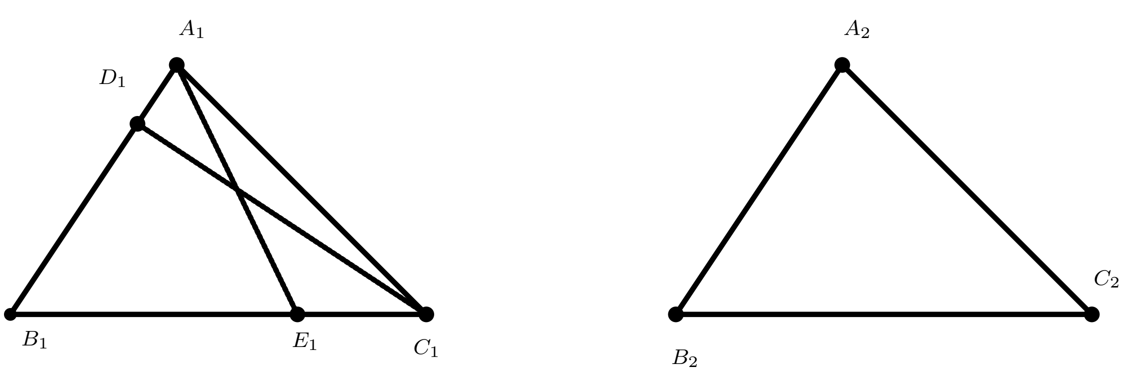


Figure 3:

angle $A_1E_1B_1$ = the interior angle $A_1E_1B_1$, which is against the corollary 1 to Theorem 4 unless the point E_1 coincides with C_1 in which case $\Delta A_1B_1C_1 \equiv \Delta A_2B_2C_2$.

Theorem 8. (SSS Theorem) If the three sides of one triangle are respectively equal to the three sides of another triangle, then the two triangles are congruent.

Proof. In triangles $A_1B_1C_1$ and $A_2B_2C_2$ we are given that $A_1B_1 = A_2B_2$, $B_1C_1 = B_2C_2$ and $C_1A_1 = C_2A_2$. Suppose $\angle A_1 = \angle A_2$, or $\angle B_1 = \angle B_2$, then by our fundamental SAS test the two triangles are congruent. Otherwise assume that $\angle A_1 \neq \angle A_2$ and $\angle B_1 \neq \angle B_2$. Draw A_1C_3 as in Fig. 3.25 such that $\angle B_1A_1C_3 = \angle B_2A_2C_2$ and C_3, C_1 lie on the same side of the side A_1B_1, and further such that $A_1C_3 = A_2C_2$. Now, $A_1C_1 = A_2C_2$ by assumption. Therefore $\Delta A_1C_1C_3$ is isosceles. Again in triangles $A_1B_1C_3$ and $A_2B_2C_2$ we have $A_1B_1 = A_2B_2$, $A_1C_3 = A_2C_2$ and $\angle B_1A_1C_3 = \angle B_2A_2C_2$ (by construction). Applying the SAS test we note that $\Delta A_1B_1C_3 = \Delta A_2B_2C_2$. Therefore $B_1C_3 = B_2C_2$; also $B_1C_1 = B_2C_2$ by hypothesis. This implies that $\Delta B_1C_1C_3$ is isosceles. If D is the midpoint of C_1C_3 then A_1D and B_1D are both on C_1C_3 (Cor. to Theorem 7). Now, the straight lines A_1D and B_1D are distinct since D lies on the segment C_1C_3 and C_1, C_3 are both on the same side of the straight line A_1B_1. This means that we have two distinct perpendiculars DA_1, DB_1 through the point D on C_1C_3 to the straight line C_1C_3, which is impossible. Our assumption $\angle A_1 \neq \angle A_2$ and $\angle B_1 \neq \angle B_2$ has led to this impossibility. Therefore $\angle A_1 = \angle A_2$ or $\angle B_1 = \angle B_2$ and in either case we have already observed that the two triangles $A_1B_1C_1$ and $A_2B_2C_2$ are congruent.

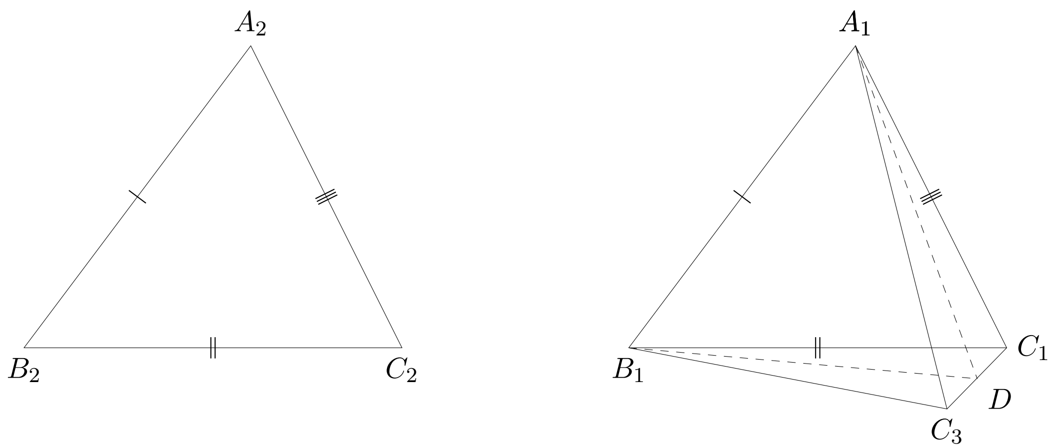


Figure 4:

Theorem 9. (RHS Theorem) If in two right-angled triangles, the hypotenuse and a side of one triangle are respectively equal to the hypotenuse and a side of the other, then the two triangles are congruent.

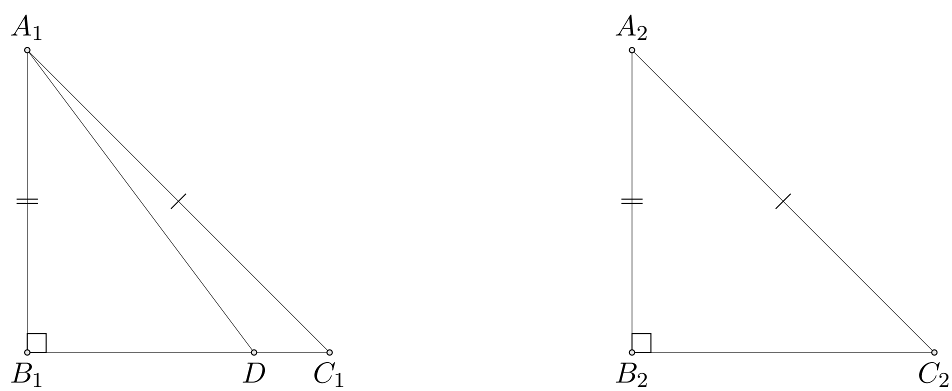


Figure 5:

Proof. In the triangles $A_1B_1C_1$ and $A_2B_2C_2$ we are given that $\angle B_1 = \angle B_2 = 90°$, the hypotenuse A_1C_1 is equal to the hypotenuse A_2C_2 and $A_1B_1 = A_2B_2$. If $B_1C_1 = B_2C_2$ then by SSS Theorem, the two triangles are congruent. Suppose $B_1C_1 \neq B_2C_2$. We may assume $B_1C_1 > B_2C_2$. Take D on B_1C_1 such that $B_1D = B_2C_2$. Then by construction $\Delta A_1B_1D = \Delta A_2B_2C_2$ (SAS test). This implies that $A_1D = A_2C_2$; but by hypothesis $A_1C_1 = A_2C_2$. Therefore $A_1D = A_1C_1$ and the ΔA_1C_1D is isosceles. Hence the base angles A_1C_1D and A_1DC_1 must be equal. By

Theorem 4, in the right-angled ΔA_1B_1D, $\angle A_1DB_1$ has to be necessarily acute and hence $\angle A_1DC_1$ is obtuse. This means that ΔA_1C_1D has two obtuse angles contradicting Theorem 4. Hence our supposition that $B_1C_1 \neq B_2C_2$ is wrong and we must have $B_1C_1 = B_2C_2$. This in turn implies that $\Delta A_1B_1C_1 \equiv \Delta A_2B_2C_2$.

Theorem 10 If two sides of a triangle are not equal, then the greater side has the greater angle opposite to it.

Proof. In ΔABC we are given that $AC > AB$. We want to prove that $\angle B > \angle C$. Take the point D on AC such that $AD = AB$. Then by construction ΔABD is isosceles and hence $\angle ADB = \angle ABD$. By the Corollary 1 to Theorem 4, the exterior angle $BDA > \angle ACB$. Therefore $\angle ABD > \angle ACB$. Clearly, $\angle ABC > \angle ABD$ (Fig. 6). Thus $\angle ABC > \angle ACB$ or $\angle B > \angle C$ whenever $AC > AB$.

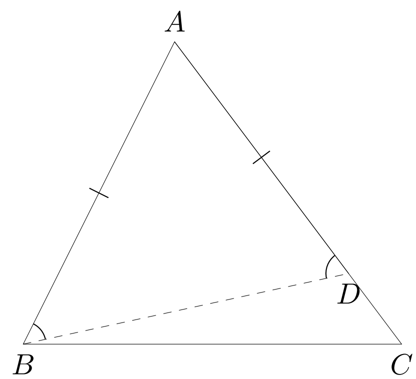


Figure 6:

Theorem 11 If two angles of a triangle are unequal, the greater angle has the greater side opposite to it.

Proof. In ΔABC we are given that $\angle B > \angle C$ (Fig. 7). We want to prove that $AC > AB$. Since $\angle B > \angle C$, we note that $AB \neq AC$. If $AC < AB$, then by Theorem 10 we must have $\angle C > \angle B$, which is against our hypothesis. Therefore $AC > AB$.

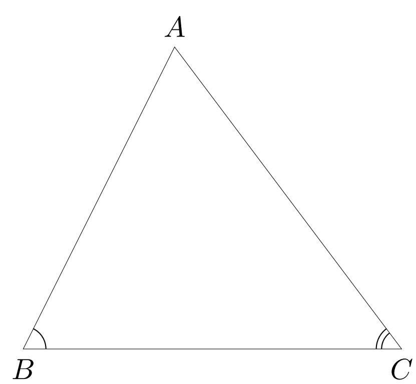


Figure 7:

Definition: The locus of a point equidistant from two fixed points is the perpendicular bisector of the line segment joining the two points.

Definition: The locus of a point which is equidistant from two intersecting straight lines is the pair of bisectors of the angles formed by the two straight lines.

12.2 Some properties of a triangle

Theorem The perpendicular bisectors of the three sides of a triangle concur at a point.

Proof. Let ΔABC be a triangle; let D, E, F be the midpoints of the sides BC, CA, AB respectively. Suppose the $\perp$ bisectors of BC and CA meet at S. Then it is required to prove that $SF \perp AB$. S being a point on the

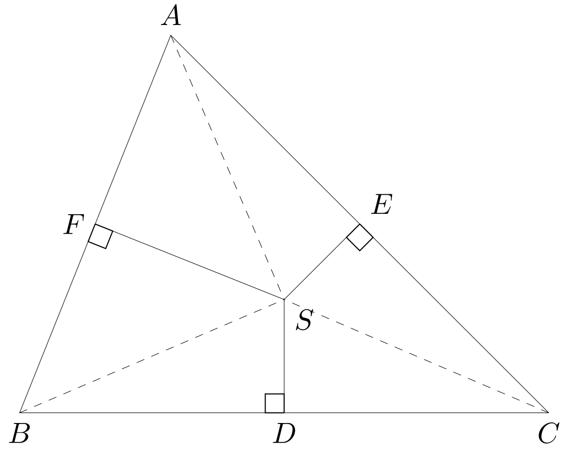


Figure 8:

perpendicular bisector of BC, we have $SB = SC$ (Theorem 12). Again, S lies on the perpendicular bisector of CA implies that $SC = SA$. Thus $SA = SB = SC$. In triangles ASF and BSF we have $AF = BF$ (Hypothesis), $SA = SB$ (proved above) and $SF = SF$ (common side). Therefore, $\Delta ASF \equiv \Delta BSF$. This implies that $\angle AFS = \angle BFS = 90°$ or $SF \perp AB$.

Note. The point of concurrence S, of the perpendicular bisectors of the sides of a triangle ΔABC is known as the *circumcentre* of ΔABC.

Theorem 24 The bisectors of the three angles of a triangle meet at a point.

Proof. Let ΔABC be a triangle and let the bisectors of the angles B and C meet at I (Fig. 9). It is required to prove that AI bisects $\angle A$. Draw IX, IY, IZ perpendicular to BC, CA, AB respectively (Fig. 9). Since I lies on the bisector BI of $\angle B$ we have $IX = IZ$ (Theorem 13). Similarly, the fact that I lies on the bisector of $\angle C$ implies that $IX = IY$. Thus $IX = IY = IZ$. Now $IY = IZ$ implies, again by Theorem 13, that I lies on the bisector of $\angle A$. Hence the bisectors of the three angles of a triangle concur at a point.

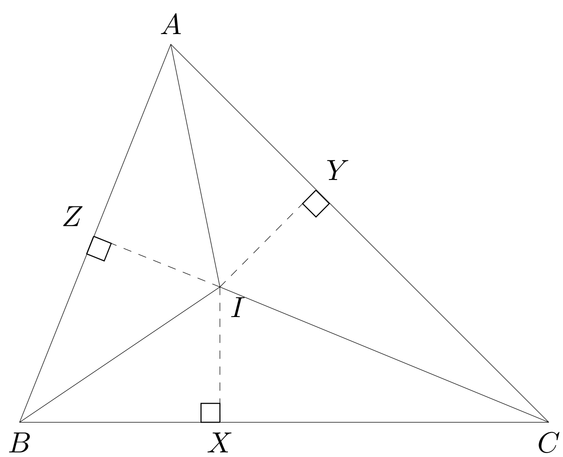


Figure 9:

Theorem The three medians of a triangle meet at a point and the point of concurrence trisects each median.

Proof. Let the medians BE and CF of ΔABC meet at G and let AG meet BC at D. It is required to prove that $BD = DC$ and that $AG/GD = BG/GE = CG/GF = 2/1$. Draw $BH \parallel FC$ meeting AD at H. In ΔABH, $FG \parallel BH$ and F is the midpoint of AB. Therefore, by Theorem 22, G must be the midpoint of AH. This means that in ΔAHC, $GE \parallel HC$ (by Theorem 22). This in turn implies that $BHCG$ is a parallelogram and the diagonals BC and GH bisect each other at D. Hence $BD = DC$, proving that the three medians of a triangle meet at a point.

Further, as already observed, $AG = GH$ and $GD = DH = (1/2)GH$ implies that $AG/GD = 2/1$. Similarly, BE and CF are also trisected by G.

Note. G is known as the *centroid* of ΔABC.

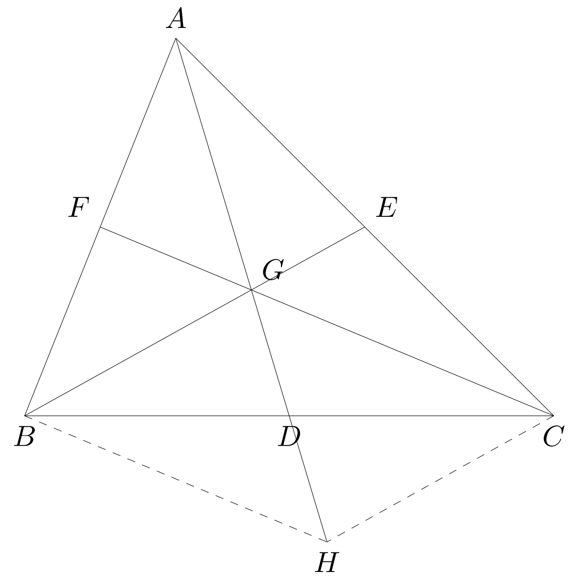


Figure 10:

12.3 Similar Triangles

Theorem 27 Parallelograms on the same base and between the same parallels are equal in area.

Proof. Let $ABCD$ and $ABXY$ be two parallelograms having the same base AB and lying between the same parallels, namely the straight line AB and the straight line YC (Fig. 3.51). The parallelogram $ABCD =$ Trapezium $ABCY - \Delta ADY$ and the parallelogram $ABXY =$ Trapezium $ABCY - \Delta BCX$ (in area). Therefore to prove that the two parallelograms $ABCD$ and $ABXY$ have equal areas, it is enough to prove that ΔADY and ΔBCX have equal areas. We have $\angle ADY = \angle BCX$ (corresponding angles), $\angle AYD = \angle BXC$ (corresponding angles) and $AY = BX$ (since $ABXY$ is a parallelogram). Therefore by the ASA theorem, the two triangles ΔADY and ΔBCX are congruent. So they have equal areas.

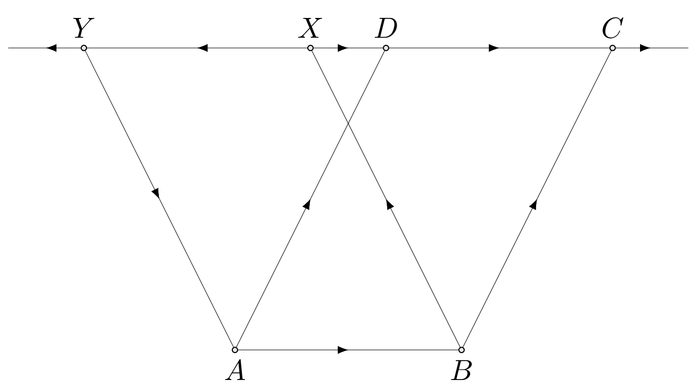


Figure 11:

Theorem 29 If a straight line is drawn parallel to one side of a triangle, then it divides the other two sides proportionally. Also, conversely, if a straight line divides two sides of a triangle proportionally, then it is parallel to the third side.

Proof. Let XY be a straight line parallel to BC meeting AB, AC at X, Y (Fig. 3.56). We want to prove that

$AX/XB = AY/YC$. The triangles AXY and BXY have equal altitudes and hence

$$\frac{\Delta AXY}{\Delta BXY} = \frac{AX}{XB}$$

Similarly,

$$\frac{\Delta AXY}{\Delta CXY} = \frac{AY}{YC}$$

Now the triangles BXY and CXY have the same base XY and are between the same parallels. Hence $\Delta BXY = \Delta CXY$. This gives

$$\frac{AX}{XB} = \frac{\Delta AXY}{\Delta BXY} = \frac{\Delta AXY}{\Delta CXY} = \frac{AY}{YC}$$

Conversely, suppose the straight line XY meets AB, AC at X, Y and

$$\frac{AX}{XB} = \frac{AY}{YC}$$

We want to prove that $XY \parallel BC$. Again, we have

$$\frac{\Delta AXY}{\Delta BXY} = \frac{AX}{XB} \quad \text{and} \quad \frac{\Delta AXY}{\Delta CXY} = \frac{AY}{YC}$$

By our hypothesis, $\frac{AX}{XB} = \frac{AY}{YC}$ and therefore $\Delta BXY = \Delta CXY$. Now BXY and CXY are two triangles of equal areas on XY and are on the same side of XY. Hence $XY \parallel BC$.

Theorem 31. The internal (or external) bisector of an angle of a triangle divides the opposite side internally (or externally) in the ratio of the sides containing the angle.

Proof. Let AD be the internal (external) bisector of $\angle A$ of $\triangle ABC$ meeting BC (or BC produced) at D. It is required to prove that

$$\frac{BD}{DC} = \frac{AB}{AC}$$

Draw $CE \parallel AD$ meeting BA or BA produced at E.

Let F be a point on BA or BA produced.

Then

$$\angle FAD = \angle AEC = \frac{\angle A}{2} \text{ or } \left(90^\circ - \frac{\angle A}{2}\right)$$

Also,

$$\angle DAC = \angle ACE = \frac{\angle A}{2} \text{ or } \left(90^\circ - \frac{\angle A}{2}\right)$$

Thus, in $\angle AEC$, we have $\angle AEC = \angle ACE$ and hence $AE = AC$. In $\triangle BCE$, we have $AD \parallel EC$ and therefore by Theorem 29, we get

$$\frac{BD}{DC} = \frac{BA}{AE} = \frac{BA}{AC} \quad \text{(Since } AE = AC \text{ as already observed)}$$

Thus,

$$\frac{BD}{DC} = \frac{AB}{AC}$$

Definition 7. If a line segment AB is divided internally and externally in the same ratio at P and Q respectively, then AB is said to be divided harmonically at P and Q. P and Q are called **harmonic conjugates** with respect to AB.

$$\frac{AP}{PB} = \frac{AQ}{BQ}$$

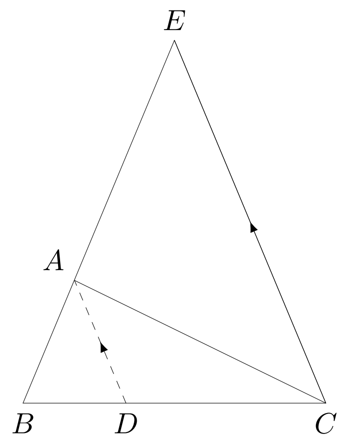


Figure 12:

Figure 13: P and Q are harmonic conjugates with respect to AB

1. If P and Q are harmonic conjugates with respect to AB, then A and B are harmonic conjugates with respect to PQ.
$$\frac{AP}{PB} = \frac{AQ}{QB} \implies \frac{PA}{AQ} = -\frac{AP}{AQ} = -\frac{PB}{BQ} = -\frac{PB}{BQ}$$

2. If P and Q divide AB harmonically, then AP, AB, and AQ are in harmonic progression.

   We have
$$\frac{AP}{AQ} = \frac{PB}{BQ} = \frac{AB - AP}{AQ - AB}$$
   and therefore,
$$AP(AQ - AB) = AQ(AB - AP) \quad \text{or} \quad 2AP \cdot AQ = (AQ + AP) \cdot AB$$
   This gives
$$\frac{2}{AB} = \frac{1}{AP} + \frac{1}{AQ}$$

3. If O is the midpoint of AB and P, Q divide AB harmonically, then $OB^2 = OP \cdot OQ$.

   We have
$$\frac{AP}{PB} = \frac{AQ}{BQ} \quad \text{or} \quad \frac{AP + PB}{AP - PB} = \frac{AQ + BQ}{AQ - BQ}$$
   Therefore,
$$\frac{AB}{AO + OP} = \frac{20B}{20P} = \frac{20O}{20B}$$
   or
$$OB^2 = OP \cdot OQ$$

Definition 8. Two triangles are similar if the three angles of one are equal to the three angles of the other taken in order and the sides about the equal angles are proportional.

In other words, $\triangle A_1B_1C_1 \sim \triangle A_2B_2C_2$ if $\angle A_1 = \angle A_2$, $\angle B_1 = \angle B_2$, $\angle C_1 = \angle C_2$ and
$$\frac{A_1B_1}{A_2B_2} = \frac{B_1C_1}{B_2C_2} = \frac{C_1A_1}{C_2A_2}$$

We write $\triangle A_1B_1C_1 \sim \triangle A_2B_2C_2$ to mean that the two triangles are similar. We observe the following:

1. Any triangle is similar to itself.
2. If $\triangle A_1B_1C_1 \sim \triangle A_2B_2C_2$, then $\triangle A_2B_2C_2 \sim \triangle A_1B_1C_1$.
3. If $\triangle A_1B_1C_1 \sim \triangle A_2B_2C_2$ and $\triangle A_2B_2C_2 \sim \triangle A_3B_3C_3$, then $\triangle A_1B_1C_1 \sim \triangle A_3B_3C_3$.
4. If two triangles are congruent, then they are also similar. (How about the converse statement?)

12.4 Concurrence and Collinearity

Three points A, B, C are collinear if they all lie on a straight line. If A, B, C are as shown in Figure 70, then $AB + BC = AC$. If we use directed segments, we always have

$$\overrightarrow{AB} + \overrightarrow{BC} + \overrightarrow{CA} = 0.$$

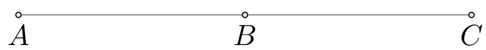


Figure 14: Collinear points A, B, and C

Theorem 39. (Stewart's theorem)
If A, B, C are three collinear points and P any other point, then

$$PA^2 \cdot BC + PB^2 \cdot CA + PC^2 \cdot AB + BC \cdot CA \cdot AB = 0$$

(using directed segments).

Case (i) P does not lie on the straight line ABC.

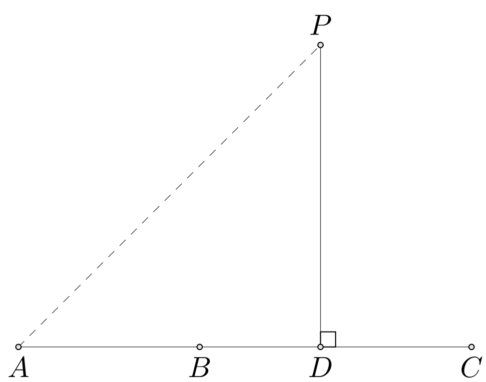


Figure 15: Point P not on the line ABC

Proof. Let D be the foot of the perpendicular from P on the line ABC. Then we have

$$PA^2 = PD^2 + DA^2 = PD^2 + (DC + CA)^2$$
$$= PD^2 + DC^2 + CA^2 + 2DC \cdot CA.$$

Similarly,

$$PB^2 = PD^2 + DB^2 = PD^2 + (DC + CB)^2$$
$$= PD^2 + DC^2 + CB^2 + 2DC \cdot CB.$$

Now

$$PC^2 = PD^2 + DC^2 \quad \text{and hence we get}$$
$$PA^2 = PC^2 + CA^2 + 2DC \cdot CA.$$
$$PB^2 = PC^2 + CB^2 - 2DC \cdot BC \quad (\text{since } CB = -BC).$$

This gives

$$PA^2 \cdot BC + PB^2 \cdot CA = PC^2 \cdot BC + CA^2 \cdot BC + 2DC \cdot CA \cdot BC + PC^2 \cdot CA + CB^2 \cdot CA - 2DC \cdot BC \cdot CA.$$
$$= PC^2 \cdot (BC + CA) + (BC \cdot CA)(BC + CA) + (BC \cdot CA)(-AB).$$
$$= (PC^2 + BC \cdot CA)(-AB).$$

Hence

$$PA^2 \cdot BC + PB^2 \cdot CA + PC^2 \cdot AB + BC \cdot CA \cdot AB = 0.$$

Case (ii) P lies on the straight line ABC.

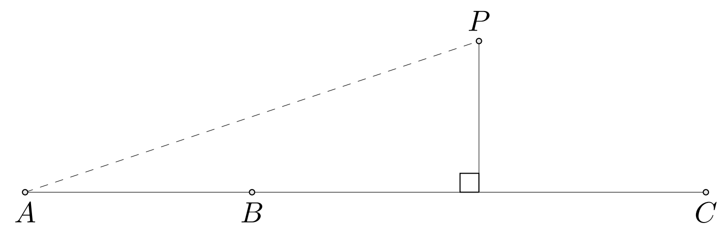


Figure 16: Point P on the line ABC

Let Q be any point on the perpendicular through P to the line ABC. Then by case (i) we have

$$QA^2 \cdot BC + QB^2 \cdot CA + QC^2 \cdot AB + BC \cdot CA \cdot AB = 0.$$

We note that

$$QA^2 = QP^2 + PA^2, \quad QB^2 = QP^2 + PB^2, \quad QC^2 = QP^2 + PC^2.$$

Substituting in the above equation we get

$$QP^2(BC + CA + AB) + PA^2 \cdot BC + PB^2 \cdot CA + PC^2 \cdot AB + BC \cdot CA \cdot AB = 0.$$

Now $BC + CA + AB = 0$ and hence we get our required result.

Theorem (Menelaus Theorem) If a transversal cuts the sides BC, CA and AB of a triangle ABC at D, E and F respectively then

$$\frac{BD}{DC}\frac{CE}{EA}\frac{AF}{FB} = -1$$

Proof. Draw $CX \parallel BA$ meeting the transversal at X (Fig. 3.73). The triangles FBD and XCD are similar since $BF \parallel CX$. Therefore,

$$\frac{BD}{DC} = \frac{FB}{CX} \quad \text{(in magnitudes of the segments).}$$

Again, the triangles EAF and ECX are similar and so

$$\frac{CE}{EA} = \frac{CX}{AF} \quad \text{(in magnitudes of the segments).}$$

Hence, we get

$$\frac{BD}{DC} \cdot \frac{CE}{EA} = \frac{FB}{CX} \cdot \frac{CX}{AF}$$
$$\Rightarrow \frac{BD}{DC} \cdot \frac{CE}{EA} \cdot \frac{AF}{FB} = 1 \quad \text{in magnitude.}$$

Now, we shall examine the sign of the product. A transversal cuts two sides internally and the other side externally as in Fig. 3.73 or cuts all the three sides externally as in Fig. 3.74.

In the former case (as in Fig. 3.73) we have one ratio negative and the other two positive. In our Fig. 3.73,

$$\frac{BD}{DC} < 0, \quad \frac{CE}{EA} \quad \text{and} \quad \frac{AF}{FB} \quad \text{are positive.}$$

In the latter case (as in Fig. 3.74), all the ratios

$$\frac{BD}{DC}, \quad \frac{CE}{EA}, \quad \text{and} \quad \frac{AF}{FB} \quad \text{are negative.}$$

Thus the product

$$\frac{BD}{DC} \cdot \frac{CE}{EA} \cdot \frac{AF}{FB}$$

is always negative and

$$\frac{BD}{DC} \cdot \frac{CE}{EA} \cdot \frac{AF}{FB} = -1.$$

---

13 Geometry: Circles

13.1 Circles Introduction

A circle is a geometric figure in a plane such that all its points are equidistant from a fixed point in the plane. The fixed point is the centre of the circle and the constant distance from the centre is the radius of the circle.

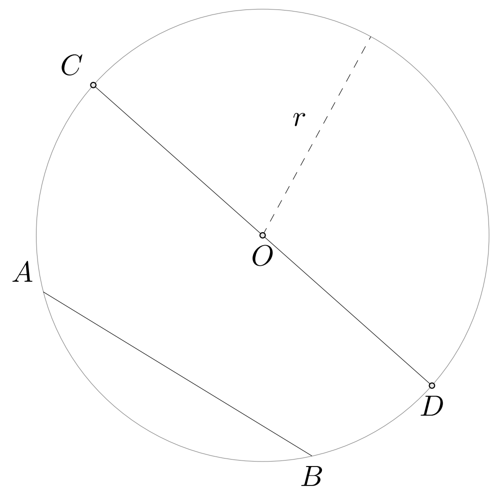


Figure 17:

The circle S in Fig. 17 has centre O and radius r.

A chord of a circle is a straight line segment joining any two points on the circle. A chord passing through the centre is called a *diameter* of the circle. In Fig. 17, AB is a chord of the circle S and CD is a diameter. Circles which have the same centre are called *concentric circles*.

We observe that a point is within, upon, or outside a circle according as its distance from the centre is less than, equal to, or greater than the radius. Concentric circles whose radii are unequal, do not intersect with each other. A circle is symmetric about any of its diameters . Also, a circle is symmetric about its centre.

Theorem 1. The perpendicular bisector of any chord of a circle passes through the centre of the circle.

Proof. Let O be the centre of a circle S and AB be any chord; let C be the midpoint of AB (See Fig. 18). We want to prove that the perpendicular bisector of AB passes through O. In other words, we wish to prove that $OC \perp AB$. In the triangles AOC and BOC we have $OA = OB$ (radius of the circle), $AC = CB$ (by hypothesis) and OC is common. Therefore the two triangles are congruent. Hence $\triangle OCA \equiv \triangle OCB$ which implies that $\angle OCA = \angle OCB = 90°$ or $OC \perp AB$.

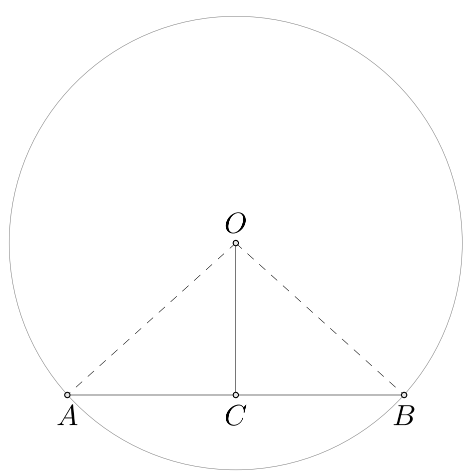


Figure 18:

Corollary 1: If two circles have three points in common then they must coincide.

Corollary 2: Two circles cannot intersect at more than two points.

Corollary 3 If A, B, C are any three points on a circle and O is a point within the circle such that $OA = OB = OC$ then O is the centre of the circle.

Corollary 4 Two circles cannot have a common arc unless they coincide.

Theorem 3
Equal chords of a circle are equidistant from the centre. Conversely, if two chords of a circle are equidistant from the centre, then they are equal.
Proof. Suppose AB and CD are two equal chords of a circle with centre O. Let OX, OY be the perpendiculars from O onto the chords AB, CD respectively (Fig. 19). It is required to prove that $OX = OY$. By Theorem 1, OX and OY are the perpendicular bisectors of AB and CD. Hence $AX = CY = \frac{1}{2}AB = \frac{1}{2}CD$. Now, in $\triangle AOX$ and $\triangle COY$ we have $\angle AXO = \angle CYO = 90°$, hypotenuse AO = hypotenuse CO (radii) and $AX = CY$. Therefore $\triangle AOX \cong \triangle COY$ and hence $OX = OY$. Thus, the two equal chords AB and CD are equidistant from the centre O.

Converse. We may use the same figure, Fig. 19. But now we assume $OX = OY$ and we wish to prove that $AB = CD$. Again, we compare the right triangles AOX and COY. We have hypotenuse AO = hypotenuse CO and $OX = OY$. Therefore, the two triangles are congruent and hence we get $AX = CY$. But by Theorem 1, $AX = \frac{1}{2}AB$ and $CY = \frac{1}{2}CD$. Therefore, $AX = CY$ implies that $AB = CD$.

Theorem 4 Given any two chords of a circle, the one which is nearer to the centre is greater than the one more remote.

Proof. Let AB, CD be two chords of a circle with centre O. Let OX, OY be the perpendiculars to AB, CD meeting them at X, Y respectively (Fig. 19). Suppose $OX < OY$. Then from the right triangles AOX and COY we have $AO^2 = OX^2 + AX^2$ and $CO^2 = OY^2 + CY^2$. But $AO = CO$ = radius of the circle. Therefore we get $OX^2 + AX^2 = OY^2 + CY^2$. By assumption $OX < OY$ and so $OX^2 + AX^2 < OY^2 + CY^2$. This can hold good if and only if $AX > CY$. But by Theorem 1, $AX = \frac{1}{2}AB$ and $CY = \frac{1}{2}CD$. Thus $OX < OY$ implies that $AB > CD$.

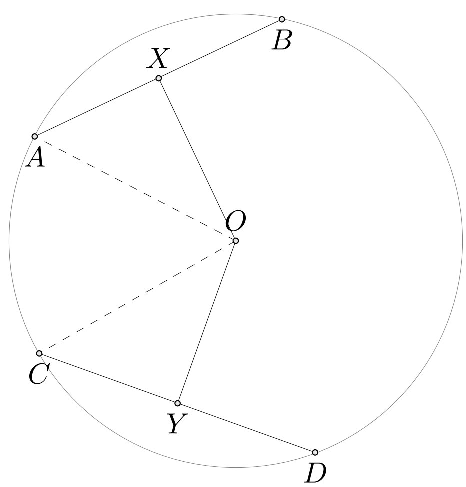


Figure 19:

Theorem 5: The angle subtended at the center is double the angle subtended by the same chord on the circumference

Theorem 6: Angle in the same segment of the circle are equal.

13.2 Tangents

In general, we have seen that a straight line cuts a circle at, utmost two points. If a straight line has just one common point with a circle, we say that the straight line touches the circle. In that case, the straight line is called a *tangent* to the circle and the point at which a tangent touches the circle is known as the point of contact of the tangent. Two circles touch one another when they have only one point in common and have a common tangent at this point. Circles may touch externally in which case they are on opposite sides of the common tangent or they may touch internally in which case they are on the same side on the common tangent.

Theorem 7. One and only one tangent can be drawn to a circle at any point on its circumference and this tangent is perpendicular to the radius through the point of contact.
Proof. Let P be any point on a circle with centre O.

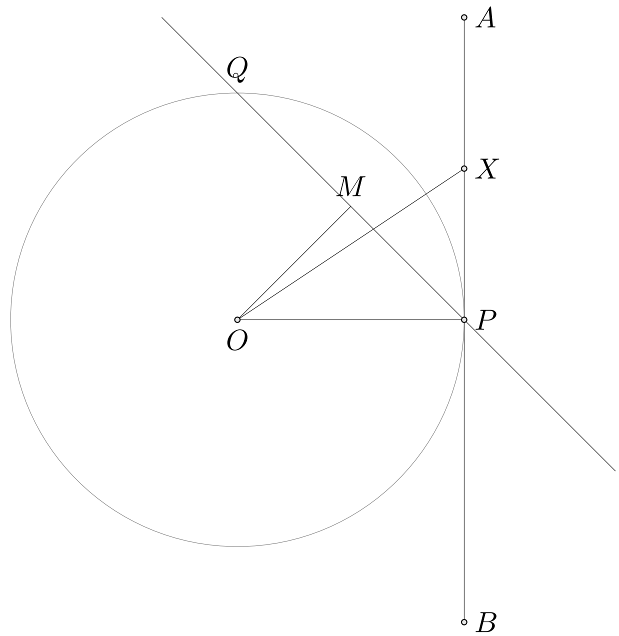


Figure 20:

Proof: Draw $APB \perp OP$ as in Fig. 20. If X is any point on the straight line APB different from P, then $\angle OPX$ is a right triangle with OX as its hypotenuse. Therefore $OX > OP$ as the radius of the circle. This means that X lies outside the given circle. This is true for every point X on the straight line APB except P. Hence the straight line AB touches the circle at P or in other words, the straight line through P perpendicular to the radius OP is a tangent to the circle at P. If any other straight line l through P is considered, let M be the foot of the perpendicular from O on l. Then as l is not perpendicular to OP, we see that $M \neq P$. On this straight line cut off MQ equal to PM (Fig. 4.13). Then by construction, OM is the perpendicular bisector of PQ; and therefore $OP = OQ$. This means that the point Q also lies on the given circle; and the straight line l cuts the circle at two distinct points P and Q. This says that l is not a tangent to the circle. Hence the theorem.

Theorem 9. If two tangents are drawn to a circle from an exterior point then (i) the lengths of the tangents are equal (ii) they subtend equal angles at the centre (iii) the angle between them is bisected by the straight line joining the point and the centre.

Proof. See Fig. 21. Let A be an exterior point to the circle with centre O and AP, AQ be two tangents from A to the circle touching the circle at P and Q respectively. Then it is required to prove that (i) $AP = AQ$ (ii) $\angle AOP = \angle AOQ$ (iii) $\angle PAO = \angle QAO$. As AP and AQ are the tangents to the circle at P and Q. We have $\angle APO = \angle AQO = 90°$. We note that the right-angled triangles OAP and OAQ are congruent (RHS theorem). Therefore $AP = AQ$, $\angle AOP = \angle AOQ$ and $\angle PAO = \angle QAO$.

Given a circle and a point A exterior to it, how many tangents to the circle can be drawn through A? The following theorem answers this question.

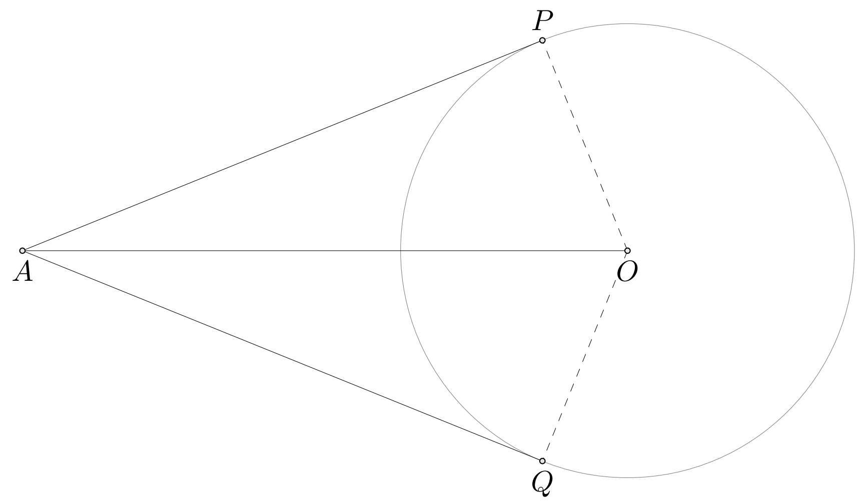


Figure 21:

Theorem 10. There are exactly two tangents from an exterior point to a given circle.

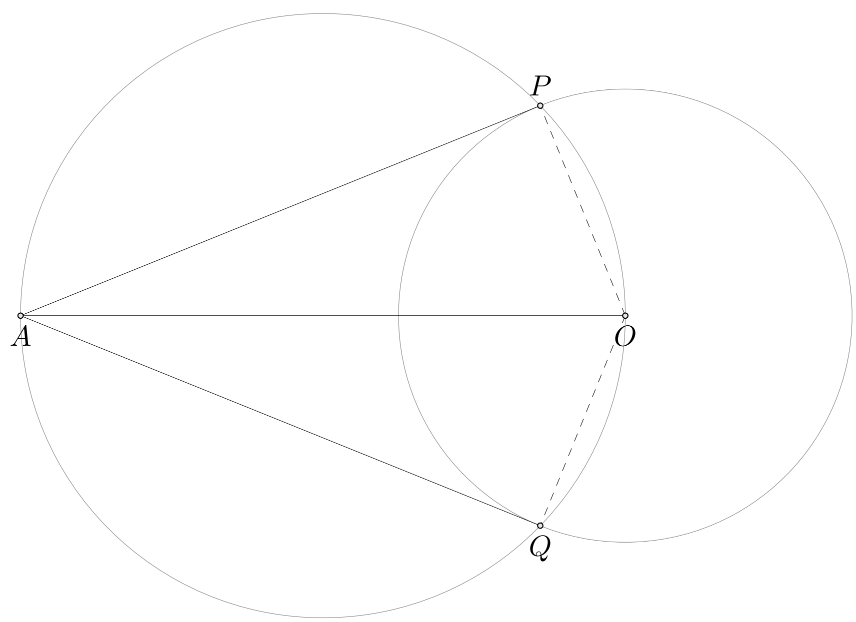


Figure 22:

Proof. Suppose P is the point of contact of a tangent to the circle from A. Then as $\angle APO = 90°$, P must lie on the circle AO as diameter (Theorem 7). Now, the circle on AO as diameter and the given circle cut exactly at two distinct points since A lies outside the given circle (Fig. 22). Therefore, the points of contact of the tangents from A to the given circle must be the two points of intersection of the circle on AO as diameter and the given circle. Thus there are exactly two tangents from an exterior point to a given circle.

We have already seen that if A lies on the circle, there is a unique tangent to the circle through A. If A lies inside the circle and AP is a tangent to the circle with P as its point of contact, then $\angle APO$ must be a right-angled triangle, right-angled at P. Therefore $AO^2 = AP^2 + OP^2$ and $AP^2 = AO^2 - OP^2$. But A lies inside the circle implies that $AO^2 - OP^2 < 0$. This gives $AP^2 < 0$ which is impossible since the square of any real number is always non-negative. Hence there is no tangent to the circle through an interior point of the circle.

Theorem 11. If two circles touch one another, then the point of contact lies on the straight line joining the centres.

Proof. Let two circles with centres A and B touch each other at P. It is required to prove that A, P, B are

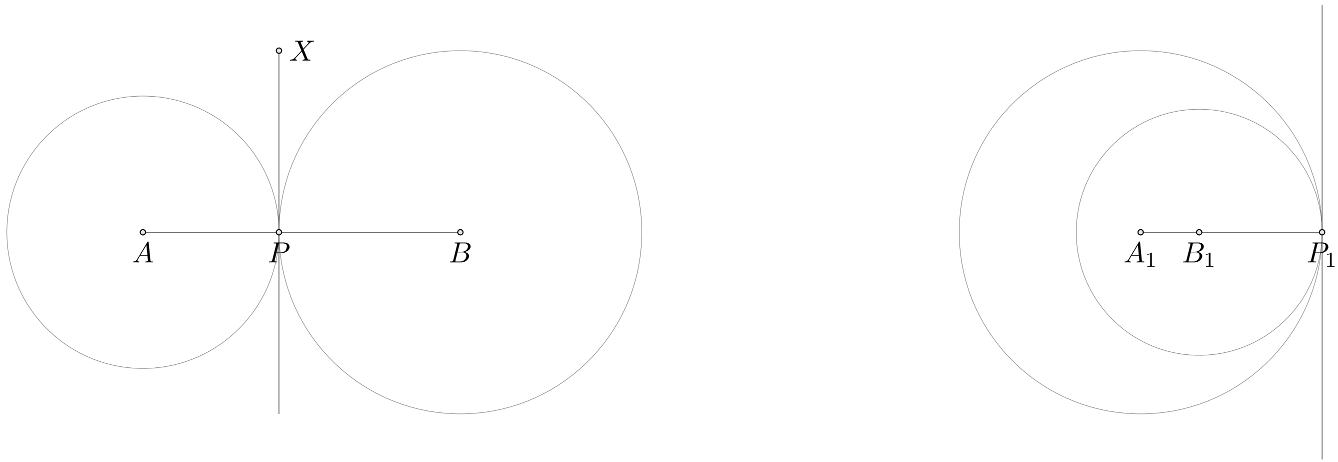


Figure 23:

collinear. Since the circles touch each other at P (Fig. 4.16), they have a common tangent PX at P. Hence PA and PB are both perpendicular to the common tangent XP at P. This is possible only if A, P and B are collinear and the straight line AB is perpendicular to the common tangent.

Corollary. If two circles touch each other, then the distance between their centres is equal to the sum or difference of their radii.

Proof. If A and B are the centres of two touching circles with radii r_1 and r_2 and if P is their point of contact, then by Theorem 11, A, P and B are collinear. When the circles touch externally, P lies in the line segment AB and we have $AP + PB = AB$ or $r_1 + r_2 = AB$. When they touch internally, P lies outside the segment AB and we have $AB = AP - BP$ or $BP - AP$ depending upon $AP \geq BP$ or $AP \leq BP$. Thus $AB = |AP \pm BP| = |r_1 \pm r_2|$ = sum or difference of their radii.

Remark. The perfect symmetry of a circle about its centre and about any of its diameters tells us that equal arcs subtend equal angles at the centre; and conversely if two arcs subtend equal angles at the centre then they are equal in length.

Theorem 12. In equal circles (or in the same circle) if two chords are equal, then they cut off equal arcs on the circles.

Theorem 13. In any circle. the angle between a tangent and a chord though the point of contact is equal to the angle in the alternate segment.

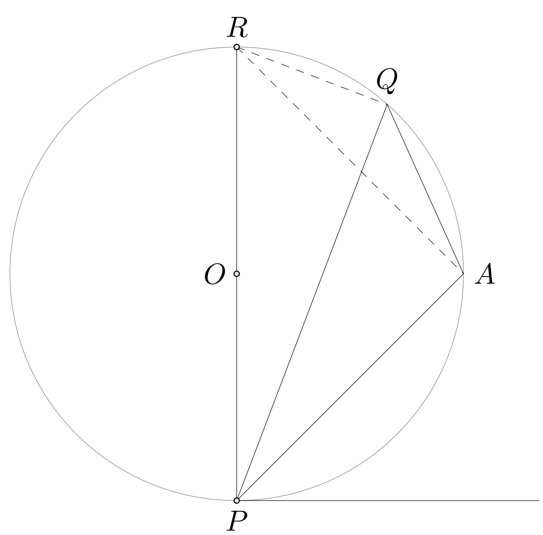
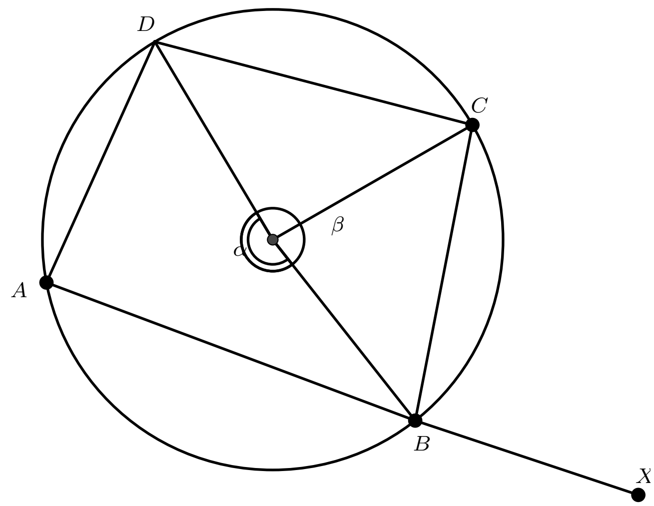


Figure 24:

Proof. Let PT be a tangent to a circle with centre O, the point of contact being P. Let AP be any chord through P. It is required to prove that $\angle APT = \angle AQP$ where Q is any point on the other segment determined by AP. Let PR be the diameter through P. Then $\angle PAR = 90°$ (angle in a semi-circle) and $\angle RPT = 90°$ (Fig. 24). Therefore $\angle ARP = 90° - \angle APR$ (from the right triangle RAP) $= \angle TPR - \angle APR = \angle APT$. But $\angle ARP = \angle AQP$ and hence $\angle APT = \angle AQP =$ angle in the alternate segment.

Theorem 14: A common tangent to two circles divides the straight line segment joining the centres, externally or internally in the ratio of their radii.

13.3 Cyclic Quadrilaterals



Definition Suppose we have a quadrilateral $ABCD$, it is called a cyclic quadrilateral if there exists a circles with the points A,B,C and D lying on it. In other words the points are said to be con cyclic.

Some properties of Cyclic quadrilaterals are as follows

1. Opposite angles of a cyclic quadrilateral are supplementary. The converse is also true.
2. Exterior angle of a cyclic quadrilateral is equal to the opposite interior angle.

Theorem: If AB and CD are any two chords of a circle meeting at a point P then $PA.PB = PC.PD$. This is known as the secant property of circle.

Proof: In $\triangle APC$ and $\triangle DPB$ we have

$$\angle APC = \angle DPB$$

$$\angle PDB = \angle PAC \quad \angle PAC = \text{ int. opp } \angle PDB)$$

$$\angle DBP = \angle ACP \quad \text{(reasons same as above)}$$

Hence the two triangles are similar. This gives

$$\frac{PA}{PD} = \frac{PC}{PB} \quad \text{or} \quad PA \cdot PB = PC \cdot PD.$$

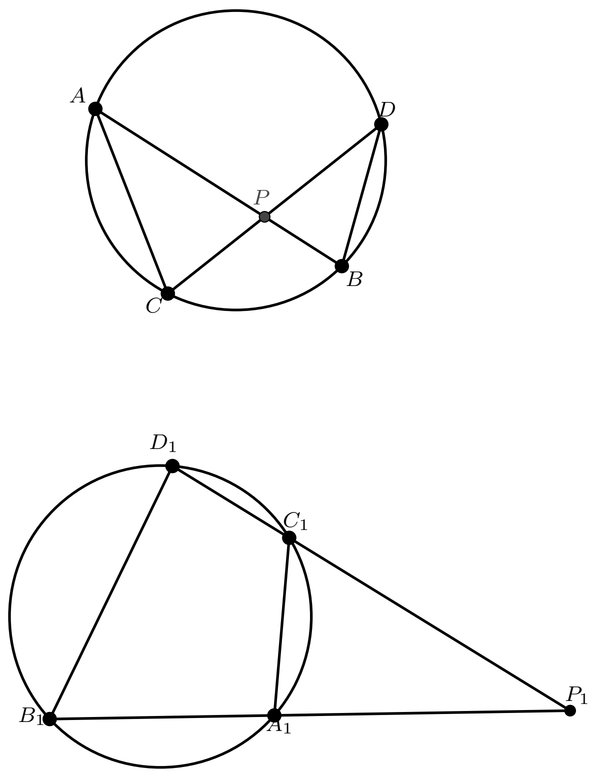


Figure 25:

Theorem: If P is any point on a chord AB (or AB produced) of a circle with centre O and radius r, then $AP \cdot PB = r^2 - OP^2$ or $PA \cdot PB = OP^2 - r^2$ according as P is within the circle or outside the circle.

Definition: If P is any point in the plane of a circle with centre O and radius r, the *power* of P with respect to the circle is defined as $OP^2 - r^2$. Thus if directed segments are used then $PA \cdot PB =$ Power of P with respect to the circle whenever P is a point on the chord AB (or AB produced).

13.4 Triangles Revisited

Theorem: Let ABC be a triangle, AD the altitude through A and AK the circumdiameter through A. Then $\angle DAK = \angle B - \angle C$. Further the angular bisector AX of $\angle A$ bisects $\angle DAK$.

Proof: We have

$$\angle ABC = \angle AKC \quad \text{(angles in the same segment).}$$

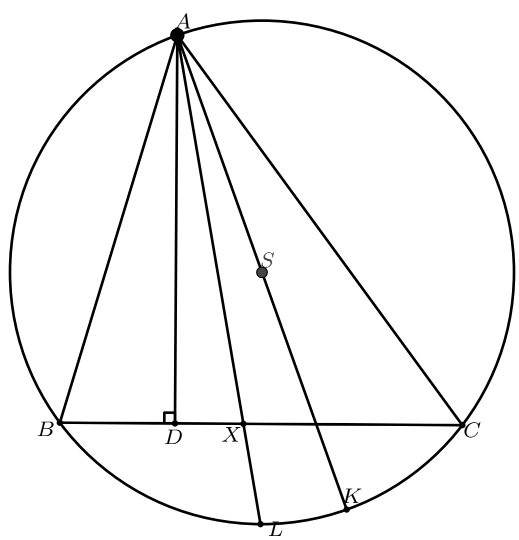
$$\angle BAD = 90^\circ - \angle ABC = 90^\circ - \angle AKC = \angle KAC$$

$$\angle DAK = \angle BAC - 2\angle BAD = \angle A - 2(90^\circ - \angle B) = \angle A + 2\angle B - 180^\circ = \angle B - \angle C \quad \text{(since } A + B + C = 180^\circ\text{).}$$

This proves the first part of the theorem. We have taken B, C both acute in The same proof works when one of B and C is obtuse. Let AXL be the angular bisector of $\angle A$. We have

$$\angle DAX = \frac{\angle A}{2} - \angle BAD = \frac{\angle A}{2} - \angle CAK = \angle XAK.$$

Thus AX also bisects $\angle DAK$.



Theorem: If m_a, m_b, m_c are the lengths of the medians of $\triangle ABC$, through A, B, C respectively then

$$2m_a^2 = b^2 + c^2 - \frac{a^2}{2},$$

$$2m_b^2 = c^2 + a^2 - \frac{b^2}{2} \quad \text{and} \quad 2m_c^2 = a^2 + b^2 - \frac{c^2}{2},$$

where a, b, c are the lengths of the sides BC, CA, AB of $\triangle ABC$.

Proof. Let AD be the median through A and AX the altitude through A. We use Pythagoras's theorem repeatedly.

We have

$$\begin{aligned} AB^2 &= AX^2 + XB^2 \\ &= (AD^2 - DX^2) + XB^2 \\ &= AD^2 + (DB - DX)^2 - DX^2 \\ &= AD^2 + DB^2 + 2DC.DX \end{aligned}$$

Similarly,

$$AC^2 = AD^2 + DC^2 + 2CD.DX$$

Adding we get

$$AB^2 + AC^2$$

or

$$2AD^2 = AB^2 + AC^2 - \frac{1}{2}(BC^2) \quad \text{as } DB = \frac{BC}{2}$$

i.e.,

$$2m_a^2 = b^2 + c^2 - \frac{a^2}{2}.$$

Similarly,

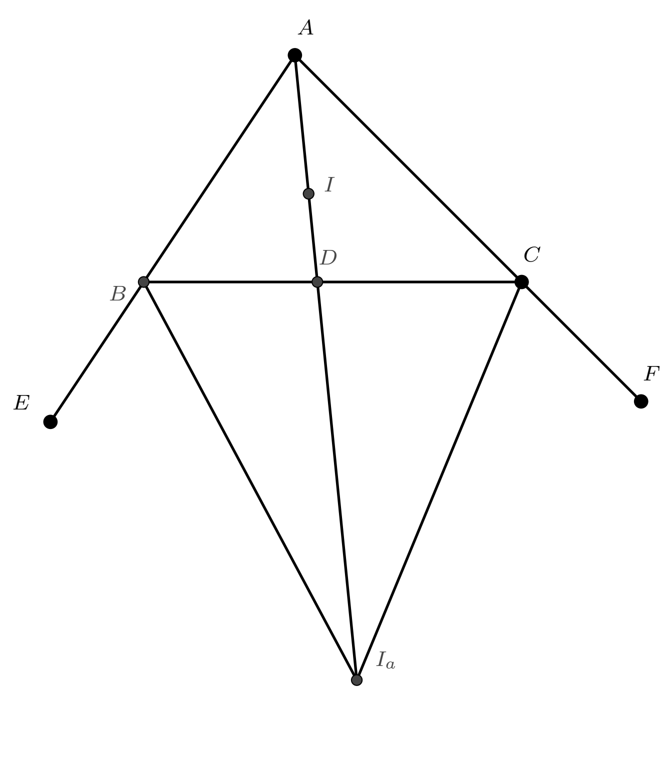
$$2m_b^2 = c^2 + a^2 - \frac{b^2}{2} \quad \text{and} \quad 2m_c^2 = a^2 + b^2 - \frac{c^2}{2}.$$

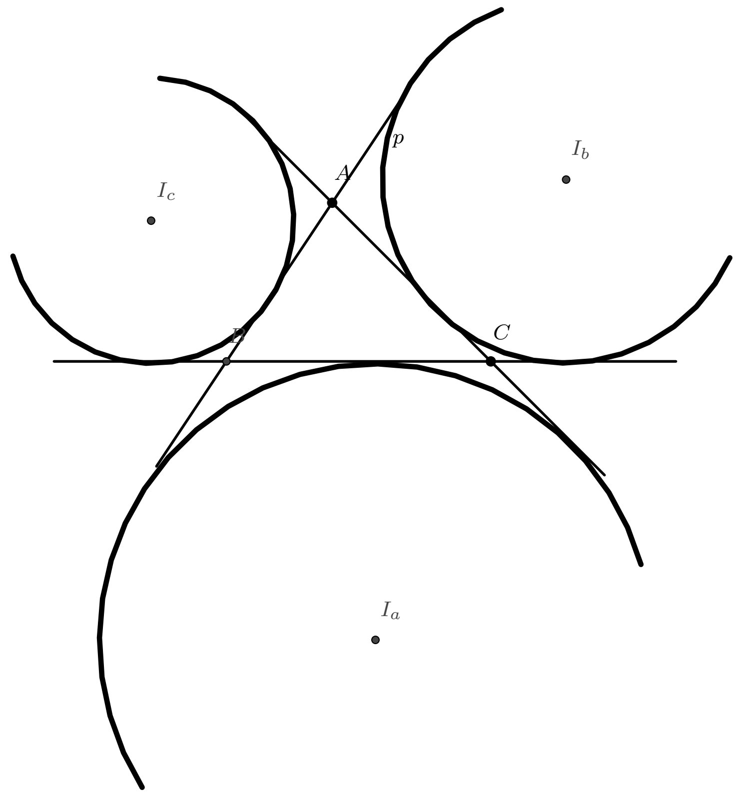
Theorem 30. The external bisectors of any two angles of a triangle are concurrent with the internal bisector of the third angle.

Proof. Let the external bisectors of $\angle B$ and $\angle C$ of $\triangle ABC$ meet at I_a (Fig. 4.40). Then the distances of I_a from BC and AB are equal as I_a lies on the external bisector of $\angle B$. Also I_a lies on the external bisector of $\angle C$ implies that the distance of I_a from BC and CA are equal. Thus I_a is at the same distance, say r_a, from the three sides of $\triangle ABC$. Hence I_a must lie on the internal bisector AI of $\angle A$.

The point I_a is called the *excentre* opposite to A. Similarly, the external bisectors of $\angle C$ and $\angle A$ meet the internal bisector of $\angle B$ at a point I_b called the excentre opposite to B; and the external bisectors of $\angle A$ and $\angle B$ meet the internal bisector of $\angle C$ at I_c, the excentre opposite to C.

We note that the incentre I is equidistant from the three sides BC, CA, AB of $\triangle ABC$. If r is the distance of I from the sides of $\triangle ABC$ then the circle with centre I and radius r touches all the three sides of the triangle and is inscribed in the triangle. It is called the *incircle* of $\triangle ABC$. The circle with centre I_a and radius r_a touches the sides BC, CA, AB of $\triangle ABC$. It touches BC at a point on the line segment BC, whereas it touches the other two sides CA, AB at points on CA, AB produced. The circles (I_a, r_a), (I_b, r_b), (I_c, r_c) are the three escribed circles known as the *excircles* opposite to A, B and C respectively. (See Fig. 4.41).





Theorem 31. The incentre I and the excentre I_a opposite to A divide the bisector AU harmonically, where U is the point of intersection of the internal bisector of $\angle A$ and BC.

Proof. It is required to prove that

$$\frac{AI}{IU} = \frac{AI_a}{UI_a}.$$

Consider $\triangle BAU$. Then we have

$$\frac{AI}{IU} = \frac{BA}{BU} = \frac{AI}{UI_a} \quad \text{since } BI \text{ and } BI_a \text{ are the bisectors of } \angle ABU \text{ of } \triangle ABC.$$

In fact, we have

$$\frac{BU}{UC} = \frac{c}{b} \quad \text{and} \quad \frac{BV}{CV} = \frac{c}{b}$$

$$\frac{BU}{BU+UC} = \frac{c}{c+b} \quad \text{or} \quad BU = BC \cdot \frac{c}{c+b} = \frac{ac}{b+c},$$

$$\frac{BV}{CV-BV} = \frac{c}{b-c} \quad \text{or} \quad BV = BC \cdot \frac{c}{b-c} = \frac{ac}{b-c}.$$

$$\frac{AI}{IU} = \frac{BA}{BU} = \frac{c}{ac(b+c)} = \frac{b+c}{a} \quad \text{and}$$

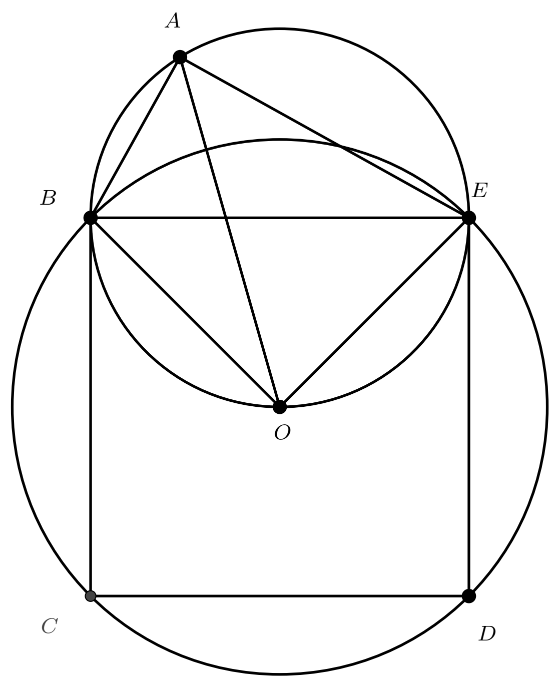
$$\frac{AI_c}{I_cV} = \frac{BA}{BV} = \frac{c}{ac(b-c)} = \frac{b-c}{a}.$$

13.5 Some Solved Examples

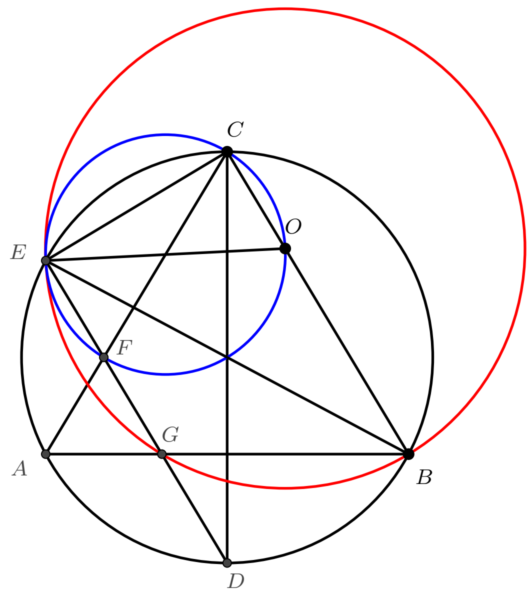
Example 1: Let $ABCDE$ be a convex pentagon such that $BCDE$ is a square with center O and $\angle A = 90°$. Prove that $\overline{AO}$ bisects $\angle BAE$.

Solution: Observe that $\angle BAE = 90°$ and $\angle BOE = 90°$. It follows that $ABOE$ is cyclic. So $\angle OAE = \angle OBE = 45°$ and $\angle BAO = \angle BEO = 45°$. It follows that $\angle OAE = \angle BAO = 45°$, as needed.

The condition that $ABCDE$ is convex ensures that A lies on the opposite side of $\overline{BE}$ as O, so there is no need to worry about configuration issues and it is fine to just use standard angles.



Example 2: In triangle ABC with $CA = CB$, point E lies on the circumcircle of ABC such that $\angle ECB = 90°$. The line through E parallel to CB intersects CA in F and AB in G. Prove that the centre of the circumcircle of triangle EGB lies on the circumcircle of triangle ECF.



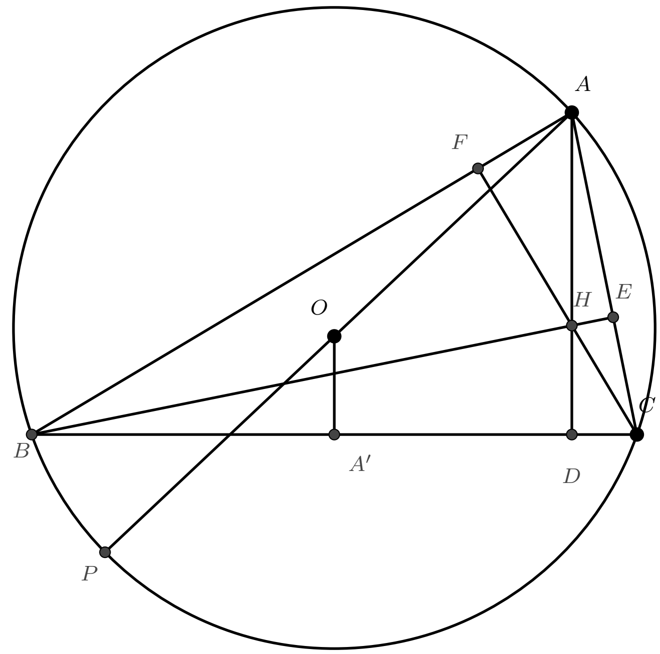
Solution: We have $FG = FA$ since FG is parallel to BC. But also $\triangle GAE$ is a right angle triangle since $\angle BCE = 90^\circ$ and $BCEA$ is a cyclic quadrilateral. Thus, if F' is the midpoint of GE, then $\angle GAF = \angle FGA = \angle F'GA = \angle GAF'$ which implies $F \equiv F'$. Thus, F is the midpoint of GE.

If O is the circumcenter of $\triangle EBG$, then

$$\angle FOE = \angle GBE = \angle ABE = \angle ACE = \angle FCE.$$

Thus, we get $\angle FOE = \angle FCE$ as desired.

Example 3: If H is the orthocenter of $\triangle ABC$ and AP is a circumdiameter, then PH and BC bisect each other. If $OA' \perp BC$, where O is the circumcenter of $\triangle ABC$, then $AH = 2OA'$.



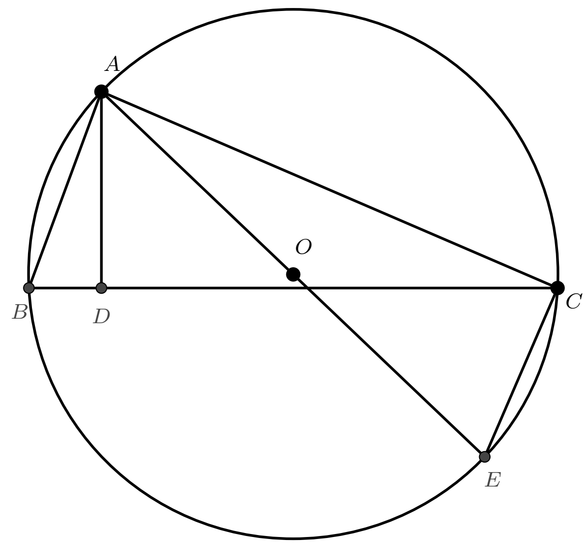
Solution: As in the figure above, $BE \perp AC$ and $PC \perp AC$. Hence $BH \parallel PC$. Similarly, $BP \parallel HC$. Thus $BPCH$ is a parallelogram and so its diagonals BC and PH bisect each other at A'. Next, A' is the midpoint of PH. Hence from $\triangle APH$, we get $AH = 2OA'$.

Example 4: If in $\triangle ABC$, AD is the altitude and AE is the diameter of the circumcircle through A, then

$$AB \cdot AC = AD \cdot AE.$$

Proof: As shown in the figure below $\triangle ABD \sim \triangle AEC$ so that

$$\frac{AB}{AE} = \frac{AD}{AC}.$$



Example 6: Three circles C_1, C_2, C_3 with radii r_1, r_2, r_3 $(r_1 < r_2 < r_3)$ respectively are given. They are placed such that C_2 lies to the right of C_1 and touches it externally; C_3 lies to the right of C_2 and touches it externally. Further, there exist two straight lines each of which is a direct common tangent simultaneously to all the three circles. Find r_2 in terms of r_1 and r_3.

Solution. Let the given common tangents l, m meet at P. We observe that the centres, say A, B, C of the given circles will lie on the angle-bisector of the angle between l and m. Let these circles touch m at D, E, F respectively. Draw $AK \perp BE$. We have

$$\begin{aligned} DE = AK &= \sqrt{(AB)^2 - (BK)^2} \\ &= \sqrt{(r_2 + r_1)^2 - (r_2 - r_1)^2} = 2\sqrt{r_1 r_2}. \end{aligned}$$

Similarly $EF = 2\sqrt{r_2 r_3}$. Let $m\angle APD = \theta$ and $PD = x$. Then

$$\tan\theta = \frac{AD}{PD} = \frac{BE}{PE} = \frac{CF}{PF} = \frac{r_1}{x} = \frac{r_2}{x + 2\sqrt{r_1 r_2}} = \frac{r_3}{x + 2\sqrt{r_1 r_2} + \sqrt{r_2 r_3}}.$$

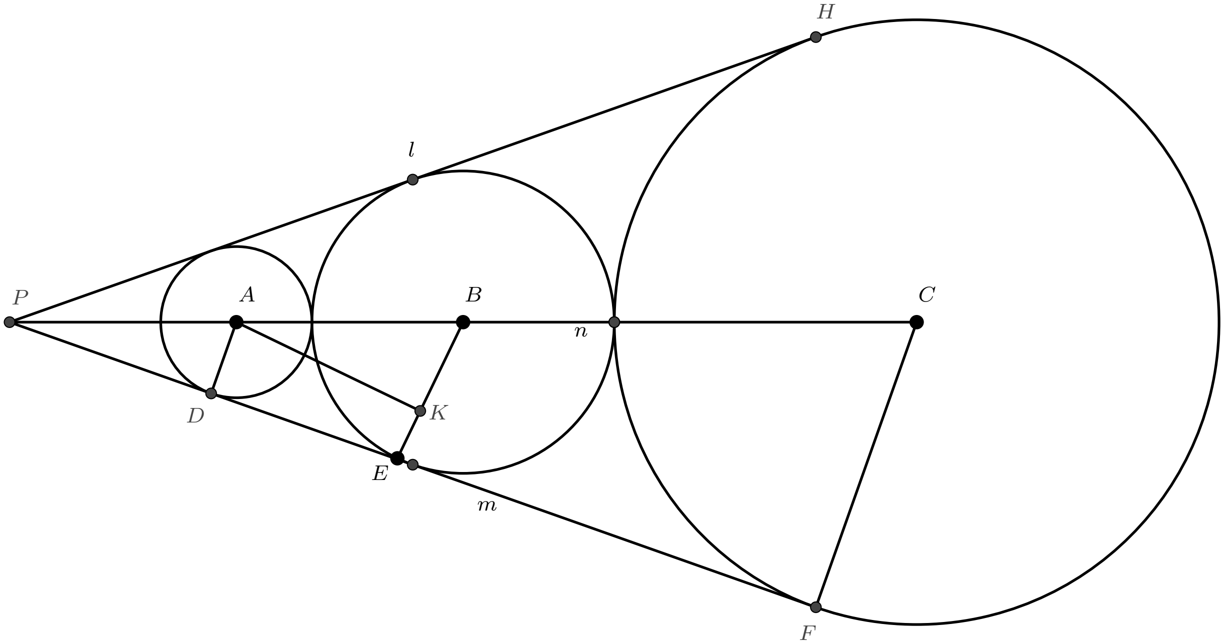
Hence,

$$\frac{r_2 - r_1}{2\sqrt{r_1 r_2}} = \frac{r_3 - r_2}{2\sqrt{r_2 r_3}}.$$

Thus, $\sqrt{r_3(r_2 - r_1)} = \sqrt{r_1(r_3 - r_2)}$. Therefore,

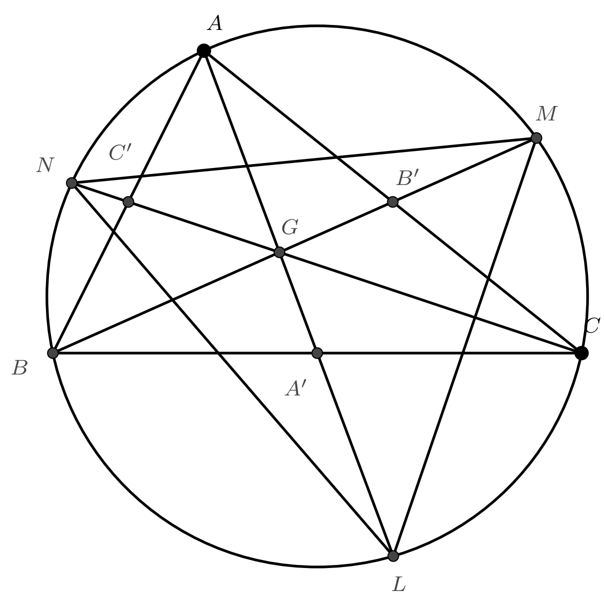
$$r_2(\sqrt{r_3} + \sqrt{r_1}) = \sqrt{r_1 r_3(\sqrt{r_1} + \sqrt{r_3})}.$$

Hence, $r_2 = \sqrt{r_1 r_3}$.



Example 7: Let ABC be a triangle with unequal sides. The medians of $\triangle ABC$, when extended, intersect its circumcircle in points L, M, N. If L lies on the median through A and $LM = LN$, prove that

$$2BC^2 = CA^2 + AB^2.$$



Solution. We note that the triangles AGB and MGL are similar because $\angle GAB = \angle GML$ (same segment) and $\angle AGB = \angle MGL$. Hence

Similarly, $\triangle AGC \sim \triangle NGL$ and so

$$\frac{AG}{NG} = \frac{AC}{NL} \text{ i.e. } AG = NG \cdot \frac{b}{NL}. \tag{2}$$

Also, by data, $LM = LN$. Hence by (1), (2) we get

$$\frac{MG}{GN} = \frac{b}{c}. \tag{3}$$

Since the chord BM and CN intersect at G, we have

$$BG \cdot GM = CG \cdot GN.$$

So by (3), $BG \cdot b = CG \cdot c$ and so

$$\frac{2}{3}BB' \cdot b = \frac{2}{3}CC' \cdot c \text{ or } 2BB'^2 \cdot b^2 = 2CC'^2 \cdot c^2.$$

So, applying Apollonius' theorem twice we get

$$b^2(c^2 + a^2 - 2AB^2) = c^2(a^2 + b^2 - 2AC'^2),$$

$$b^2(c^2 + a^2 - \frac{1}{2}b^2) = c^2(a^2 + b^2 - \frac{1}{2}c^2),$$

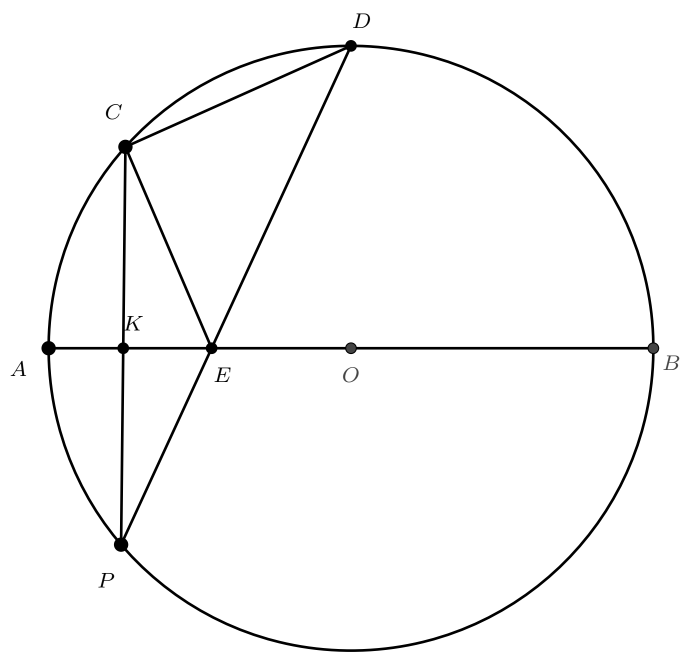
$$a^2(b^2 - c^2) = \frac{1}{2}(b^4 - c^4),$$

$$2a^2 = b^2 + c^2, \text{ as } b \neq c.$$

Example 8: Let ω be a semicircle with AB as the bounding diameter and let CD be a variable chord of the semicircle of constant length such that C, D lie in the interior of the arc AB. Let E be a point on AB such that CE and DE are equally inclined to the line AB. Prove that

(a) the measure of $\angle CED$ is a constant;

(b) the circumcircle of triangle CED passes through a fixed point.



Solution: Construct the circle with AB as diameter and let this circle be Ω. Draw $CK \perp AB$ with K on AB. Let CK produced meet Ω again in P. Join EP. Observe that

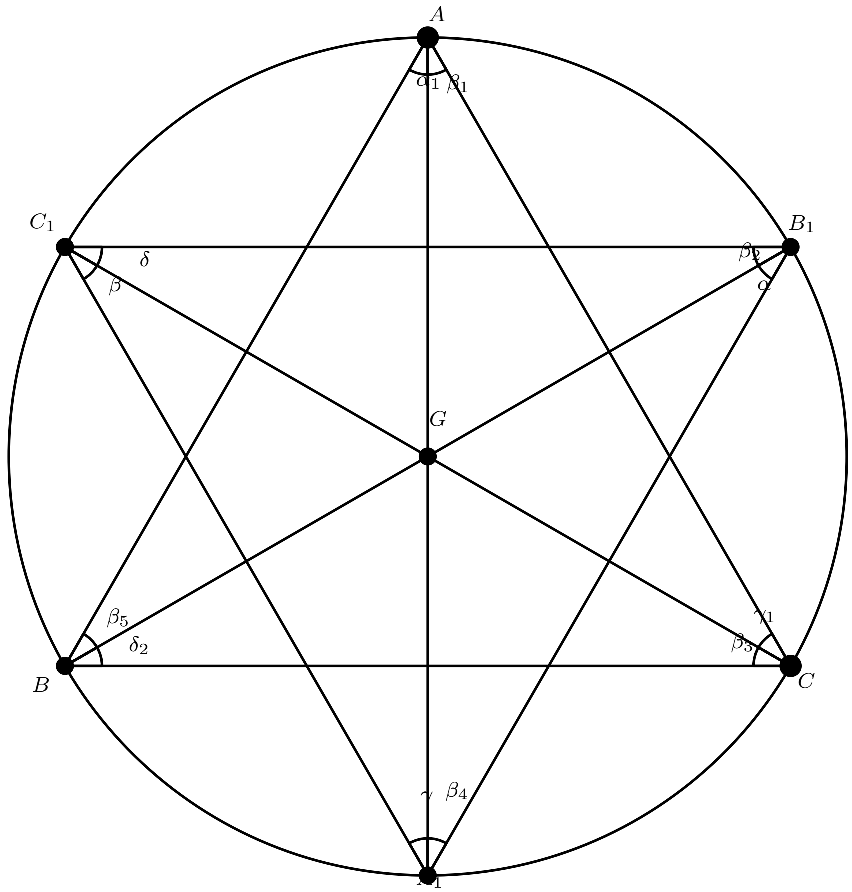
$$\angle DEB = \angle CEK = \angle PEK.$$

Hence $\angle PEK + \angle CEK + \angle CED = 180°$. Therefore P, E, D are collinear. This shows that

$$\angle CED = 2\angle CPD$$

is a constant. If O is the centre of Ω then we get $\angle COD = 2\angle CPD = \angle CED$. Hence the circumcircle of triangle CED passes through O which is a fixed point.

Example 9: Let ABC be a triangle with circumcircle Ω and let G be the centroid of triangle ABC. Extend AG, BG, and CG to meet the circle Ω again in A_1, B_1, and C_1, respectively. Suppose $\angle BAC = \angle A_1B_1C_1$, $\angle ABC = \angle A_1C_1B_1$, and $\angle ACB = \angle B_1A_1C_1$. Prove that ABC and $A_1B_1C_1$ are equilateral triangles.



Solution: Let $\angle BAA_1 = \alpha$ and $\angle A_1AC = \beta$. Then $\angle BB_1A_1 = \alpha$. Using that angles at A and B_1 are same, we get $\angle BB_1C_1 = \beta$. Then $\angle C_1CB = \beta$. If $\angle ACC_1 = \gamma$, we see that $\angle C_1AA_1 = \gamma$. Therefore $\angle AA_1B_1 = \beta$. Similarly, we see that $\angle B_1BA = \alpha$ and $\angle B_1C_1C = \delta$.

Since $\angle FBG = \angle BCG = \beta$, it follows that FB is tangent to the circumcircle of $\triangle BGC$ at B. Therefore $FB^2 = FG \cdot FC$. Since $FA = FB$, we get $FA^2 = FG \cdot FC$. This implies that FA is tangent to the circumcircle of $\triangle AGC$ at A. Therefore $\alpha = \angle GAF = \angle GCA = \gamma$. A similar analysis gives $\alpha = \delta$.

It follows that all the angles of $\triangle ABC$ are equal and all the angles of $\triangle A_1B_1C_1$ are equal. Hence ABC and $A_1B_1C_1$ are equilateral triangles.

Exercises

1. In a triangle ABC, let H be the orthocenter, and let D, E, F be the feet of altitudes from A, B, C to the opposite sides, respectively. Let L, M, N be midpoints of segments AH, EF, BC, respectively. Let X, Y be feet of altitudes from L, N onto the line DF. Prove that XM is perpendicular to MY.

2. Let ABC be an acute-angled triangle with $AB < AC$. Let I be the incenter of triangle ABC, and let D, E, F be the points at which its incircle touches the sides BC, CA, AB, respectively. Let BI, CI meet the line EF at Y, X, respectively. Further assume that both X and Y are outside the triangle ABC. Prove that

(i) B, C, Y, X are concyclic; and

(ii) I is also the incenter of triangle DYX.

3. Let ABC be a triangle with integer sides in which $AB < AC$. Let the tangent to the circumcircle of triangle ABC at A intersect the line BC at D. Suppose AD is also an integer. Prove that $\gcd(AB, AC) > 1$.

4. Let AOB be a given angle less than $180°$ and let P be an interior point of the angular region determined by $\angle AOB$. Show, with proof, how to construct, using only ruler and compasses, a line segment CD passing through P such that C lies on the ray OA and D lies on the ray OB, and $CP : PD = 1 : 2$.

5. Let Ω be a circle with a chord AB which is not a diameter. Let Γ_1 be a circle on one side of AB such that it is tangent to AB at C and internally tangent to Ω at D. Likewise, let Γ_2 be a circle on the other side of AB such that it is tangent to AB at E and internally tangent to Ω at F. Suppose the line DC intersects Ω at $X \neq D$ and the line FE intersects Ω at $Y \neq F$. Prove that XY is a diameter of Ω.

6. Let ABC be a triangle with centroid G. Let the circumcircles of $\triangle AGB$ and $\triangle AGC$ intersect the line BC in X and Y respectively, which are distinct from B, C. Prove that G is the centroid of $\triangle AXY$.

7. Let ABC be a right-angled triangle with $\angle B = 90°$. Let I be the incenter of ABC. Draw a line perpendicular to AI at I. Let it intersect the line CB at D. Prove that CI is perpendicular to AD and prove that $ID = \sqrt{b(b-a)}$ where $BC = a$ and $CA = b$.

8. Let ABC be a right-angled triangle with $\angle B = 90°$. Let I be the incenter of ABC. Let AI extended intersect BC in F. Draw a line perpendicular to AI at I. Let it intersect AC in E. Prove that $IE = IF$.

9. Let ABC be a triangle and D be the midpoint of BC. Suppose the angle bisector of $\angle ADC$ is tangent to the circumcircle of triangle ABD at D. Prove that $\angle A = 90°$.

10. Let ABC be a right-angled triangle with $\angle B = 90°$. Let I be the incenter of ABC. Extend AI and CI; let them intersect BC in D and AB in E respectively. Draw a line perpendicular to AI at I to meet AC in J; draw a line perpendicular to CI at I to meet AC in K. Suppose $DJ = EK$. Prove that $BA = BC$.

11. Let ABC be a right triangle with $\angle B = 90°$. Let E and F be respectively the midpoints of AB and AC. Suppose the incenter I of triangle ABC lies on the circumcircle of triangle AEF. Find the ratio BC/AB.

12. Σ in the plane intersect at two distinct points A and B, and the center of Σ lies on Γ. Let points C and D be on Γ and Σ, respectively, such that C, B, and D are collinear. Let point E on Σ be such that DE is parallel to AC. Show that $AE = AB$.

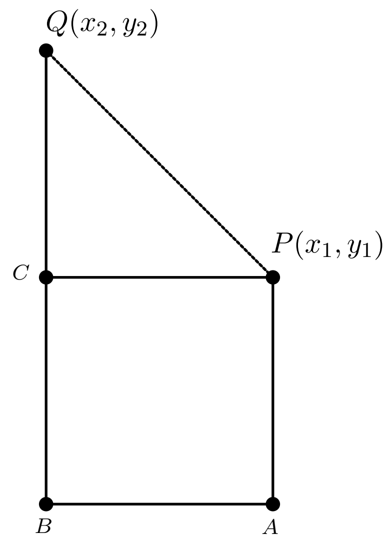
13. In a cyclic quadrilateral $ABCD$, let the diagonals AC and BD intersect at X. Let the circumcircles of triangles AXD and BXC intersect again at Y. If X is the incenter of triangle ABY, show that $\angle CAD = 90°$.

14. Let ABC be a triangle with circumcircle Γ and incenter I. Let the internal angle bisectors of $\angle A$, $\angle B$, and $\angle C$ meet Γ in A', B', and C' respectively. Let $B'C'$ intersect AA' in P and AC in Q, and let BB' intersect AC in R. Suppose the quadrilateral $PIRQ$ is a kite; that is, $IP = IR$ and $QP = QR$. Prove that ABC is an equilateral triangle.

15. Two circles Γ and Σ, with centers O and O', respectively, are such that O' lies on Γ. Let A be a point on Σ and M the midpoint of the segment AO'. If B is a point on Σ different from A such that AB is parallel to OM, show that the midpoint of AB lies on Γ.

14 Coordinate Geometry

Descartes (1596 – 1650) re-created Geometry by using algebraic formulations and methods. The Geometry that arose thus has been called *Cartesian Geometry* for that very reason. It is also called *Analytic Geometry* or *Coordinate Geometry* for reasons which will be obvious in this Chapter. The application of algebra to geometry which became the fashion after Descartes's time may well be named as the key step for all exploration of natural phenomena by mathematics in the past three centuries.



The veritcal line as you know is known as the y-axis and the horizontal line is known as the x-axis and the point of their intersection is known as the origin denoted by $O(0,0)$. Each point is uniquely determined by a set of coordinates. The x-coordinate known as the abscissa which is the horizontal distance of the point from the origin and the y-coordinate known as the ordinate which is the vertical distance of the point from the origin. Thus any point in the $X - Y$ plane looks like some $P(x, y)$.

Often in geometry we are interested in the distance between points. Consider now two points $P(x_1, y_1)$ and $Q(x_2, y_2)$ with respect to our fixed rectangular axes $x'Ox$ and $y'Oy$. Then $OA = x_1$, $AP = y_1$, $OB = x_2$ and $BQ = y_2$. (Note that the coordinates of a point could be positive or negative). From the right-angled triangle PCQ we get

$$PQ^2 = PC^2 + CQ^2 = (OA \pm OB)^2 + (BQ - BC)^2 = (x_1 - x_2)^2 + (y_1 - y_2)^2$$

Example 1. Show that the triangle whose vertices are $A(-3,-4)$, $B(2,6)$, and $C(-6,10)$ is right-angled.

Solution: We observe that

$$AB^2 = (-3-2)^2 + (-4-6)^2 = 125$$

$$BC^2 = (2-(-6))^2 + (6-10)^2 = 80$$

$$CA^2 = (-6-(-3))^2 + (10-(-4))^2 = 205$$

Thus $CA^2 = 205 = 125 + 80 = AB^2 + BC^2$ and hence $\triangle ABC$ is right-angled at B.

Example 4. Find the circumcentre and circumradius of the triangle ABC whose vertices are $A(1,1)$, $B(2,-1)$, and $C(3,2)$.

Solution. Let $S(x, y)$ be the circumcentre and r be the circumradius of $\triangle ABC$. Then $AS^2 = BS^2 = CS^2 = r^2$. This gives

$$(x-1)^2 + (y-1)^2 = (x-2)^2 + (y+1)^2 = (x-3)^2 + (y-1)^2 = r^2.$$

This in turn gives

$$-2x - 2y + 2 = -4x + 2y + 5 \quad \Rightarrow \quad 2x - 4y = 3$$

$$-4x + 2y + 5 = -6x - 4y + 13 \quad \Rightarrow \quad 2x + 6y = 8$$

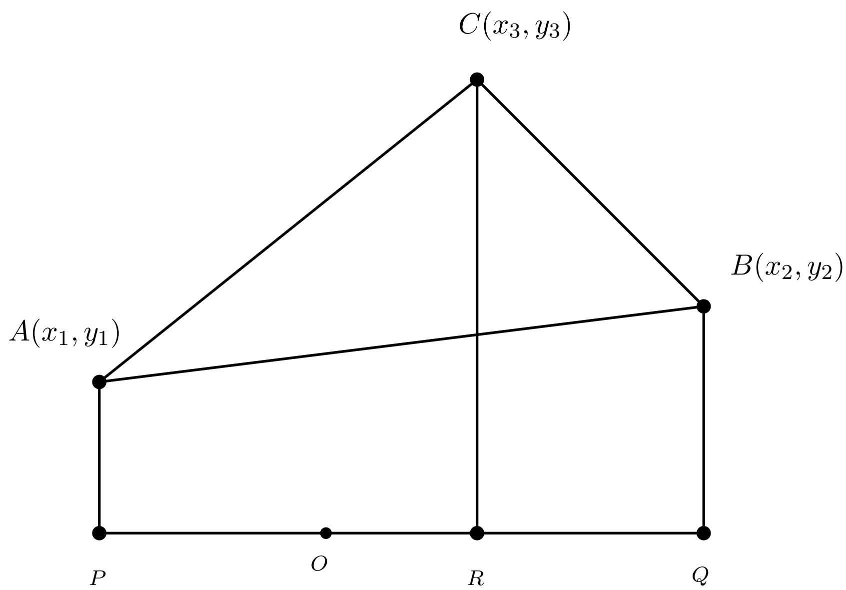
Solving, we get $x = 5/2$, $y = 1/2$. Therefore S is $(5/2, 1/2)$ and the circumradius is

$$r = \sqrt{AS^2} = \sqrt{\left(\frac{5}{2} - 1\right)^2 + \left(\frac{1}{2} - 1\right)^2} = \frac{\sqrt{10}}{2} \text{ units.}$$

To find the area of the triangle ABC with vertices $A(x_1, y_1)$, $B(x_2, y_2)$, and $C(x_3, y_3)$

We have area of ABC = area of trapezium $APRC$ + area of trapezium $CRQB$ - area of trapezium $APQB$

$$\begin{aligned}
&= \frac{1}{2}(AP + CR)PR + \frac{1}{2}(CR + QB)RQ - \frac{1}{2}(AP + QB)PQ \\
&= \frac{1}{2}(y_1 + y_3)(x_3 - x_1) + \frac{1}{2}(y_2 + y_3)(x_2 - x_3) - \frac{1}{2}(y_1 + y_2)(x_2 - x_1) \\
&= \frac{1}{2}\{x_1(y_2 - y_3) + x_2(y_3 - y_1) + x_3(y_1 - y_2)\}
\end{aligned}$$



Section Formula

$$\frac{m}{n} = \frac{AC}{CB} = \frac{AD}{CE} = \frac{x - x_1}{x_2 - x}$$

and this gives

$$x = \frac{mx_2 + nx_1}{m + n}.$$

Similarly,

$$\frac{m}{n} = \frac{AC}{CB} = \frac{DC}{EB} = \frac{y - y_1}{y_2 - y}$$

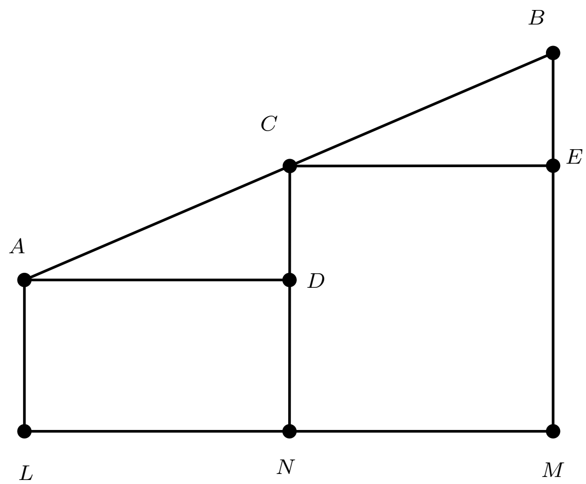
gives

$$y = \frac{my_2 + ny_1}{m + n}$$

.

Therefore, the required point C is

$$C\left(\frac{mx_2 + nx_1}{m+n}, \frac{my_2 + ny_1}{m+n}\right).$$



Example 3: To find the incentre of the triangle ABC with vertices $A(x_1, y_1)$, $B(x_2, y_2)$ and $C(x_3, y_3)$.

Solution: The incentre I of the triangle ABC is the point of concurrence of the angular bisectors of the internal angles of triangle ABC. Let AD, BE and CF be the internal angular bisectors of $\triangle ABC$, meeting the opposite sides at D, E, F . By the bisector theorem, we have $BD/DC = AB/AC = c/b$; $CE/EA = a/c$ and $AF/FB = b/a$ where a, b, c stand, as usual, for the lengths of the sides BC, CA, AB respectively. Hence D has coordinates

$$D = \left(\frac{cx_3 + bx_2}{c+b}, \frac{cy_3 + by_2}{c+b}\right) \text{ (using the section formula)}$$

Again in $\triangle ABD$, the angular bisector BI meets AD at I.

$$\frac{AI}{ID} = \frac{AB}{BD}. \text{ Now } \frac{BD}{DC} = \frac{c}{b} \text{ gives}$$

$$\frac{BD}{BD + DC} = \frac{c}{c+b} \text{ or } \frac{BD}{a} = \frac{c}{c+b}$$

$$\therefore \frac{AI}{ID} = \frac{c+b}{a}$$

Using the section formula once more we get

$$I = \left(\frac{(c+b)\left(\frac{cx_3+bx_2}{c+b}\right) + ax_1}{c+b+a}, \frac{(c+b)\left(\frac{cy_3+by_2}{c+b}\right) + ay_1}{c+b+a}\right)$$

$$= \left(\frac{ax_1 + bx_2 + cx_3}{a+b+c}, \frac{ay_1 + by_2 + cy_3}{a+b+c}\right)$$

14.1 Exercise 1

1. Prove that $(4, -4)$, $(-2, 4)$ and $(6, 10)$ are the vertices of an isosceles triangle.

2. Prove that $P(6, 2)$ is collinear with $A(-2, 2)$ and $B(12, 5)$; find the ratio in which P divides AB.

4. Show that $(2, -1)$ is the centre of the circumcircle of $\triangle ABC$, where A is $(-3, -1)$, B is $(-1, 3)$ and C is $(6, 2)$. Find the circumradius.

5. Prove that the lines joining the midpoints of the opposite sides of a quadrilateral bisect one another.

6. Show that $(7, 5)$ divides AB and CD in the same ratio where A is $(1, 2)$; B is $(5, 4)$; C is $(-5, -1)$ and D is $(3, 3)$.

7. If G is the centroid of $\triangle ABC$, prove that

1. $AB^2 + BC^2 + CA^2 = 3(GA^2 + GB^2 + GC^2)$
2. $OA^2 + OB^2 + OC^2 = GA^2 + GB^2 + GC^2 + 3GO^2$ (where O is any point in the plane ABC).

8. Find the incentre of the triangle whose vertices are $(0, 0)$, $(20, 15)$, and $(36, 15)$.

9. In $\triangle ABC$, D is the midpoint of BC. Prove that $AB^2 + AC^2 = 2AD^2 + 2DC^2$.

10. If O is the origin and A, B are the points (x_1, y_1) and (x_2, y_2), prove that

$$OA \cdot OB \cos \angle AOB = x_1 x_2 + y_1 y_2.$$

11. A point P moves so that its distance from the point $(-1, 0)$ is always three times its distance from $(0, 2)$. Find the locus of P.

12. If A is $(a, 0)$ and B is $(-a, 0)$, find the locus of P when

1. $PA^2 - PB^2 = 2k^2 =$ constant.
2. $PA + PB = c =$ constant.
3. $PB^2 + PC^2 = 2PA^2$ where C is $(c, 0)$.

14.2 Straight Lines

Equation of a straight line passing through two given points.
Let $A(x_1, y_1)$ and $B(x_2, y_2)$ be the given two points and let $P(x', y')$ be any point on the straight line. In the adjoining figure, the triangles BRA and ASP are similar.

$$\frac{AS}{BR} = \frac{PS}{AR} \quad \text{and hence} \quad \frac{x' - x_1}{x_1 - x_2} = \frac{y' - y_1}{y_1 - y_2}$$

Also conversely if (x', y') satisfies $\frac{x'-x_1}{x_1-x_2} = \frac{y'-y_1}{y_1-y_2}$ then (x', y') should lie on AB. In other words, the equation to the straight line AB joining the given points $A(x_1, y_1)$ and $B(x_2, y_2)$ is given by

$$\frac{x - x_1}{x_1 - x_2} = \frac{y - y_1}{y_1 - y_2}$$

Equation of a straight line in terms of the intercepts it makes with the coordinate axes.

Let L be a straight line making intercepts $OA = a$ and $OB = b$ on the coordinate axes. In our figure (Fig. 7.21), we have $a > 0$, $b > 0$. If $a < 0$, the corresponding point $A(a, 0)$ will be on the negative x-axis. Similarly if $b < 0$ the corresponding point $(0, b)$ will be on the negative y-axis. If L makes intercepts a and b on the x and y axes respectively, then L passes through $(a, 0)$ and $(0, b)$. Therefore the equation to the straight line L is

$$\frac{x - a}{a - 0} = \frac{y - 0}{0 - b} \quad \text{or} \quad \frac{x}{a} - 1 = \frac{y}{b} \quad \text{or} \quad \frac{x}{a} + \frac{y}{b} = 1.$$

Note. The equation of the straight line L making intercepts a and b can be directly derived, without using the 2-point formula.

Let $P(x, y)$ be any point on AB, and let $PM \perp OX$ as in Fig. 7.22. The triangles AOB and AMP are similar.

$$\frac{OM}{OA} = \frac{BP}{BA} \quad \text{or} \quad \frac{x}{a} = \frac{PB}{AB}$$

and

$$\frac{PM}{BO} = \frac{AP}{AB} \quad \text{gives} \quad \frac{y}{b} = \frac{AP}{AB}.$$

Adding we get

$$\frac{x}{a} + \frac{y}{b} = \frac{AP + PB}{AB} = 1.$$

We have taken P between A and B, the reader may check the validity of the equation in all the other cases. Thus, equation of the straight line AB is

$$\frac{x}{a} + \frac{y}{b} = 1.$$

Again, $P(x, y)$ lies on AB if and only if the area of the triangle PAB is zero.

$$0 = x(0 - b) + a(b - y) + 0(y - 0) \quad \text{i.e.} \quad bx + ay = ab$$

Dividing by ab,

$$\frac{x}{a} + \frac{y}{b} = 1.$$

Example 2. Find the equation of the straight line when the portion of it intercepted between the axes is divided by the point $(3, 1)$ in the ratio $1 : 3$.

Solution. Let the required straight line meet the x-axis at $A(a, 0)$ and meet the y-axis at $B(0, b)$. It is given that the point $C(3, 1)$ divides AB or BA in the ratio $1 : 3$. Therefore by the section formula, C must be the point

$$\left(\frac{1 \cdot a + 3 \cdot 0}{4}, \frac{1 \cdot b + 3 \cdot 0}{4}\right) = \left(\frac{a}{4}, \frac{b}{4}\right) \quad \text{if} \quad \frac{AC}{CB} = \frac{1}{3}$$

or the point

$$\left(\frac{1 \cdot a + 3 \cdot 0}{4}, \frac{1 \cdot b + 3 \cdot 0}{4}\right) = \left(\frac{a}{4}, \frac{b}{4}\right) \quad \text{if} \quad \frac{BC}{CA} = \frac{1}{3}$$

$C(3, 1) = \left(\frac{3a}{4}, \frac{b}{4}\right)$ gives $a = 4, b = 4$ and $C(3, 1) = \left(\frac{a}{4}, \frac{3b}{4}\right)$ gives $a = 12, b = 4/3$. Hence the required line is either

$$\frac{x}{4} + \frac{y}{4} = 1 \quad \text{or} \quad \frac{x}{12} + \frac{y}{4/3} = 1 \quad \text{i.e., either}$$

$$x + y = 4 \quad \text{or} \quad x + 9y = 12.$$

EXAMPLE 3. Find the distance of the line $3x - y = 0$ from the point $(4, 1)$ measured along a line making an angle of $135°$ with the x-axis.

SOLUTION. The straight line L through $(4, 1)$ making an angle of $135°$ with the x-axis is

$$\frac{x-4}{\cos 135°} = \frac{y-1}{\sin 135°} = r. \quad \text{i.e.} \quad \frac{x-4}{-\frac{1}{\sqrt{2}}} = \frac{y-1}{\frac{1}{\sqrt{2}}} = r.$$

Any point P on this straight line is of the form $x = 4 - r\sqrt{2}, y = 1 + r\sqrt{2}$. Where r is the algebraic distance AP. If this point $(4 - r\sqrt{2}, 1 + r\sqrt{2})$ were to be on $3x - y = 0$ then

$$3(4 - r\sqrt{2}) - (1 + r\sqrt{2}) = 0, \quad 11 = 4r\sqrt{2} = 2\sqrt{2}r. \quad \text{Therefore} \quad r = \frac{11}{2\sqrt{2}} = 11\sqrt{2}/4 \text{ units.}$$

Thus the distance of $3x - y = 0$ from $(4, 1)$ measured along L is $11\sqrt{2}/4$ units.

Angle between Straight lines: Consider two straight lines $y = m_1x + C_1$ and $y = m_2x + C_2$. Then the two angles between these straight lines are supplementary angles. It is clear that the two angles between the two straight lines are $\theta_2 - \theta_1$ and $\pi - (\theta_2 - \theta_1)$ where θ_1 and θ_2 are the angles made by the given lines with the positive x-axis. Therefore we have

$$\tan\theta_1 = m_1 \quad \text{and} \quad \tan\theta_2 = m_2$$

and the angles between the straight lines are given by the equation

$$\tan\theta = \pm\tan(\theta_1 - \theta_2) = \pm\frac{\tan\theta_1 - \tan\theta_2}{1 + \tan\theta_1\tan\theta_2} = \pm\frac{m_1 - m_2}{1 + m_1m_2}$$

If $\frac{m_1-m_2}{1+m_1m_2} > 0$ then $\tan\theta = \frac{m_1-m_2}{1+m_1m_2}$ gives the acute angle between the two straight lines and if $\frac{m_1-m_2}{1+m_1m_2} < 0$ then $\tan\theta = \frac{m_1-m_2}{1+m_1m_2}$ gives the obtuse angle between the straight lines.

Equation of a family of straight lines passing through the intersection of two given lines

Consider two straight lines $L_1 = a_1x + b_1y + c_1 = 0$ and $L_2 = a_2x + b_2y + c_2 = 0$ intersecting at a point $P(h,k)$. Now

$$L_1 + \lambda L_2 \equiv (a_1x + b_1y + c_1) + \lambda(a_2x + b_2y + c_2) = 0 \quad (*)$$

is again a linear equation, namely

$$(a_1 + \lambda a_2)x + (b_1 + \lambda b_2)y + (c_1 + \lambda c_2) = 0$$

and hence is also a straight line. Further the point (h,k) satisfies $(a_1h+b_1k+c_1)+\lambda(a_2h+b_2k+c_2) = 0+\lambda\cdot 0 = 0$. Therefore, (*) is a straight line passing through the point of intersection of L_1 and L_2. Conversely, suppose L is any straight line passing through the point of intersection of L_1 and L_2. Let $px + qy + r = 0$ be the straight line L.

Then L can be written as $y - k = m(x-h)$ where m is its slope. Solving $a_1h + b_1k + c_1 = 0, a_2h + b_2k + c_2 = 0$ we get

$$h = \frac{b_1c_2 - b_2c_1}{a_1b_2 - a_2b_1} \quad \text{and} \quad k = \frac{a_2c_1 - a_1c_2}{a_1b_2 - a_2b_1}$$

$$\therefore y - \frac{a_2c_1 - a_1c_2}{a_1b_2 - a_2b_1} = m\left(x - \frac{b_1c_2 - b_2c_1}{a_1b_2 - a_2b_1}\right) \quad \text{is the equation of } L.$$

Simplifying, we get

$$m(a_1b_2 - a_2b_1)x - y(a_1b_2 - a_2b_1) + (a_2c_1 - a_1c_2) - m(b_1c_2 - b_2c_1) = 0$$

i.e.,

$$(a_1 + mb_2)(a_1x + b_1y + c_1) - (a_1 + mb_1)(a_2x + b_2y + c_2) = 0$$

which is of the form

$$a_1x + b_1y + c_1 + \lambda(a_2x + b_2y + c_2) = 0$$

where

$$\lambda = -\frac{a_1 + mb_1}{a_2 + mb_2}$$

Note. When we vary λ in $L_1 + \lambda L_2 = 0$ we get the family of straight lines passing through the intersection of $L_1 = 0$ and $L_2 = 0$.

14.3 Exercise

1. If (x_1, y_1) is the midpoint of the portion of a straight line intercepted between the coordinate axes, prove that the equation of the line is $x/2x_1 + y/2y_1 = 1$.

2. Find the equations of the straight lines through the origin whose intercepts between the lines $5x + 12y = 15$ and $5x + 12y = 30$ are each equal to three.

3. Show that the lines $3x + y + 4 = 0$, $3x + 4y - 15 = 0$, and $24x - 7y - 3 = 0$ form an isosceles triangle.

4. Find the area of the triangle formed by the lines $2x - y + 4 = 0$, $3x + 2y - 5 = 0$, and $x + y + 1 = 0$.

5. Straight lines are drawn from $A(3, 2)$ to meet the line $6x + 7y = 30$ and these straight lines are bisected. Find the locus of the midpoints.

6. Find the area of the triangle formed by the lines $y = m_1x + c_1$, $y = m_2x + c_2$, and $x = 0$.

7. Find the acute angle between $3x - 2y + 3 = 0$ and $2x + y - 5 = 0$.

8. Find the equations of the lines through $(2, 3)$ which make $45°$ with $3x - y + 5 = 0$.

9. If (h, k) is the foot of the perpendicular from (x_1, y_1) to the straight line $Lx + My + n = 0$, show that

$$(h - x_1)M = (k - y_1)m(Lx_1 + My_1 + n)/(L^2 + M^2).$$

10. A vertex of an equilateral triangle is at $(2, 3)$ and the opposite side is $x + y = 2$. Find the equations to the other sides of the triangle.

11. A triangle is formed by the lines $ax + by + c = 0$, $Lx + My + n = 0$, and $px + qy + r = 0$. Show that

$$(ax + by + c)/(ap + bq) = (Lx + My + n)/(Lp + Mq)$$

passes through the orthocentre.

12. Show that the origin is within the triangle formed by the lines $4x + 7y + 19 = 0$, $4x + y - 11 = 0$, and $4x - 5y + 7 = 0$.

13. Find the inradius of the triangle formed by the lines $x = 0$, $y = 0$, and $x/3 + y/4 = 1$.

14. Show that the following pair of equations represent the same family of straight lines

$$2x + 3y - 8 + \lambda(4x - 7y + 10) = 0 \quad \text{and} \quad 3x + 4y - 11 + \mu(2x - 5y + 8) = 0.$$

14.4 Circles

The equation to the circle with centre origin and radius r is $x^2 + y^2 = r^2$. In fact any point $P(x, y)$ lying on the circle satisfies $OP^2 = r^2$ or $x^2 + y^2 = r^2$.

Conversely, if $x^2 + y^2 = r^2$ then (x, y) lies on the circle. If the centre is (a, b) instead of $(0, 0)$ then the equation to the circle with centre (a, b) and radius r is $(x - a)^2 + (y - b)^2 = r^2$. In general, the equation to any circle is of the form $x^2 + y^2 + 2gx + 2fy + c = 0$. We have already seen that the circle with centre (a, b) and radius r has the equation

$$(x - a)^2 + (y - b)^2 = r^2 \quad \text{or} \quad x^2 + y^2 - 2ax - 2by + a^2 + b^2 - r^2 = 0$$

which is of the above mentioned form. Conversely, consider the set of points (x, y) satisfying $x^2+y^2+2gx+2fy+c = 0$. We may write this equation in the form $(x+g)^2+(y+f)^2+(c-g^2-f^2) = 0$ or $(x-(-g))^2+(y-(-f))^2 = g^2+f^2-c$ which is the equation to the circle with centre $(-g, -f)$ and radius $\sqrt{g^2 + f^2 - c}$ whenever $g^2 + f^2 - c \geq 0$.

Thus we have

Proposition 1. $x^2 + y^2 + 2gx + 2fy + c = 0$ represents a circle whenever $g^2 + f^2 - c = 0$ and any circle can be put in the form $x^2 + y^2 + 2gx + 2fy + c = 0$. In fact $(-g, -f)$ is the centre and $\sqrt{g^2 + f^2 - c}$ is the radius. Proposition 1 says that the general second degree equation $ax^2 + 2hxy + by^2 + 2gx + 2fy + c = 0$ is a circle if and only if $a = b$ and $h = 0$.

Some immediate observations

1. A circle is a second degree curve.

2. In the general circle $x^2 + y^2 + 2gx + 2fy + c = 0$ there are three independent constants $g, f,$ and c. Any three independent conditions enable us to fix $g, f,$ and c and hence the circle. In particular any three non-collinear points determine a circle.

3. A straight line is given by a linear equation of the form $ax + by + d = 0$ and a circle has the second degree equation $x^2 + y^2 + 2gx + 2fy + c = 0$. Therefore if we solve $ax + by + d = 0$ and $x^2 + y^2 + 2gx + 2fy + c = 0$ we have (i) two distinct points of intersection or (ii) two coincident points of intersection or (iii) two imaginary points of intersection. In other words a straight line either cuts a circle at two distinct points or touches a circle at two coincident points or never meets the circle at all. When the two points of intersection are coincident, the straight line is a tangent to the circle.

4. Two circles $S_1 \equiv x^2 + y^2 + 2g_1x + 2f_1y + c_1 = 0$ and $S_2 \equiv x^2 + y^2 + 2g_2x + 2f_2y + c_2 = 0$ intersect in general at two points. The points of intersection satisfy both $S_1 = 0, S_2 = 0$ and hence

$$S_1 - S_2 = 2(g_1 - g_2)x + 2(f_1 - f_2)y + c_1 - c_2 = 0.$$

This is a straight line which becomes the common chord when the two circles intersect.

Note. In general, two quadratic curves

$$a_1x^2 + 2h_1xy + b_1y^2 + 2g_1x + 2f_1y + c_1 = 0 \quad \text{and} \quad a_2x^2 + 2h_2xy + b_2y^2 + 2g_2x + 2f_2y + c_2 = 0$$

have four points in common! (as seen in algebra).

5. A point $P(x_1, y_1)$ lies inside a circle, on the circle, or outside the circle $x^2 + y^2 + 2gx + 2fy + c = 0$ according as $S_1 = x_1^2+y_1^2+2gx_1+2fy_1+c_1 < 0$, $S_1 = 0$ or $S_1 > 0$. In particular, the origin lies within $x^2+y^2+2gx+2fy+c = 0$ if and only if $c < 0$.

Proposition 2. The length of the tangent from (x_1, y_1) to the circle $x^2+y^2+2gx+2fy+c = 0$ is $\sqrt{x_1^2 + y_1^2 + 2gx_1 + 2fy_1 +}$

Proof. Let P be (x_1, y_1) and PT be a tangent from P to the circle $x^2 + y^2 + 2gx + 2fy + c = 0$. Then $\triangle OTP$ is a right-angled triangle and $PT^2 = OP^2 - OT^2 = OP^2 - (\text{radius})^2$

$$= (x_1 + g)^2 + (y_1 + f)^2 - (g^2 + f^2 - c)$$

$$= x_1^2 + y_1^2 + 2gx_1 + 2fy_1 + c.$$

Definition. The *power* of $P(x_1, y_1)$ with respect to the circle $x^2 + y^2 + 2gx + 2fy + c = 0$ is $OP^2 - r^2$, i.e., $x_1^2 + y_1^2 + 2gx_1 + 2fy_1 + c$.

Proposition 3. The tangent at (x_1, y_1) to the circle $x^2 + y^2 + 2gx + 2fy + c = 0$ has the equation $xx_1 + yy_1 + g(x + x_1) + f(y + y_1) + c = 0$.

Proof. The centre O has coordinates $(-g, -f)$ and hence the slope of the radius OP is $\frac{y_1+f}{x_1+g}$. For a circle, the tangent at P is perpendicular to the radius OP and hence the tangent at $P(x_1, y_1)$ has the slope $-\frac{x_1+g}{y_1+f}$.

Therefore, the equation to the tangent at P is

$$y - y_1 = -\frac{x_1 + g}{y_1 + f}(x - x_1).$$

i.e.,

$$(y - y_1)(y_1 + f) + (x_1 + g)(x - x_1) = 0$$

i.e.,

$$x_1 x + y_1 y + gx + fy = x_1^2 + y_1^2 + gx_1 + fy_1.$$

Adding $gx_1 + fy_1 + c$ we get

$$x_1 x + y_1 y + g(x + x_1) + f(y + y_1) + c = S_1 = 0$$

(where $S_1 = x_1^2 + y_1^2 + 2gx_1 + 2fy_1 + c$) since (x_1, y_1) lies on the circle.

Thus the tangent at $P(x_1, y_1)$ to the circle $x^2 + y^2 + 2gx + 2fy + c = 0$ is

$$xx_1 + yy_1 + g(x + x_1) + f(y + y_1) + c = 0.$$

Proposition 4. The straight line $y = mx + c$ is a tangent to the circle $x^2 + y^2 = a^2$ if and only if $c^2 = a^2(1 + m^2)$.

Proof. Solving $y = mx + c$ with $x^2 + y^2 = a^2$ algebraically, we get the quadratic equation

$$x^2 + (mx + c)^2 = a^2 \quad \text{or} \quad (1 + m^2)x^2 + 2mcx + c^2 - a^2 = 0.$$

This quadratic equation has equal roots if and only if its discriminant is zero; in other words $m^2c^2 = (1+m^2)(c^2-a^2)$ or $c^2 = a^2(1 + m^2)$. Hence $y = mx + c$ is a tangent to $x^2 + y^2 = a^2$ if $c^2 = a^2(1 + m^2)$.

Corollary. The point of contact of the tangent $y = mx + c$ with the circle $x^2 + y^2 = a^2$ is $\left(-\frac{a^2m}{c}, \frac{a^2}{c}\right)$.

Proof. As in the proof of the proposition the equal roots for x satisfy $(1 + m^2)x^2 + 2mcx + c^2 - a^2 = 0$ with $c^2 = a^2(1 + m^2)$.

$$\therefore x = \frac{-mc}{1 + m^2} = -\frac{a^2m}{c}.$$

This gives the point of contact as

$$\left(-\frac{a^2m}{c}, \frac{a^2}{c}\right).$$

$$= \left(-\frac{am}{(1 + m^2)}, \frac{a}{(1 + m^2)}\right) \quad \text{or} \quad \left(\frac{am}{(1 + m^2)}, -\frac{a}{(1 + m^2)}\right)$$

according as $c = \pm a\sqrt{1 + m^2}$.

Proposition 5. From a given point P outside a circle S two tangents can be drawn to the circle S.

Proof. We may take S to be $x^2+y^2=a^2$ and P to be (x_1,y_1). Any tangent to S is of the form $y=mx\pm a\sqrt{1+m^2}$. If it passes through (x_1,y_1) then we have $y_1=mx_1\pm a\sqrt{1+m^2}$. This gives

$$(y_1-mx_1)^2=a^2(1+m^2).$$

or

$$m^2(x_1^2-a^2)-2x_1y_1m+y_1^2-a^2=0.$$

This is a quadratic in m with discriminant

$$4(x_1^2y_1^2-(x_1^2-a^2)(y_1^2-a^2))=4a^2(x_1^2+y_1^2-a^2)>0$$

since $P(x_1,y_1)$ is outside the circle.

$\therefore$ It has two distinct roots giving rise to two tangents from P to the circle.

Proposition 6. The equation to the chord of contact of tangents to the circle $x^2+y^2+2gx+2fy+c=0$ from a point outside it is

$$xx_1+yy_1+g(x+x_1)+f(y+y_1)+c=0.$$

Proof. Let $A(x_2,y_2)$ and $B(x_3,y_3)$ be the points of contact of the tangents from $P(x_1,y_1)$ to the given circle. Then the tangent at A has the equation $xx_2+yy_2+g(x+x_2)+f(y+y_2)+c=0$. The tangent at $B(x_3,y_3)$ has the equation $xx_3+yy_3+g(x+x_3)+f(y+y_3)+c=0$. Now (x_1,y_1) lies on both these tangents. Hence, we have

$$(*)\quad x_1x_2+y_1y_2+g(x_1+x_2)+f(y_1+y_2)+c=0$$

$$x_1x_3+y_1y_3+g(x_1+x_3)+f(y_1+y_3)+c=0.$$

But (*) implies that (x_2,y_2) and (x_3,y_3) lie on the straight line

$$xx_1+yy_1+g(x+x_1)+f(y+y_1)+c=0.$$

Example . Show that the circle on the intercept of the line $lx+my=1$ with $ax^2+2hxy+by^2=0$ as diameter is

$$(am^2-2hlm+bl^2)(x^2+y^2)+2x(hm-bl)+2y(hl-am)+a+b=0.$$

Solution. $ax^2+2hxy+by^2=0$ represents a pair of lines $y=m_1x, y=m_2x$ through the origin got by factorizing

$$\frac{y^2}{x^2}+\frac{2h}{b}\frac{y}{x}+\frac{a}{b}\text{ as }\left(\frac{y}{x}-m_1\right)\left(\frac{y}{x}-m_2\right).$$

Therefore we have $m_1+m_2=-\frac{2h}{b}$ and $m_1m_2=\frac{a}{b}$.

Let OA be $y=m_1x$ and OB be $y=m_2x$. Then $A(x_1,y_1)$ and $B(x_2,y_2)$ satisfy

$$lx_1+m_1mx_1=1\text{ or }x_1=\frac{1}{l+m_1m},$$

$$y_1=\frac{m_1}{l+m_1m}.$$

Similarly

$$x_2=\frac{1}{l+m_2m}\text{ and }y_2=\frac{m_2}{l+m_2m}.$$

The equation to the circle on AB as diameter is

$$(x-x_1)(x-x_2)+(y-y_1)(y-y_2)=0\text{ or}$$

$$x^2+y^2-(x_1+x_2)x-(y_1+y_2)y+x_1x_2+y_1y_2=0.\quad(*)$$

We have

$$x_1 + x_2 = \frac{1}{l+m_1m} + \frac{1}{l+m_2m} = \frac{l+m_1m+l+m_2m}{(l+m_1m)(l+m_2m)} = \frac{2l+m_1+m_2}{l^2+lm_1m+lm_2m+m_1m_2m^2}$$

$$= \frac{2l-2hm/b}{l^2+lm_1m+lm_2m+am^2/b} = \frac{2bl-2hm}{bl^2+lm_1bm+lm_2bm+am^2} = \frac{2l-2hm/b}{l^2+lm_1m+lm_2m+m_1m_2m^2}.$$

Similarly,

$$y_1 + y_2 = \frac{-2hl+2ma}{bl^2-2hlm+am^2}.$$

Also

$$x_1x_2 = \frac{1}{(l+m_1m)(l+m_2m)} = \frac{1}{b^2-2hlm+am^2} \quad \text{from (**)},$$

$$y_1y_2 = \frac{m_1m_2}{(l+m_1m)(l+m_2m)} = \frac{a}{(bl^2-2hlm+am^2)}.$$

Substituting in (*) we get the required circle as

$$x^2+y^2 - \frac{2(bl-hm)}{bl^2-2hlm+am^2}x - \frac{2(hm-bl)}{bl^2-2hlm+am^2}y + \frac{a+b}{bl^2-2hlm+am^2} = 0$$

or

$$(am^2-2hlm+bl^2)(x^2+y^2) + 2x(hm-bl) + 2y(hl-am) + a + b = 0.$$

Example 7. Find the circumcentre of the triangle formed by $x+y=0$, $x-y=0$, and $lx+my=1$. If l and m vary such that $l^2+m^2=1$, show that the locus of its circumcentre is the curve $(x^2-y^2)^2 = x^2+y^2$.

Solution. Solving the straight lines $x-y=0$, $x+y=0$, and $lx+my=1$ two by two we get the vertices as

$$A(0,0), \quad B\left(\frac{1}{l+m}, \frac{1}{l+m}\right), \quad \text{and} \quad C\left(\frac{1}{l-m}, \frac{1}{m-l}\right).$$

If (h,k) is the circumcentre, then $SA^2 = SB^2 = SC^2$ and hence

$$h^2+k^2 = \left(h - \frac{1}{l+m}\right)^2 + \left(k - \frac{1}{l+m}\right)^2$$

$$= \left(h - \frac{1}{l-m}\right)^2 + \left(k + \frac{1}{l-m}\right)^2.$$

$$\frac{-2h}{l+m} + \frac{2k}{l+m} + \frac{2}{(l+m)^2} = 0 \quad \text{or} \quad h+k = \frac{1}{l+m} \tag{1}$$

$$\frac{-2h}{l-m} + \frac{2k}{l-m} + \frac{2}{(l-m)^2} = 0 \quad \text{or} \quad h-k = \frac{1}{l-m} \tag{2}$$

If l, m vary such that $l^2+m^2=1$, then the locus of the circumcentre is got from

$$h^2+k^2 = \frac{1}{(l^2+m^2)(l^2-m^2)^2} = \frac{1}{(l^2-m^2)^2} = (h^2-k^2)^2.$$

Hence the locus of the circumcentre is $(x^2-y^2)^2 = x^2+y^2$.

Example 10. The circle $x^2+y^2=a^2$ is given by the parametric equation $x = a\cos\theta$, $y = a\sin\theta$. Find the equation to the chord joining θ and ϕ on the circle $x^2+y^2=a^2$.

Solution. The point θ is $(a\cos\theta, a\sin\theta)$ and ϕ is $(a\cos\phi, a\sin\phi)$. Therefore the equation to the chord joining θ and ϕ is

$$\frac{x - a\cos\theta}{a\cos\theta - a\cos\phi} = \frac{y - a\sin\theta}{a\sin\theta - a\sin\phi}$$

or

$$\frac{x - a\cos\theta}{2\sin\frac{\theta+\phi}{2}\sin\frac{\phi-\theta}{2}} = \frac{y - a\sin\theta}{2\sin\frac{\theta+\phi}{2}\cos\frac{\theta-\phi}{2}}$$

Therefore

$$\frac{x - a\cos\theta}{\sin\frac{\theta+\phi}{2}} = \frac{y - a\sin\theta}{\cos\frac{\theta+\phi}{2}}$$

or

$$x\cos\frac{\theta+\phi}{2} + y\sin\frac{\theta+\phi}{2} = a\left(\cos\theta\cos\frac{\theta+\phi}{2} + \sin\theta\sin\frac{\theta+\phi}{2}\right)$$

or

$$x\cos\frac{\theta+\phi}{2} + y\sin\frac{\theta+\phi}{2} = a\cos\frac{\theta-\phi}{2}$$

As a corollary we note that the tangent at θ to the circle $x^2 + y^2 = a^2$ is $x\cos\theta + y\sin\theta = a$ (obtained by putting $\theta = \phi$ in the chord equation).

14.5 Exercise

1. Show that the circle $x^2 + y^2 + 4x - 4y + 4 = 0$ touches the coordinate axes.

2. Show that $x^2 + y^2 = 400$ and $x^2 + y^2 - 10x - 24y + 120 = 0$ touch one another internally. Find the coordinates of the point of contact.

3. Find the locus of the centre of a circle which touches $x \cos\alpha + y \sin\alpha = p$ and the circle $(x - a)^2 + (y - b)^2 = c^2$.

4. The lines $lx + my + n = 0$ intersect the curve $ax^2 + 2hxy + by^2 = 1$ at P, Q which lie at finite distances from $(0, 0)$. The circle on PQ as diameter passes through $(0, 0)$. Show that $n^2(a + b) = l^2 + m^2$.

5. Find the points on $x - y + 1 = 0$, the tangents from which to the circle $x^2 + y^2 - 3x = 0$ are of length 2.

6. Find the locus of a point the tangents from which to the circle $4x^2 + 4y^2 - 9 = 0$ and $9x^2 + 9y^2 - 16 = 0$ are in the ratio 3:4.

7. Find the equation of a line inclined at $45°$ to the axis of x, such that $x^2+y^2 = 4$ and $x^2+y^2-10x-14y-15 = 0$ cut off equal lengths on it.

8. If $x \cos\alpha + y \sin\alpha = p$ touches $(x - a)^2 + (y - b)^2 = c^2$, then prove that $a \cos\alpha + b \sin\alpha - p = \pm c$.

9. Show that the locus of the feet of the perpendiculars drawn from the point $(a, 0)$ on tangents to the circle $x^2 + y^2 = a^2$ is $(x^2 + y^2 - ax)^2 = y^2(x - a)^2$.

10. Show that the locus of the midpoints of the chords of contact of tangents drawn to a given circle from points on another given circle is a third circle.

11. Find the equation of the common tangents to the circles $x^2+y^2-22x+4y+100 = 0$ and $x^2+y^2+22x-4y-100 = 0$.

12. Show that the tangents to the circle $x^2 + y^2 = 25$ which pass through $(-1, 7)$ are at right angles.

14.6 Coordinate Geometry MCQ

1. A point P on the line $3x + 5y = 15$ is equidistant from the coordinate axes: P can lie in

(A) quadrant I only;

(B) quadrant I or quadrant II;

(C) quadrant I or quadrant III;

(D) any quadrant.

2. The set of all points (x, y) in the plane satisfying the equation $5x^2y - xy + y = 0$ forms

(A) a straight line;

(B) a parabola;

(C) a circle;

(D) none of the foregoing curves.

3. The equation of the line through the intersection of the lines

$$2x + 3y + 4 = 0 \quad \text{and} \quad 3x + 4y - 5 = 0$$

and perpendicular to $7x - 5y + 8 = 0$ is

(A) $5x + 7y = 1$;

(B) $7x + 5y + 1 = 0$;

(C) $5x - 7y + 1 = 0$;

(D) $7x - 5y - 1 = 0$.

4. Two equal sides of an isosceles triangle are given by the equations $y = 7x$ and $y = -x$ and its third side passes through $(1, -10)$. Then the equation of the third side is

(A) $3x + y + 7 = 0$ or $x - 3y - 31 = 0$;

(B) $x + 3y + 29 = 0$ or $-3x + y + 13 = 0$;

(C) $3x + y + 7 = 0$ or $x + 3y + 29 = 0$;

(D) $x - 3y - 31 = 0$ or $-3x + y + 13 = 0$.

5. The equations of two adjacent sides of a rhombus are given by $y = x$ and $y = 7x$. The diagonals of the rhombus intersect each other at the point $(1, 2)$. The area of the rhombus is

(A) $\frac{10\sqrt{2}}{3}$;

(B) $\frac{20\sqrt{2}}{3}$;

(C) $\frac{50\sqrt{2}}{3}$;

(D) none of the foregoing quantities.

6. It is given that three distinct points (x_1, y_1), (x_2, y_2), and (x_3, y_3) are collinear. Then a necessary and sufficient condition for (x_2, y_2) to lie on the line segment joining (x_3, y_3) to (x_1, y_1) is

(A) either $x_1 + y_1 < x_2 + y_2 < x_3 + y_3$ or $x_3 + y_3 < x_2 + y_2 < x_1 + y_1$;

(B) either $x_1 < x_2 < x_3$ or $x_3 < x_2 < x_1$;

(C) either $0 < \frac{x_2 - x_1}{x_1 - x_3} < 1$ or $0 < \frac{y_2 - y_1}{y_1 - y_3} < 1$;

(D) none of the foregoing statements.

7. Let $A(x_1, y_1)$, $B(x_2, y_2)$, $C(x_3, y_3)$, $D(x_4, y_4)$ be four points such that x_1, x_2, x_3, x_4 and y_1, y_2, y_3, y_4 are both in A.P. If Δ denotes the area of the quadrilateral $ABCD$, then

(A) $\Delta = 0$;

(B) $\Delta > 1$;

(C) $\Delta < 1$;

(D) Δ depends on the coordinates of A, B, C and D.

8. The number of points (x, y) satisfying (i) $3y - 4x = 20$ and (ii) $x^2 + y^2 \leq 16$ is

(A) 0;

(B) 1;

(C) 2;

(D) infinite.

9. The equation of the line parallel to the line $3x + 4y = 0$ and touching the circle $x^2 + y^2 = 9$ in the first quadrant is

(A) $3x + 4y = 9$;

(B) $3x + 4y = 45$;

(C) $3x + 4y = 15$;

(D) none of the foregoing equations.

10. The difference between the radii of the largest and the smallest circles, which have their centres on the circumference of the circle $x^2 + 2x + y^2 + 4y = 4$ and pass through the point (a, b) lying outside the given circle, is

(A) 6;

(B) $\sqrt{(a+1)^2 + (b+2)^2}$;

(C) 3;

(D) $\sqrt{(a+1)^2 + (b+2)^2} - 3$.

11. The perimeter of the region bounded by $x^2 + y^2 \leq 100$ and $x^2 + y^2 - 10x - 10(2 - \sqrt{3})y \leq 0$ is

(A) $\frac{5\pi}{3}(5 + \sqrt{6} - \sqrt{2})$;

(B) $\frac{5\pi}{3}(1 + \sqrt{6} - \sqrt{2})$;

(C) $\frac{5\pi}{3}(1 + 2\sqrt{6} - 2\sqrt{2})$;

(D) $\frac{5\pi}{3}(5 + 2\sqrt{6} - 2\sqrt{2})$.

12. The equation of the circle which has both coordinate axes as its tangents and which touches the circle $x^2 + y^2 = 6x + 6y - 9 - 4\sqrt{2}$ is:

(A) $x^2 + y^2 = 2x + 2y + 1$;

(B) $x^2 + y^2 = 2x - 2y + 1$;

(C) $x^2 + y^2 = 2x + 2y - 1$;

(D) $x^2 + y^2 = 2x - 2y - 1$.

13. A circle and a square have the same perimeter. Then

(A) their areas are equal;

(B) the area of the circle is larger;

(C) the area of the square is larger;

(D) the area of the circle is π times the area of the square.

14. The equation $x^2 + y^2 - 2xy - 1 = 0$ represents

(A) two parallel straight lines;

(B) two perpendicular straight lines;

(C) a circle;

(D) a hyperbola.

15. The equation $x^3 - yx^2 + x - y = 0$ represents

(A) a straight line;

(B) a parabola and two straight lines;

(C) a hyperbola and two straight lines;

(D) a straight line and a circle.

16. The equation $x^3y + xy^3 + xy = 0$ represents

(A) a circle;

(B) a circle and a pair of straight lines;

(C) a rectangular hyperbola;

(D) a pair of straight lines.

17. A circle of radius r touches the parabola $x^2 + 4ay = 0$ $(a > 0)$ at the vertex of the parabola. The centre of the circle lies below the vertex and the circle lies entirely within the parabola. Then the largest possible value of r is

(A) a;

(B) $2a$;

(C) $4a$;

(D) none of the foregoing expressions.

18. The equation $16x^4 - y^4 = 0$ represents

(A) a pair of straight lines;

(B) one straight line;

(C) a point;

(D) a hyperbola.

19. The equation of the straight line which passes through the point of intersection of the lines $x + 2y + 3 = 0$ and $3x + 4y + 7 = 0$ and is perpendicular to the straight line $y - x = 8$ is

(A) $6x + 6y - 8 = 0$;

(B) $x + y + 2 = 0$;

(C) $4x + 8y + 12 = 0$;

(D) $3x + 3y - 6 = 0$.

20. Two circles with equal radii are intersecting at the points $(0, 1)$ and $(0, -1)$. The tangent at $(0, 1)$ to one of the circles passes through the centre of the other circle. Then the centres of the two circles are at

(A) $(2, 0)$ and $(-2, 0)$;

(B) $(0.75, 0)$ and $(-0.75, 0)$;

(C) $(1, 0)$ and $(-1, 0)$;

(D) none of the foregoing pairs of points.

ANSWER KEY

1	2	3	4	5	6	7	8	9	10
B	A	A	A	A	C	A	B	C	A
11	12	13	14	15	16	17	18	19	20
C	D	B	A	A	D	B	A	A	D

15 Sequences

15.1 Introduction

A sequence of real numbers means writing some real numbers one after the other like $1, 1/2, 1/3, \cdots$ or $1, -1, 1, \cdots$. Observe that whenever we say a sequence, it is infinite sequence by default. Let us formalise this idea of a sequence

Definition: A sequence of real numbers is a function $f : \mathbb{N} \to \mathbb{R}$ written as $a_1, a_2, \cdots$ where $a_n = f(n)$ for all $n \geq 1$

Observe that a sequence doesn't need a closed form for its nth term. For example if we look at the sequence of primes p_n doesn't have a closed form. We denote the sequence $a_1, a_2, \ldots$ as $\{a_n\}_{n\geq 1}$ or simply $\{a_n\}$.

We say a sequence $\{x_n\}$ is an increasing sequence if $x_{n+1} \geq x_n$ for all n. Similarly we say a sequence $\{x_n\}$ is a decreasing sequence if $x_{n+1} \leq x_n$ for all n. You can also talk about a strictly increasing or strictly decreasing sequence when the inequalities are strict. If a sequence is either increasing or decreasing then it is called a monotonic sequence.

One more of classifying a sequence is if the sequence is bounded or not. A sequence $\{x_n\}$ is bounded if there exists $M \in \mathbb{R}$ such that $|x_n| \leq M$. A sequence doesnt have to bounded on both sides, We could have a sequence which is bounded above i.e. $x_n \leq M$ for all n. Similarly we can have a sequence that is bounded below that is $x_n \geq M$ for all n.

15.2 Exercise 15.1

1. Can a sequence be both increasing and decreasing?

2. Show that a sequence $\{x_n\}$ is increasing if and only if the sequence $\{-x_n\}$ is decreasing.

3. Consider the sequence $\{2^n - n^2\}_{n\geq 1}$. Is it monotonic?

4. Which of the following sequences are bounded

1. $\{\sin n\}$
2. $\{2^n/n\}$
3. $2^{-n}/n$

5. Let $\{x_n\}$ be a bounded sequence. Show that the sequence $s_n = (x_1 + \cdots + x_n)/n$ is also bounded.

15.3 Convergence of sequences

There are a number of different limit concepts in real analysis. The notion of limit of a sequence is the most basic, and it will be the focus of this section.

Definition: A sequence $X = (x_n)$ in $\mathbb{R}$ is said to **converge** to $x \in \mathbb{R}$, or x is said to be a **limit** of (x_n), if for every $\epsilon > 0$ there exists a natural number $K(\epsilon)$ such that for all $n \geq K(\epsilon)$, the terms x_n satisfy $|x_n - x| < \epsilon$.
If a sequence has a limit, we say that the sequence is **convergent**; if it has no limit, we say that the sequence is **divergent**.

Note The notation $K(\epsilon)$ is used to emphasize that the choice of K depends on the value of ϵ. However, it is often convenient to write K instead of $K(\epsilon)$. In most cases, a "small" value of ϵ will usually require a "large" value of K to guarantee that the distance $|x_n - x|$ between x_n and x is less than ϵ for all $n \geq K = K(\epsilon)$.

When a sequence has limit x, we will use the notation

$$\lim X = x \quad \text{or} \quad \lim(x_n) = x.$$

We will sometimes use the symbolism $x_n \to x$, which indicates the intuitive idea that the values x_n "approach" the number x as $n \to \infty$.

Theorem : (Uniqueness of Limits) A sequence in $\mathbb{R}$ can have at most one limit.

Proof. Suppose that x' and x'' are both limits of (x_n). For each $\epsilon > 0$ there exist K' such that $|x_n - x'| < \epsilon/2$ for all $n \geq K'$, and there exists K'' such that $|x_n - x''| < \epsilon/2$ for all $n \geq K''$. We let K be the larger of K' and K''. Then for $n \geq K$ we apply the Triangle Inequality to get

$$|x' - x''| = |x' - x_n + x_n - x''| \leq |x' - x_n| + |x_n - x''| < \epsilon/2 + \epsilon/2 = \epsilon.$$

Since $\epsilon > 0$ is an arbitrary positive number, we conclude that $x' - x'' = 0$.

For $x \in \mathbb{R}$ and $\epsilon > 0$, recall that the ϵ-neighbourhood of x is the set

$$V_\epsilon(x) := \{u \in \mathbb{R} : |u - x| < \epsilon\}.$$

Since $u \in V_\epsilon(x)$ is equivalent to $|u - x| < \epsilon$, the definition of convergence of a sequence can be formulated in terms of neighbourhoods. We give several different ways of saying that a sequence x_n converges to x in the following theorem.

Theorem Let $X = (x_n)$ be a sequence of real numbers, and let $x \in \mathbb{R}$. The following statements are equivalent.

(a) X converges to x.

(b) For every $\epsilon > 0$, there exists a natural number K such that for all $n \geq K$, the terms x_n satisfy $|x_n - x| < \epsilon$.

(c) For every $\epsilon > 0$, there exists a natural number K such that for all $n \geq K$, the terms x_n satisfy $x - \epsilon < x_n < x + \epsilon$.

(d) For every ϵ-neighbourhood $V_\epsilon(x)$ of x, there exists a natural number K such that for all $n \geq K$, the terms x_n belong to $V_\epsilon(x)$.

Proof. The equivalence of (a) and (b) is just the definition. The equivalence of (b), (c), and (d) follows from the following implications:

$$|u - x| < \epsilon \iff -\epsilon < u - x < \epsilon \iff x - \epsilon < u < x + \epsilon \iff u \in V_\epsilon(x).$$

Example 1: $\lim 1/n = 0$

Solution: If $\epsilon > 0$ is given, then $1/\epsilon > 0$. But there is a natural number $K = K(\epsilon)$ such that $1/K < \epsilon$. Then, if $n \geq K$, we have $1/n \leq 1/K < \epsilon$. Consequently, if $n \geq K$, then

$$\left|\frac{1}{n} - 0\right| = \frac{1}{n} < \epsilon.$$

Therefore, we can assert that the sequence $(1/n)$ converges to 0.

Example 2: $\lim 1/(n^{+}1) = 0$

Solution: $\lim \left(\frac{1}{n^2+1}\right) = 0.$
Let $\epsilon > 0$ be given. To find K, we first note that if $n \in \mathbb{N}$, then

$$\frac{1}{n^2+1} < \frac{1}{n^2} \leq \frac{1}{n}.$$

Now choose K such that $1/K < \epsilon$, as in (a) above. Then $n \geq K$ implies that $1/n < \epsilon$, and therefore

$$\left|\frac{1}{n^2+1} - 0\right| = \frac{1}{n^2+1} < \frac{1}{n} < \epsilon.$$

Hence, we have shown that the limit of the sequence is zero.

Example 3: $\lim \left(\frac{3n+2}{n+1}\right) = 3.$

Solution: Given $\epsilon > 0$, we want to obtain the inequality

$$\left|\frac{3n+2}{n+1} - 3\right| < \epsilon \tag{1}$$

when n is sufficiently large. We first simplify the expression on the left:

$$\left|\frac{3n+2}{n+1} - 3\right| = \left|\frac{3n+2-3n-3}{n+1}\right| = \left|\frac{-1}{n+1}\right| = \frac{1}{n+1} < \frac{1}{n}.$$

Now if the inequality $1/n < \epsilon$ is satisfied, then the inequality (1) holds. Thus if $1/K < \epsilon$, then for any $n \geq K$, we also have $1/n < \epsilon$ and hence (1) holds. Therefore the limit of the sequence is 3.

Example 4: If $0 < b < 1$, then $\lim(b^n) = 0$.

Solution: We will use elementary properties of the natural logarithm function. If $\epsilon > 0$ is given, we see that

$$b^n < \epsilon \quad \Longleftrightarrow \quad n \ln b < \ln \epsilon \quad \Longleftrightarrow \quad n > \frac{\ln \epsilon}{\ln b}.$$

(The last inequality is reversed because $\ln b < 0$.) Thus if we choose K to be a number such that $K > \ln \epsilon / \ln b$, then we will have $0 < b^n < \epsilon$ for all $n \geq K$. Thus we have $\lim(b^n) = 0$. For example, if $b = .8$, and if $\epsilon = .01$ is given, then we would need $K > \ln .01 / \ln .8 \approx 20.6377$. Thus $K = 21$ would be an appropriate choice for $\epsilon = .01$.

Definition A sequence $X = (x_n)$ of real numbers is said to be **bounded** if there exists a real number $M > 0$ such that $|x_n| \leq M$ for all $n \in \mathbb{N}$.

Thus, the sequence (x_n) is bounded if and only if the set $\{x_n : n \in \mathbb{N}\}$ of its values is a bounded subset of $\mathbb{R}$.

Theorem: A **convergent** sequence of real numbers is bounded.

Proof. Suppose that $\lim(x_n) = x$ and let $\epsilon := 1$. Then there exists a natural number $K = K(1)$ such that $|x_n - x| < 1$ for all $n \geq K$. If we apply the Triangle Inequality with $n \geq K$ we obtain

$$|x_n| = |x_n - x + x| \leq |x_n - x| + |x| < 1 + |x|.$$

If we set

$$M := \sup\{|x_1|, |x_2|, \ldots, |x_{K-1}|, 1 + |x|\},$$

then it follows that $|x_n| \leq M$ for all $n \in \mathbb{N}$.

Theorem (a) Let $X = (x_n)$ and $Y = (y_n)$ be sequences of real numbers that converge to x and y, respectively, and let $c \in \mathbb{R}$. Then the sequences $X + Y$, $X - Y$, $X \cdot Y$, and cX converge to $x + y$, $x - y$, xy, and cx, respectively.

(b) If $X = (x_n)$ converges to x and $Z = (z_n)$ is a sequence of nonzero real numbers that converges to z and if $z \neq 0$, then the quotient sequence X/Z converges to x/z.

Proof. (a) To show that $\lim(x_n + y_n) = x + y$, we need to estimate the magnitude of $|(x_n + y_n) - (x + y)|$. To do this we use the Triangle Inequality 2.2.3 to obtain

$$|(x_n + y_n) - (x + y)| = |(x_n - x) + (y_n - y)| \leq |x_n - x| + |y_n - y|.$$

By hypothesis, if $\epsilon > 0$ there exists a natural number K_1 such that if $n \geq K_1$, then $|x_n - x| < \epsilon/2$; also there exists a natural number K_2 such that if $n \geq K_2$, then $|y_n - y| < \epsilon/2$. Hence if $K(\epsilon) := \sup(K_1, K_2)$, it follows that if $n \geq K(\epsilon)$ then

$$|(x_n + y_n) - (x + y)| \leq |x_n - x| + |y_n - y| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Since $\epsilon > 0$ is arbitrary, we infer that $X + Y = (x_n + y_n)$ converges to $x + y$.

Precisely the same argument can be used to show that $X - Y = (x_n - y_n)$ converges to $x - y$.

To show that $X \cdot Y = (x_n y_n)$ converges to xy, we make the estimate

$$|x_n y_n - xy| = |(x_n y_n - xy) + (xy - xy)| \leq |x_n y_n - xy| + |xy - xy| = |x_n||y_n - y| + |y||x_n - x|.$$

Then there exists a real number $M_1 > 0$ such that $|x_n| \leq M_1$ for all $n \in \mathbb{N}$ and we set $M := \sup\{M_1, |y|\}$. Hence we have the estimate

$$|x_n y_n - xy| \leq M|y_n - y| + M|x_n - x|.$$

From the convergence of X and Y we conclude that if $\epsilon > 0$ is given, then there exist natural numbers K_1 and K_2 such that if $n \geq K_1$, then $|x_n - x| < \epsilon/2M$, and if $n \geq K_2$ then $|y_n - y| < \epsilon/2M$. Now let $K(\epsilon) := \sup\{K_1, K_2\}$; then, if $n \geq K(\epsilon)$ we infer that

$$|x_n y_n - xy| \leq M|y_n - y| + M|x_n - x| < M(\epsilon/2M) + M(\epsilon/2M) = \epsilon.$$

Since $\epsilon > 0$ is arbitrary, this proves that the sequence $X \cdot Y = (x_n y_n)$ converges to xy.

The fact that $cX = (cx_n)$ converges to cx can be proved in the same way; it can also be deduced by taking Y to be the constant sequence $(c, c, c, \ldots)$. We leave the details to the reader.

(b) We next show that if $Z = (z_n)$ is a sequence of nonzero numbers that converges to a nonzero limit z, then the sequence $(1/z_n)$ of reciprocals converges to $1/z$. First let $\alpha := \frac{1}{2}|z|$ so that $\alpha > 0$. Since $\lim(z_n) = z$, there exists a natural number K_1 such that if $n \geq K_1$, then $|z_n - z| < \alpha$. It follows from the Triangle Inequality that

$$-\alpha < -|z_n - z| \leq |z_n| - |z| < |z_n| \leq |z| + \alpha \text{ for } n \geq K_1,$$

whence it follows that $\frac{1}{2}|z| = |z| - \alpha \leq |z_n|$ for $n \geq K_1$. Therefore $|1/z_n| \leq 2/|z|$ for $n \geq K$, so we have the estimate

$$\left|\frac{1}{z_n} - \frac{1}{z}\right| = \left|\frac{z - z_n}{z_n z}\right| = \frac{1}{|z_n z|}|z - z_n| \leq \frac{2}{|z|^2}|z - z_n| \text{ for all } n \geq K_1.$$

Now, if $\epsilon > 0$ is given, there exists a natural number K_2 such that if $n \geq K_2$ then $|z_n - z| < \frac{1}{2}\epsilon|z|^2$. Therefore, it follows that if $K(\epsilon) = \sup\{K_1, K_2\}$, then

$$\left|\frac{1}{z_n} - \frac{1}{z}\right| < \epsilon \text{ for all } n \geq K(\epsilon).$$

Since $\epsilon > 0$ is arbitrary, it follows that

$$\lim\left(\frac{1}{z_n}\right) = \frac{1}{z}.$$

Theorem: (Sandwich Theorem) Suppose that $X = (x_n)$, $Y = (y_n)$, and $Z = (z_n)$ are sequences of real numbers such that

$$x_n \leq y_n \leq z_n \quad \text{for all } n \in \mathbb{N},$$

and that $\lim(x_n) = \lim(z_n)$. Then $Y = (y_n)$ is convergent and

$$\lim(x_n) = \lim(y_n) = \lim(z_n).$$

Proof. Let $w := \lim(x_n) = \lim(z_n)$. If $\epsilon > 0$ is given, then it follows from the convergence of X and Z to w that there exists a natural number K such that if $n \geq K$ then

$$|x_n - w| < \epsilon \quad \text{and} \quad |z_n - w| < \epsilon.$$

Since the hypothesis implies that

$$x_n - w \leq y_n - w \leq z_n - w \quad \text{for all } n \in \mathbb{N},$$

it follows (why?) that

$$-\epsilon < y_n - w < \epsilon$$

for all $n \geq K$. Since $\epsilon > 0$ is arbitrary, this implies that $\lim(y_n) = w$.

Example 5:. For any integer $n \geq 1$, let $\langle n \rangle$ be the closest integer to $\sqrt{n}$. Compute

$$\lim_{n\to\infty} \sum_{j=1}^{n} \frac{2^{\langle j \rangle} + 2^{-\langle j \rangle}}{2^j}.$$

Solution. Since $(k - 1/2)^2 = k^2 - k + 1/4$ and $(k + 1/2)^2 = k^2 + k + 1/4$, it follows that $\langle n \rangle = k$ if and only if $k^2 - k + 1 \leq n \leq k^2 + k$. Hence

$$\lim_{n\to\infty} \sum_{j=1}^{n} \frac{2^{\langle j \rangle} + 2^{-\langle j \rangle}}{2^j} = \sum_{k=1}^{\infty} \sum_{\langle j \rangle = k} \frac{2^k + 2^{-k}}{2^j} = \sum_{k=1}^{\infty} \sum_{n=k^2-k+1}^{k^2+k} \frac{2^k + 2^{-k}}{2^n}$$

$$= \sum_{k=1}^{\infty} (2^k + 2^{-k}) \left(2^{-k^2+k-1} - 2^{-k^2-k}\right) = \sum_{k=1}^{\infty} \left(2^{-k(k-2)} - 2^{-k(k+2)}\right)$$

$$= \sum_{k=1}^{\infty} 2^{-k(k-2)} - \sum_{k=3}^{\infty} 2^{-k(k-2)} = 3.$$

Example 6: Let

$$S_n = \sum_{k=1}^{n} \left(\sqrt{1 + \frac{k}{n^2}} - 1 \right).$$

Show that $\lim_{n\to\infty} S_n = 1/4$.

Solution. We first observe that for all $x > -1$,

$$\frac{x}{2+x} < \sqrt{1+x} - 1 < \frac{x}{2}.$$

Hence, setting $x = k/n^2$, we obtain

$$\frac{k}{2n^2 + k} < \sqrt{1 + \frac{k}{n^2}} - 1 < \frac{k}{2n^2}.$$

Therefore

$$\sum_{k=1}^{n} \frac{k}{2n^2 + k} < S_n < \frac{1}{2n^2} \sum_{k=1}^{n} k.$$

We have

$$\frac{1}{2n^2} \sum_{k=1}^{n} k = \frac{n(n+1)}{4n^2} \to \frac{1}{4} \text{ as } n \to \infty.$$

On the other hand,

$$\lim_{n\to\infty}\left\{\frac{1}{2n^2}\sum_{k=1}^{n}k-\frac{n}{2n^2+k}\sum_{k=1}^{n}\frac{k}{2n^2+k}\right\}=\lim_{n\to\infty}\sum_{k=1}^{n}\frac{k^2}{2n^2(2n^2+k)}.$$

But

$$\sum_{k=1}^{n}\frac{k^2}{2n^2(2n^2+k)}<\sum_{k=1}^{n}\frac{k^2}{4n^4}=\frac{n(n+1)(2n+1)}{24n^4}.$$

We deduce that

$$\lim_{n\to\infty}\left\{\frac{1}{2n^2}\sum_{k=1}^{n}k-\frac{n}{2n^2+k}\sum_{k=1}^{n}\frac{k}{2n^2+k}\right\}=0$$

and

$$\lim_{n\to\infty}\sum_{k=1}^{n}\frac{k}{2n^2+k}=\frac{1}{4},$$

hence the desired conclusion.

Example 7: (IMO 1993.) Let $n>1$ be an integer. There are n lamps $L_0,\ldots,L_{n-1}$ arranged in a circle. Each lamp is either ON or OFF. A sequence of steps $S_0,\ldots,S_i,\ldots$ is carried out. Step S_j affects the state of L_j only (leaving the states of all other lamps unaltered) as follows:

If L_{j-1} is ON, S_j changes the state of L_j from ON to OFF or from OFF to ON;

If L_{j-1} is OFF, S_j leaves the state L_j unchanged.

The lamps are labeled mod n, that is, $L_{-1}=L_{n-1}, L_0=L_n, L_1=L_{n+1}$. Initially all lamps are ON. Show that

(a) there is a positive integer $M(n)$ such that after $M(n)$ steps all the lamps are ON again;

(b) if n has the form 2^k, then all lamps are ON after (n^2-1) steps;

(c) if n has the form 2^k+1, then all the lamps are ON after (n^2-n+1) steps.

Solution: Let $x_j\in\{0,1\}$ represent the state of lamp L_j (0 for OFF, 1 for ON). Operation S_j affects the state of L_j, which in the previous round has been set to the value x_{j-n}. At the moment when S_j is being performed, lamp L_{j-1} is in state x_{j-1}. Consequently,

$$x_j\equiv x_{j-n}+x_{j-1}\pmod 2.\quad (1)$$

This is true for all $j\geq 0$. Note that the initial state (all lamps ON) corresponds to

$$x_{-n}=x_{-n+1}=x_{-n+2}=\cdots=x_{-2}=x_{-1}=1.\quad (2)$$

The state of the system at instant j can be represented by the vector $\vec{v}_j=[x_{j-n},\ldots,x_{j-1}]$, $\vec{v}_0=[1,\ldots,1]$. Since there are only 2^n feasible vectors, repetitions must occur in the sequence $\vec{v}_0,\vec{v}_1,\vec{v}_2,\ldots$. The operation that produces $\vec{v}_{j+1}$ from $\vec{v}_j$ is invertible. Hence, the equality $\vec{v}_{j+m}=\vec{v}_j$ implies $\vec{v}_m=\vec{v}_0$; the initial state recurs in at most 2^n steps, proving (a).

To prove (b) and (c), notice that, in view of (1),

$$\begin{aligned}x_j&\equiv x_{j-n}+x_{j-1}\\&\equiv(x_{j-2n}+x_{j-n+1})+(x_{j-1-n}+x_{j-2})\\&\equiv x_{j-2n}+2x_{j-n-1}+x_{j-2}\\&\equiv x_{j-3n}+3x_{j-n-2}+x_{j-3},\text{ and so on.}\end{aligned}$$

After r applications of (1), we arrive at the equality

$$x_j \equiv \sum_{i=0}^{r} \binom{r}{i} x_{j-(r-i)n-i} \pmod 2,$$

holding for all j and r such that $j-(r-i)n-i \geq -n$. In particular, if r is of the form $r=2^k$, then the binomial coefficients $\binom{r}{i}$ are even, except the two outer ones, and we obtain

$$x_j \equiv x_{j-rn} + x_{j-r} \quad (\text{for } r = 2^k), \quad (3)$$

provided the subscripts do not go below $-n$, i.e., for $j \geq (r-1)n$.

Now, if $n=2^k$, choose $j \geq n^2-n$, and set in (3) $r=n$, obtaining, in view of (1),

$$x_j \equiv x_{j-n^2} + x_{j-n} \equiv x_{j-n^2} + (x_j - x_{j-1}).$$

Hence, $x_{j-n^2} \equiv x_{j-1}$, showing that the sequence x_j is periodic with period n^2-1. Thus, the string (2) of ones reappears after exactly n^2-1 steps; claim (b) results.

And if $n=2^k+1$, choose $j \geq n^2-2n$, and set in (3) $r=n-1$, obtaining, in view of (1),

$$x_j \equiv x_{j-n^2+n} + x_{j-n+1} \equiv x_{j-n^2+n} + (x_{j+1} - x_j) \equiv x_{j-n^2+n} - x_j + x_j,$$

(because $x \equiv -x \pmod 2$). Hence $x_{j-n^2+n} \equiv x_{j+1}$, showing that the sequence x_j is periodic with period n^2-n+1 and proving claim (c).

15.4 Exercise 15.2

1. The sequence $a_0, a_1, a_2, \ldots$ satisfies

$$a_{m+n} + a_{m-n} = \frac{1}{2}(a_{2m} + a_{2n}),$$

for all nonnegative integers m and n with $m \geq n$. If $a_1 = 1$, determine a_n.

2. Find a formula for the general term of the sequence

$$1, 2, 2, 3, 3, 3, 4, 4, 4, 4, 5, 5, 5, 5, 5, \ldots$$

3. Prove that $\lim_{n\to\infty} \sqrt[n]{n} = 1$.

4. $a_0 = a_1 = 1, \quad a_{n+1} = a_{n-1}a_n + 1, \quad (n \geq 1)$. Show that $4 \nmid a_{1964}$.

5. There does not exist a monotonically increasing sequence of nonnegative integers $a_1, a_2, a_3, \ldots$ so that $a_{nm} = a_n + a_m$ for all $n, m \in \mathbb{N}$.

6.Let

$$a_n = \frac{2^3 - 1}{2^3 + 1} \cdot \frac{3^3 - 1}{3^3 + 1} \cdot \frac{4^3 - 1}{4^3 + 1} \cdots \frac{n^3 - 1}{n^3 + 1}.$$

Find $\lim_{n\to\infty} a_n$.

7. All terms of the sequence $a_1 = a_2 = a_3 = 1$, $a_{n+1} = \frac{(1 + a_{n-1}a_n)}{a_{n-2}}$ are integers.

8. The sequence x_n is defined by $x_1 = 1/2$, $x_{k+1} = x_k^2 + x_k$. Find the integer part of the sum

$$\frac{1}{x_1 + 1} + \frac{1}{x_2 + 1} + \cdots + \frac{1}{x_{100} + 1}.$$

15.5 Convergence of Monotone Sequence

Definition Let $X = (x_n)$ be a sequence of real numbers. We say that X is **increasing** if it satisfies the inequalities

$$x_1 \leq x_2 \leq \cdots \leq x_n \leq x_{n+1} \leq \cdots .$$

We say that X is **decreasing** if it satisfies the inequalities

$$x_1 \geq x_2 \geq \cdots \geq x_n \geq x_{n+1} \geq \cdots .$$

We say that X is **monotone** if it is either increasing or decreasing.

The following sequences are increasing:

$$(1, 2, 3, 4, \ldots, n, \ldots), \quad (1, 2, 2, 3, 3, 3, \ldots), \quad (a, a^2, a^3, \ldots, a^n, \ldots) \text{ if } a > 1.$$

The following sequences are decreasing:

$$(1, 1/2, 1/3, \ldots, 1/n, \ldots), \quad (1, 1/2, 1/2^2, \ldots, 1/2^{n-1}, \ldots), \quad (b, b^2, b^3, \ldots, b^n, \ldots) \text{ if } 0 < b < 1.$$

The following sequences are not monotone:

$$(+1, -1, +1, \ldots, (-1)^{n+1}, \ldots), \quad (-1, +2, -3, \ldots, (-1)^n, \ldots).$$

The following sequences are not monotone, but they are "ultimately" monotone:

$$(7, 6, 2, 1, 2, 3, 4, \ldots), \quad (-2, 0, 1, 1/2, 1/3, 1/4, \ldots).$$

Monotone Convergence Theorem A monotone sequence of real numbers is convergent if and only if it is bounded. Further:

(a) If $X = (x_n)$ is a bounded increasing sequence, then

$$\lim(x_n) = \sup\{x_n : n \in \mathbb{N}\}.$$

(b) If $Y = (y_n)$ is a bounded decreasing sequence, then

$$\lim(y_n) = \inf\{y_n : n \in \mathbb{N}\}.$$

Proof. We already know that a convergent sequence must be bounded. Conversely, let X be a bounded monotone sequence. Then X is either increasing or decreasing.

(a) We first treat the case where $X = (x_n)$ is a bounded, increasing sequence. Since X is bounded, there exists a real number M such that $x_n \leq M$ for all $n \in \mathbb{N}$. According to the Completeness Property the supremum $x^* = \sup\{x_n : n \in \mathbb{N}\}$ exists in $\mathbb{R}$; we will show that $x^* = \lim(x_n)$.

If $\epsilon > 0$ is given, then $x^* - \epsilon$ is not an upper bound of the set $\{x_n : n \in \mathbb{N}\}$, and hence there exists a member of set x_K such that $x^* - \epsilon < x_K$. The fact that X is an increasing sequence implies that $x_K \leq x_n$ whenever $n \geq K$, so that

$$x^* - \epsilon < x_K \leq x_n \leq x^* < x^* + \epsilon \quad \text{for all } n \geq K.$$

Therefore we have

$$|x_n - x^*| < \epsilon \quad \text{for all } n \geq K.$$

Since $\epsilon > 0$ is arbitrary, we conclude that (x_n) converges to x^*.

(b) If $Y = (y_n)$ is a bounded decreasing sequence, then it is clear that $X := -Y = (-y_n)$ is a bounded increasing sequence. It was shown in part (a) that $\lim X = \sup\{-y_n : n \in \mathbb{N}\}$. Now $\lim X = -\lim Y$ and also, we have

$$\sup\{-y_n : n \in \mathbb{N}\} = -\inf\{y_n : n \in \mathbb{N}\}.$$

Therefore $\lim Y = -\lim X = \inf\{y_n : n \in \mathbb{N}\}$.

Example 1: Let $a_n = \frac{1}{1^2} + \frac{1}{2^2} + \cdots \frac{1}{n^2}$ $n \geq 1$ then is $\{a_n\}$ convergent.

Solution: Observe that if we look at $a_{n+1} - a_n = \frac{1}{(n+1)^2}$ which implies that $\{a_n\}$ is an increasing sequence and hence monotonic. Also we have

$$a_n = \frac{1}{1^2} + \frac{1}{2^2} + \cdots \frac{1}{n^2} < 1 + \frac{1}{1.2} + \frac{1}{2.3} + \cdots \frac{1}{(n-1)n} = 2 - \frac{1}{n} < 2$$

Thus we can say that $\{a_n\}$ is bounded. Hence by monotone convergence theorem we can say that $\{a_n\}$ is bounded.

Note: The Monotone Convergence theorem only tells us if the sequence is convergent or not. It doesn't tell us what the limit is.

Example 2: Suppose $\{a_n\}$ is a sequence satisfying

$$a_{n+1} = \frac{3a_n}{2 + a_n} \text{ for each } n \geq 1$$

1. If $0 < a_1 < 1$, then show that the sequence a_n in increasing and hence show that $\lim a_n = 1$
2. If $a_1 > 1$, then show that the sequence a_n in increasing and hence show that $\lim a_n = 1$

Solution:

1. First we show that $0 < a_n < 1$ for all $n \in \mathbb{N}$. Let us prove this using induction on n. The base case is already given. The induction case can be shown as follows

   $$a_n = \frac{3a_n}{2 + a_n} < \frac{2 + a_n}{2 + a_n} = 1$$

   Next we show that a_n is increasing. Observe that

   $$a_{n+1} - a_n = \frac{3a_n}{2 + a_n} - a_n = \frac{a_n(1 - a_n)}{2 + a_n} > 0$$

   The last inequality follows because $0 < a_n < 1$. Thus we got that a_n is bounded and monotonic. Hence the sequence is convergent. Now let us assume that $l = \lim a_n$. The applying limit on both sides of the recursive relation we get that

   $$l = \frac{3l}{2 + l}$$

   On solving this we get that $l = 1$ or $l = 0$. Since the sequence is of positive numbers, hence the only possibility is $l = 1$.

2. Similar to 1. Prove that $a_n > 1$ for all n and then show that a_n is a decreasing sequence. Then solve for l

We conclude this section by introducing a sequence that converges to one of the most important "transcendental" numbers in mathematics, second in importance only to π.

Example 3: Let $e_n := (1 + \frac{1}{n})^n$ for $n \in \mathbb{N}$. We will now show that the sequence $E = (e_n)$ is bounded and increasing; hence it is convergent. The limit of this sequence is the famous Euler number e, whose approximate value is $2.718281828459045\ldots$, which is taken as the base of the "natural" logarithm.

If we apply the Binomial Theorem, we have

$$e_n = \left(1 + \frac{1}{n}\right)^n = 1 + \frac{n}{1} \cdot \frac{1}{n} + \frac{n(n-1)}{2!} \cdot \frac{1}{n^2} + \frac{n(n-1)(n-2)}{3!} \cdot \frac{1}{n^3} + \cdots + \frac{n(n-1)\cdots 2 \cdot 1}{n!} \cdot \frac{1}{n^n}.$$

If we divide the powers of n into the terms in the numerators of the binomial coefficients, we get

$$e_n = 1 + 1 + \frac{1}{2!}\left(1 - \frac{1}{n}\right) + \frac{1}{3!}\left(1 - \frac{1}{n}\right)\left(1 - \frac{2}{n}\right) + \cdots + \frac{1}{n!}\left(1 - \frac{1}{n}\right)\left(1 - \frac{2}{n}\right)\cdots\left(1 - \frac{n-1}{n}\right).$$

Similarly we have

$$e_{n+1} = 1 + 1 + \frac{1}{2!}\left(1 - \frac{1}{n+1}\right) + \frac{1}{3!}\left(1 - \frac{1}{n+1}\right)\left(1 - \frac{2}{n+1}\right)$$
$$+ \cdots + \frac{1}{(n+1)!}\left(1 - \frac{1}{n+1}\right)\left(1 - \frac{2}{n+1}\right)\cdots\left(1 - \frac{n-1}{n+1}\right).$$

Note that the expression for e_n contains $n+1$ terms, while that for e_{n+1} contains $n+2$ terms. Moreover, each term appearing in e_n is less than or equal to the corresponding term in e_{n+1}, and e_{n+1} has one more positive term. Therefore we have $2 \le e_1 < e_2 < \cdots < e_n < e_{n+1} < \cdots$, so that the terms of E are increasing.

To show that the terms of E are bounded above, we note that if $p = 1, 2, \ldots, n$, then $(1 - p/n) < 1$. Moreover $2^{p-1} \le p!$ so that $1/p! \le 1/2^{p-1}$. Therefore, if $n > 1$, then we have

$$2 < e_n < 1 + 1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^{n-1}}.$$

Since it can be verified that

$$1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^{n-1}} = 1 - \frac{1}{2^{n-1}} < 1,$$

we deduce that $2 < e_n < 3$ for all $n \in \mathbb{N}$. The Monotone Convergence Theorem implies that the sequence E converges to a real number that is between 2 and 3. We define the number e to be the limit of this sequence.

15.6 Subsequence and Bolzano Weierstrass Theorem

Definition: Let $X = (x_n)$ be a sequence of real numbers and let $n_1 < n_2 < \cdots < n_k < \cdots$ be a strictly increasing sequence of natural numbers. Then the sequence $X' = (x_{n_k})$ given by

$$(x_{n_1}, x_{n_2}, \cdots, x_{n_k}, \cdots)$$

is called a **subsequence** of X.

For example, if $X := \left(\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \cdots\right)$, then the selection of even indexed terms produces the subsequence

$$X' = \left(\frac{1}{2}, \frac{1}{4}, \frac{1}{6}, \cdots, \frac{1}{2k}, \cdots\right),$$

where $n_1 = 2, n_2 = 4, \cdots, n_k = 2k, \cdots$. Other subsequences of $X = \left(\frac{1}{n}\right)$ are the following:

$$\left(\frac{1}{1}, \frac{1}{3}, \frac{1}{5}, \cdots, \frac{1}{2k-1}, \cdots\right), \quad \left(\frac{1}{2!}, \frac{1}{4!}, \frac{1}{6!}, \cdots, \frac{1}{(2k)!}, \cdots\right).$$

The following sequences are **not** subsequences of $X = \left(\frac{1}{n}\right)$:

$$\left(\frac{1}{2}, \frac{1}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{6}, \frac{1}{5}, \cdots\right), \quad \left(\frac{1}{1}, 0, \frac{1}{3}, 0, \frac{1}{5}, 0, \cdots\right).$$

Theorem: If a sequence $X = (x_n)$ of real numbers converges to a real number x, then any subsequence $X' = (x_{n_k})$ of X also converges to x.

Proof. Let $\varepsilon > 0$ be given and let $K(\varepsilon)$ be such that if $n \ge K(\varepsilon)$, then $|x_n - x| < \varepsilon$. Since $n_1 < n_2 < \cdots < n_k < \cdots$ is an increasing sequence of natural numbers, it is easily proved (by Induction) that $n_k \ge k$. Hence, if $k \ge K(\varepsilon)$, we also have $n_k \ge k \ge K(\varepsilon)$ so that $|x_{n_k} - x| < \varepsilon$. Therefore the subsequence (x_{n_k}) also converges to x.

While not every sequence is a monotone sequence, we will now show that every sequence has a monotone subsequence.

Monotone Subsequence Theorem If $X = (x_n)$ is a sequence of real numbers, then there is a subsequence of X that is monotone.

Proof. For the purpose of this proof, we will say that the m-th term x_m is a "peak" if $x_m \geq x_n$ for all n such that $n \geq m$. (That is, x_m is never exceeded by any term that follows it in the sequence.) Note that, in a decreasing sequence, every term is a peak, while in an increasing sequence, no term is a peak.

We will consider two cases, depending on whether X has infinitely many, or finitely many, peaks.

Case 1: X has infinitely many peaks. In this case, we list the peaks by increasing subscripts: $x_{m_1}, x_{m_2}, \cdots, x_{m_k}, \cdots$. Since each term is a peak, we have

$$x_{m_1} \geq x_{m_2} \geq \cdots \geq x_{m_k} \geq \cdots .$$

Therefore, the subsequence (x_{m_k}) of peaks is a decreasing subsequence of X.

Case 2: X has a finite number (possibly zero) of peaks. Let these peaks be listed by increasing subscripts: $x_{m_1}, x_{m_2}, \cdots, x_{m_r}$. Let $s_1 := m_r + 1$ be the first index beyond the last peak. Since x_{s_1} is not a peak, there exists $s_2 > s_1$ such that $x_{s_1} < x_{s_2}$. Since x_{s_2} is not a peak, there exists $s_3 > s_2$ such that $x_{s_2} < x_{s_3}$. Continuing in this way, we obtain an increasing subsequence (x_{s_k}) of X.

It is not difficult to see that a given sequence may have one subsequence that is increasing, and another subsequence that is decreasing.

We will now use the Monotone Subsequence Theorem to prove the Bolzano-Weierstrass Theorem, which states that every bounded sequence has a convergent subsequence. Because of the importance of this theorem we will also give a second proof of it based on the Nested Interval Property.

The Bolzano-Weierstrass Theorem A bounded sequence of real numbers has a convergent subsequence.

First Proof. It follows from the Monotone Subsequence Theorem that if $X = (x_n)$ is a bounded sequence, then it has a subsequence $X' = (x_{n_k})$ that is monotone. Since this subsequence is also bounded, it follows from the Monotone Convergence Theorem that the subsequence is convergent.

Second Proof. Since the set of values $\{x_n : n \in \mathbb{N}\}$ is bounded, this set is contained in an interval $I_1 := [a, b]$. We take $n_1 := 1$.

We now bisect I_1 into two equal subintervals I_1' and I_1'', and divide the set of indices $\{n \in \mathbb{N} : n > 1\}$ into two parts:

$$A_1 := \{n \in \mathbb{N} : n > n_1, x_n \in I_1'\}, \quad B_1 := \{n \in \mathbb{N} : n > n_1, x_n \in I_1''\}.$$

If A_1 is infinite, we take $I_2 := I_1'$ and let n_2 be the smallest natural number in A_1. (See 1.2.1.) If A_1 is a finite set, then B_1 must be infinite, and we take $I_2 := I_1''$ and let n_2 be the smallest natural number in B_1.

We now bisect I_2 into two equal subintervals I_2' and I_2'', and divide the set $\{n \in \mathbb{N} : n > n_2\}$ into two parts:

$$A_2 := \{n \in \mathbb{N} : n > n_2, x_n \in I_2'\}, \quad B_2 := \{n \in \mathbb{N} : n > n_2, x_n \in I_2''\}.$$

If A_2 is infinite, we take $I_3 := I_2'$ and let n_3 be the smallest natural number in A_2. If A_2 is a finite set, then B_2 must be infinite, and we take $I_3 := I_2''$ and let n_3 be the smallest natural number in B_2.

We continue in this way to obtain a sequence of nested intervals $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_k \supseteq \cdots$ and a subsequence (x_{n_k}) of X such that $x_{n_k} \in I_k$ for $k \in \mathbb{N}$. Since the length of I_k is equal to $(b-a)/2^{k-1}$, it follows that there is a (unique) common point $\xi \in I_k$ for all $k \in \mathbb{N}$. Moreover, since x_{n_k} and ξ both belong to I_k, we have

$$|x_{n_k} - \xi| \leq \frac{b-a}{2^{k-1}},$$

whence it follows that the subsequence (x_{n_k}) of X converges to ξ.

Theorem Let $X = (x_n)$ be a bounded sequence of real numbers and let $x \in \mathbb{R}$ have the property that every convergent subsequence of X converges to x. Then the sequence X converges to x

Proof. Suppose $M > 0$ is a bound for the sequence X so that $|x_n| \leq M$ for all $n \in \mathbb{N}$. If X does not converge to x, we have that there exist $\epsilon_0 > 0$ and a subsequence $X' = (x_{n_k})$ of X such that

$$|x_{n_k} - x| \geq \epsilon_0 \quad \text{for all } k \in \mathbb{N}. \tag{1}$$

Since X' is a subsequence of X, the number M is also a bound for X'. Hence the Bolzano-Weierstrass Theorem implies that X' has a convergent subsequence X''. Since X'' is also a subsequence of X, it converges to x by hypothesis. Thus, its terms ultimately belong to the ϵ_0-neighborhood of x, contradicting (1).

15.7 Cauchy Criteria

Definition A sequence $X = (x_n)$ of real numbers is said to be a *Cauchy sequence* if for every $\epsilon > 0$ there exists a natural number $H(\epsilon)$ such that for all natural numbers $n, m \geq H(\epsilon)$, the terms x_n, x_m satisfy $|x_n - x_m| < \epsilon$.

The significance of the concept of Cauchy sequence lies in the main theorem of this section, which asserts that a sequence of real numbers is convergent if and only if it is a Cauchy sequence. This will give us a method of proving a sequence converges without knowing the limit of the sequence.

However, we will first highlight the definition of Cauchy sequence in the following examples.

Exammple 1: The sequence $\left(\frac{1}{n}\right)$ is a Cauchy sequence.

Solution: If $\epsilon > 0$ is given, we choose a natural number $H = H(\epsilon)$ such that $H > 2/\epsilon$. Then if $m, n \geq H$, we have $1/n \leq 1/H < \epsilon/2$ and similarly $1/m < \epsilon/2$. Therefore, it follows that if $m, n \geq H$, then

$$\left|\frac{1}{n} - \frac{1}{m}\right| \leq \frac{1}{n} + \frac{1}{m} < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Since $\epsilon > 0$ is arbitrary, we conclude that $\left(\frac{1}{n}\right)$ is a Cauchy sequence.

Exammple 2: The sequence $(1 + (-1)^n)$ is *not* a Cauchy sequence.

Solution: The negation of the definition of Cauchy sequence is: There exists $\epsilon_0 > 0$ such that for every H there exist at least one $n > H$ and at least one $m > H$ such that $|x_n - x_m| \geq \epsilon_0$. For the terms $x_n := 1 + (-1)^n$, we observe that if n is even, then $x_n = 2$ and $x_{n+1} = 0$. If we take $\epsilon_0 = 2$, then for any H we can choose an even number $n > H$ and let $m := n + 1$ to get

$$|x_n - x_{n+1}| = 2 = \epsilon_0.$$

We conclude that (x_n) is not a Cauchy sequence.

Lemma: If $X = (x_n)$ is a convergent sequence of real numbers, then X is a Cauchy sequence.

Proof. If $x := \lim X$, then given $\epsilon > 0$ there is a natural number $K(\epsilon/2)$ such that if $n \geq K(\epsilon/2)$ then $|x_n - x| < \epsilon/2$. Thus, if $H(\epsilon) := K(\epsilon/2)$ and if $n, m \geq H(\epsilon)$, then we have

$$|x_n - x_m| = |(x_n - x) + (x - x_m)| \leq |x_n - x| + |x_m - x| < \epsilon/2 + \epsilon/2 = \epsilon.$$

Since $\epsilon > 0$ is arbitrary, it follows that (x_n) is a Cauchy sequence.

Lemma: A Cauchy sequence of real numbers is bounded.

Proof. Let $X := (x_n)$ be a Cauchy sequence and let $\epsilon := 1$. If $H := H(1)$ and $n \geq H$, then $|x_n - x_H| < 1$. Hence, by the Triangle Inequality, we have $|x_n| \leq |x_H| + 1$ for all $n \geq H$. If we set

$$M := \sup\{|x_1|, |x_2|, \ldots, |x_{H-1}|, |x_H| + 1\},$$

then it follows that $|x_n| \leq M$ for all $n \in \mathbb{N}$.

Example 3: Let $X = (x_n)$ be defined by

$$x_1 := 1, \quad x_2 := 2, \quad \text{and} \quad x_n := \frac{1}{2}(x_{n-2} + x_{n-1}) \quad \text{for} \quad n > 2.$$

It can be shown by induction that $1 \leq x_n \leq 2$ for all $n \in \mathbb{N}$. (Do so.) Some calculation shows that the sequence X is not monotone. However, since the terms are formed by averaging, it is readily seen that

$$|x_n - x_{n+1}| = \frac{1}{2^{n-1}} \quad \text{for} \quad n \in \mathbb{N}.$$

(Prove this by induction.) Thus, if $m > n$, we may employ the triangle inequality to obtain

$$\begin{aligned}
|x_n - x_m| &\le |x_n - x_{n+1}| + |x_{n+1} - x_{n+2}| + \cdots + |x_{m-1} - x_m| \\
&= \frac{1}{2^{n-1}} + \frac{1}{2^n} + \cdots + \frac{1}{2^{m-2}} \\
&= \frac{1}{2^{n-1}}\left(1 + \frac{1}{2} + \cdots + \frac{1}{2^{m-n-1}}\right) \\
&< \frac{1}{2^{n-2}}.
\end{aligned}$$

Therefore, given $\epsilon > 0$, if n is chosen so large that $1/2^n < \epsilon/4$ and $m \ge n$, then it follows that $|x_n - x_m| < \epsilon$. Therefore, X is a Cauchy sequence in $\mathbb{R}$. By the Cauchy Criterion we infer that the sequence X converges to a number x.

To evaluate the limit x, we might first "pass to the limit" in the rule of definition

$$x = \frac{1}{2}(x_{n-1} + x_{n-2})$$

to conclude that x must satisfy the relation $x = \frac{1}{2}(x + x)$, which is true, but not informative. Hence we must try something else.

Since X converges to x, so does the subsequence X' with odd indices. By induction, the reader can establish that

$$x_{2n+1} = 1 + \frac{1}{2} + \frac{1}{2^3} + \cdots + \frac{1}{2^{2n-1}} = 1 + \frac{2}{3}\left(1 - \frac{1}{4^n}\right).$$

It follows from this (how?) that $x = \lim X' = 1 + \frac{2}{3} = \frac{5}{3}$.

Example 4: Let $Y = (y_n)$ be the sequence of real numbers given by

$$y_1 := \frac{1}{1!}, \quad y_2 := \frac{1}{1!} - \frac{1}{2!}, \quad y_n := \frac{1}{1!} - \frac{1}{2!} + \cdots + \frac{(-1)^{n+1}}{n!}, \ldots$$

Clearly, Y is not a monotone sequence. However, if $m > n$, then

$$y_m - y_n = \frac{(-1)^{n+2}}{(n+1)!} + \frac{(-1)^{n+3}}{(n+2)!} + \cdots + \frac{(-1)^{m+1}}{m!}.$$

Since $2^{r-1} \le r!$, it follows that if $m > n$, then (why?)

$$|y_m - y_n| \le \frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \cdots + \frac{1}{m!} \le \frac{1}{2^{n-1}} + \frac{1}{2^n} + \cdots + \frac{1}{2^{m-1}} < \frac{1}{2^{n-1}}.$$

Therefore, it follows that (y_n) is a Cauchy sequence. Hence it converges to a limit y. At the present moment, we cannot evaluate y directly; however, passing to the limit (with respect to m) in the above inequality, we obtain

$$|y_n - y| \le \frac{1}{2^{n-1}}.$$

Hence, we can calculate y to any desired accuracy by calculating the terms y_n for sufficiently large n. The reader should do this and show that y is approximately equal to 0.632120559. (The exact value of y is $1 - 1/e$).

Example 5: The sequence $\left(\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n}\right)$ diverges.

Let $H := (h_n)$ be the sequence defined by

$$h_n := \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n} \quad \text{for } n \in \mathbb{N},$$

If $m > n$, then

$$h_m - h_n = \frac{1}{n+1} + \cdots + \frac{1}{m}.$$

Since each of these $m - n$ terms exceeds $1/m$, then $h_m - h_n > (m-n)/m = 1 - n/m$. In particular, if $m = 2n$, we have $h_{2n} - h_n > \frac{1}{2}$. This shows that H is not a Cauchy sequence (why?); therefore, H is not a convergent sequence. $\frac{1}{n}$ is divergent.

15.8 Exercise 15.3

1. Let $A_1 \geq A_2 \geq \cdots \geq A_k \geq 0$. Evaluate

$$\lim_{n\to\infty} \left(A_1^n + A_2^n + \cdots + A_k^n\right)^{1/n}.$$

2. Let $x_0 = 1$ and

$$x_n = \frac{3 + 2x_{n-1}}{3 + x_{n-1}}$$

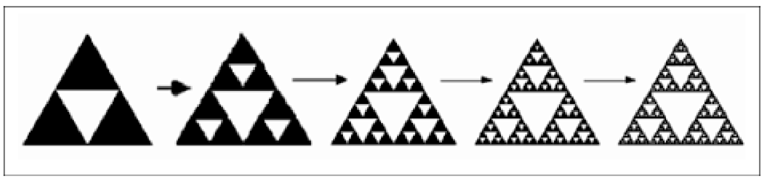
for $n = 1, 2, \ldots$. Prove that $x_\infty = \lim_{n\to\infty} x_n$ exists, and find its value.

3. Let α be a number in $(0, 1)$. Prove that any sequence (x_n) of real numbers satisfying the recurrence relation

$$x_{n+1} = \alpha x_n + (1-\alpha)x_{n-1}$$

has a limit, and find an expression for the limit in terms of α, x_0, and x_1.

4. Start with an equilateral triangle with unit side length. Subdivide it into four smaller congruent equilateral triangles and remove the central triangle. Repeat this step with each of the remaining smaller triangles.



5.Prove that

$$\lim_{n\to\infty} \left(\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n}\right) = \log 2.$$

6. Let $a_1 = 1$ and $a_n = n(a_{n-1} + 1)$ for all $n \geq 2$. Define:

$$P_n = \left(1 + \frac{1}{a_1}\right)\left(1 + \frac{1}{a_2}\right)\cdots\left(1 + \frac{1}{a_n}\right).$$

Compute $\lim_{n\to\infty} P_n$.

7. Consider the sequence

$$u_n = \sum_{r=1}^{n} \frac{r}{2^r}, \quad n \geq 1.$$

Then the limit of u_n as $n \to \infty$ is

15.9 Sequences MCQ

1. The limit of $\frac{1}{n^4}\sum_{k=1}^{n} k(k+2)(k+4)$ as $n \to \infty$

(A) exists and equals $\frac{1}{4}$; (B) exists and equals 0;

(C) exists and equals $\frac{1}{8}$; (D) does not exist.

2. The limit of the sequence $\sqrt{2}, \sqrt{2\sqrt{2}}, \sqrt{2\sqrt{2\sqrt{2}}}, \ldots$ is

(A) 1; (B) 2; (C) $2\sqrt{2}$; (D) ∞.

3. Let

$$P_n = \frac{2^3-1}{2^3+1} \cdot \frac{3^3-1}{3^3+1} \cdot \ldots \cdot \frac{n^3-1}{n^3+1}; \quad n = 2, 3, \ldots$$

Then find the limit

$$\lim_{n\to\infty} P_n \quad \text{is}$$

(A) $\frac{3}{4}$; (B) $\frac{7}{11}$; (C) $\frac{2}{3}$; (D) $\frac{1}{2}$.

4. Let $a_1 = 1$ and $a_n = n(a_{n-1}+1)$ for $n = 2, 3, \ldots$. Define

$$P_n = \left(1 + \frac{1}{a_1}\right)\left(1 + \frac{1}{a_2}\right)\cdots\left(1 + \frac{1}{a_n}\right).$$

Then $\lim_{n\to\infty} P_n$ is

(A) $1+e$; (B) e; (C) 1; (D) ∞.

5. Let x be a real number. Let $a_0 = x$, $a_1 = \sin x$ and, in general, $a_n = \sin a_{n-1}$. Then the sequence $\{a_n\}$

(A) oscillates between -1 and $+1$, unless x is a multiple of π;

(B) converges to 0 whatever x;

(C) converges to 0 if and only if x is a multiple of π;

(D) sometimes converges and sometimes oscillates depending on x.

6. If k is an integer such that

$$\lim_{n\to\infty}\left[\left(\cos\frac{k\pi}{4}\right)^n - \left(\cos\frac{k\pi}{6}\right)^n\right] = 0,$$

then

(A) k is divisible neither by 4 nor by 6;

(B) k must be divisible by 12, but not necessarily by 24;

(C) k must be divisible by 24;

(D) either k is divisible by 24 or k is divisible neither by 4 nor by 6.

7. The limit of $\sqrt{x(\sqrt{x+4}-\sqrt{x})}$ as $x \to \infty$

(A) does not exist; (B) exists and equals 0;

(C) exists and equals $\frac{1}{2}$; (D) exists and equals 2.

8. If $a_n = \left(1+\frac{1}{n^2}\right)\left(1+\frac{2^2}{n^2}\right)^2\left(1+\frac{3^2}{n^2}\right)^3\cdots\left(1+\frac{n^2}{n^2}\right)^n$, then

$$\lim_{n\to\infty} a_n^{-1/n^2}$$

is
(A) 0; (B) 1; (C) e; (D) $\sqrt{e}/2$.

9. Let $R_n = 2+\sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}$ (n square root signs). Then

$$\lim_{n\to\infty} R_n$$

equals
(A) 4; (B) 8; (C) 16; (D) e^2.

10. Let $a_1 = 2$ and for all natural number n, define $a_{n+1} = a_n(a_n+1)$. Then, as $n\to\infty$, the number of prime factors of a_n
(A) goes to infinity; (B) goes to a finite limit; (C) oscillates boundedly; (D) oscillates unboundedly.

11. Define the sequence $\{a_n\}$ by $a_1 = 1$, $a_2 = \frac{e}{2}$, $a_3 = \frac{e^2}{4}$, $a_4 = \frac{e^3}{8}$, ... Then $\lim_{n\to\infty} a_n$ is
(A) 0; (B) 1; (C) e^e; (D) infinite.

12. $\sum_{n=1}^{\infty} \frac{n^2}{n!}$ equals

(A) e; (B) $2e$; (C) e^2; (D) ∞.

13. The limit

$$\lim_{n\to\infty}\left(1+\frac{1}{n^2+\cos n}\right)^{n^2+n}$$

(A) does not exist (B) equals 1 (C) equals e (D) equals e^2.

14. The limit

$$\lim_{n\to\infty}\left(\frac{1}{6}+\frac{1}{24}+\frac{1}{60}+\frac{1}{120}+\cdots+\frac{1}{n^3-n}\right)$$

equals

(A) 1; (B) $\frac{1}{2}$; (C) $\frac{1}{4}$; (D) $\frac{1}{8}$.

15. The limit

$$\lim_{n\to\infty}\frac{\pi}{2n}\sum_{j=1}^{2n}\sin\left(\frac{j\pi}{2n}\right)$$

is equal to

(A) 0; (B) π; (C) 2; (D) 1.

16. The value of

$$\lim_{n\to\infty}\frac{\sum_{r=0}^{n}\binom{2n}{2r}3^r}{\sum_{r=0}^{n-1}\binom{2n}{2r+1}3^r}$$

is

(A) 0; (B) 1; (C) $\sqrt{3}$; (D) $\frac{\sqrt{3}-1}{\sqrt{3}+1}$.

17. For any real number x, let $\tan^{-1}(x)$ denote the unique real number θ in $(-\pi/2,\pi/2)$ such that $\tan\theta = x$. Then

$$\lim_{n\to\infty}\sum_{m=1}^{n}\tan^{-1}\left(\frac{1}{1+m+m^2}\right)$$

(A) is equal to $\pi/2$; (B) is equal to $\pi/4$;

(C) does not exist; (D) none of the above.

18. The value of

$$\lim_{n\to\infty} \sum_{r=1}^{n} \frac{6n}{9n^2 - r^2}$$

is

(A) 0; (B) $\log \frac{3}{2}$; (C) $\log \frac{2}{3}$; (D) $\log 2$.

19. Let $x_1 < -1$ and $x_{n+1} = \frac{x_n}{1+x_n}$ for all $n \geq 1$. Then

(A) $\{x_n\} \to -1$ as $n \to \infty$; (B) $\{x_n\} \to 1$ as $n \to \infty$;

(C) $\{x_n\} \to 0$ as $n \to \infty$; (D) $\{x_n\}$ diverges.

20. Let $\{a_n\}$ be a sequence of positive real numbers such that $\lim_{n\to\infty} 2^n(a_n + a_{n+1})$ is finite. Then

(A) $\{a_n\}$ converges to 1; (B) $\{a_n\}$ converges to 0;

(C) $\{a_n\}$ converges to $1/2$; (D) $\{a_n\}$ converges to $1/\sqrt{2}$.

ANSWER KEY

1	2	3	4	5	6	7	8	9	10
A	B	C	B	B	D	D	D	A	A
11	12	13	14	15	16	17	18	19	20
D	B	C	C	B	C	D	C	C	B

15.10 Series

Consider the sequence $\{a_n\}_{n=1}^{\infty}$. The sum of the terms of this sequence, $a_1 + a_2 + a_3 + \cdots$, forms a series.

For the series $S = 1 + (-1) + 1 + (-1) + \cdots$, we can attempt to evaluate it in different ways:

$$\begin{aligned} S &= 1 + (-1) + 1 + (-1) + \cdots \\ &= (1 + (-1)) + (1 + (-1)) + \cdots \\ &= 0 + 0 + 0 + \cdots = 0. \end{aligned}$$

Alternatively,

$$\begin{aligned} S &= 1 + (-1) + 1 + (-1) + \cdots \\ &= 1 + ((-1) + 1) + (-1) + \cdots \\ &= 1 + 0 + 0 + \cdots = 1. \end{aligned}$$

One might also consider:

$$\begin{aligned} S &= 1 + (-1) + 1 + (-1) + \cdots \\ &= 1 - (1 + (-1) + 1 + (-1) + \cdots) \\ &= 1 - S \implies S = \frac{1}{2}. \end{aligned}$$

Hence, we have three different results for S: 0, 1, or $\frac{1}{2}$. This leads us to question the definition of the sum of such a series.

To formally address this, we define the series sum as:

$$\sum_{n=1}^{\infty} a_n \stackrel{\text{def}}{=} \lim_{N\to\infty} \sum_{n=1}^{N} a_n.$$

Define $S_N = a_1 + a_2 + \cdots + a_N$ for $N \geq 1$. These are called "partial sums". We say that the series $\sum_{n=1}^{\infty} a_n$ converges if the sequence of partial sums $\{S_N\}_{N=1}^{\infty}$ converges to a real number.

Example:

Let $a_n = (-1)^n$ for $n \geq 1$.

$$S_n = a_1 + a_2 + \cdots + a_n = \begin{cases} 0 & \text{if } n \text{ is even} \\ -1 & \text{if } n \text{ is odd} \end{cases}$$

Thus, $\{S_n\}_{N=1}^{\infty}$ does not converge. Therefore, the series $\sum_{n=1}^{\infty} a_n$ does not have a meaning.

So, it does not make any sense to write

$$\text{“let } S = 1 + (-1) + 1 + (-1) + \cdots\text{”}.$$

Example 1: Consider the sequence $X := \{r^n\}_{n=0}^{\infty}$ where $r \in \mathbb{R}$, which generates the geometric series:

$$\sum_{n=0}^{\infty} r^n = 1 + r + r^2 + \cdots .$$

We will show that if $|r| < 1$, then this series converges to $\frac{1}{1-r}$. Indeed, if $s_n := 1 + r + r^2 + \cdots + r^n$ for $n \geq 0$, and if we multiply s_n by r and subtract the result from s_n, we obtain (after some simplification):

$$s_n(1-r) = 1 - r^{n+1}.$$

Therefore, we have

$$s_n = \frac{1}{1-r} - \frac{r^{n+1}}{1-r},$$

from which it follows that

$$\left| s_n - \frac{1}{1-r} \right| = \left| \frac{r^{n+1}}{1-r} \right|.$$

Since $|r|^{n+1} \to 0$ when $|r| < 1$, it follows that the geometric series converges to $\frac{1}{1-r}$ when $|r| < 1$.

Example 2: Consider the series

$$\sum_{n=1}^{\infty} \frac{1}{n(n+1)} = \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots .$$

By a stroke of insight, we note that

$$\frac{1}{k(k+1)} = \frac{1}{k} - \frac{1}{k+1}.$$

Hence, on adding these terms from $k = 1$ to $k = n$ and noting the telescoping that takes place, we obtain

$$s_n = 1 - \frac{1}{n+1},$$

whence it follows that $s_n \to 1$. Therefore, the series converges to 1.

The nth Term Test If the series $\sum x_n$ converges, then $\lim(x_n) = 0$.

By Definition, the convergence of $\sum x_n$ requires that $\lim(s_k)$ exists. Since $x_n = s_n - s_{n-1}$, then $\lim(x_n) = \lim(s_n) - \lim(s_{n-1}) = 0$.

Cauchy Criterion for Series The series $\sum x_n$ converges if and only if for every $\epsilon > 0$ there exists $M(\epsilon) \in \mathbb{N}$ such that if $m > n \geq M(\epsilon)$, then

$$|s_m - s_n| = |x_{n+1} + x_{n+2} + \cdots + x_m| < \epsilon.$$

The next result, although limited in scope, is of great importance and utility.

Theorem Let (x_n) be a sequence of nonnegative real numbers. Then the series $\sum x_n$ converges if and only if the sequence $S = (s_k)$ of partial sums is bounded. In this case,

$$\sum_{n=1}^{\infty} x_n = \lim(s_k) = \sup\{s_k : k \in \mathbb{N}\}.$$

Since $x_n > 0$, the sequence S of partial sums is monotone increasing:

$$s_1 \leq s_2 \leq \cdots \leq s_k \leq \cdots .$$

By the Monotone Convergence Theorem, the sequence $S = (s_k)$ converges if and only if it is bounded, in which case its limit equals $\sup\{s_k\}$.

Example 3: The 2-series $\sum_{n=1}^{\infty} \frac{1}{n^2}$ is convergent.

Since the partial sums are monotone, it suffices to show that some subsequence of (s_k) is bounded. If $k_1 := 2^1 - 1 = 1$, then $s_{k_1} = 1$. If $k_2 := 2^2 - 1 = 3$, then

$$s_{k_2} = 1 + \left(\frac{1}{2^2} + \frac{1}{3^2} \right) < 1 + \frac{2}{2^2} = 1 + \frac{1}{2},$$

and if $k_3 := 2^3 - 1 = 7$, then we have

$$s_{k_3} = s_{k_2} + \left(\frac{1}{4^2} + \frac{1}{5^2} + \frac{1}{6^2} + \frac{1}{7^2} \right) < s_{k_2} + \frac{4}{4^2} < 1 + \frac{1}{2} + \frac{1}{2^2}.$$

By Mathematical Induction, we find that if $k_j := 2^j - 1$, then

$$0 < s_{k_j} < 1 + \frac{1}{2} + \left(\frac{1}{2}\right)^2 + \cdots + \left(\frac{1}{2}\right)^{j-1}.$$

Since the term on the right is a partial sum of a geometric series with $r = \frac{1}{2}$, it is dominated by $\frac{1}{1-\frac{1}{2}} = 2$, and hence the 2-series converges.

Example 4: The p-series $\sum_{n=1}^{\infty} \frac{1}{n^p}$ converges when $p > 1$.

Since the argument is very similar to the special case considered in part (c), we will leave some of the details to the reader. As before, if $k_1 := 2^1 - 1 = 1$, then $s_{k_1} = 1$. If $k_2 := 2^2 - 1 = 3$, then since $2^p < 3^p$, we have

$$s_{k_2} = 1 + \left(\frac{1}{2^p} + \frac{1}{3^p} \right) < 1 + \frac{2}{2^p} = 1 + \frac{1}{2^{p-1}}.$$

Further, if $k_3 := 2^3 - 1$, then (how?) it is seen that

$$s_{k_3} < s_{k_2} + \frac{4}{4^p} < 1 + \frac{1}{2^{p-1}} + \frac{1}{4^{p-1}}.$$

Finally, we let $r := 1/2^{p-1}$; since $p > 1$, we have $0 < r < 1$. Using Mathematical Induction, we show that if $k_j := 2^j - 1$, then

$$0 < s_{k_j} < 1 + r + r^2 + \cdots + r^{j-1} < \frac{1}{1-r}.$$

Therefore we get that the p-series converges when $p > 1$.

Example 5: The p-series $\sum_{n=1}^{\infty} \frac{1}{n^p}$ diverges when $0 < p \le 1$.

We will use the elementary inequality $n^p \le n$ when $n \in \mathbb{N}$ and $0 < p \le 1$. It follows that

$$\frac{1}{n} \le \frac{1}{n^p} \quad \text{for } n \in \mathbb{N}.$$

Since the partial sums of the harmonic series are not bounded, this inequality shows that the partial sums of the p-series are not bounded when $0 < p \le 1$. Hence the p-series diverges for these values of p.

Comparison Test Let $X := (x_n)$ and $Y := (y_n)$ be real sequences and suppose that for some $K \in \mathbb{N}$ we have

$$0 \le x_n \le y_n \quad \text{for } n \ge K. \tag{8}$$

(a) Then the convergence of $\sum y_n$ implies the convergence of $\sum x_n$.

(b) The divergence of $\sum x_n$ implies the divergence of $\sum y_n$.

(a) Suppose that $\sum y_n$ converges and, given $\epsilon > 0$, let $M(\epsilon) \in \mathbb{N}$ be such that if $m > n \geq M(\epsilon)$, then

$$y_{n+1} + \cdots + y_m < \epsilon.$$

If $m \geq \sup\{K, M(\epsilon)\}$, then it follows that

$$0 \leq x_{n+1} + \cdots + x_m \leq y_{n+1} + \cdots + y_m < \epsilon,$$

from which the convergence of $\sum x_n$ follows. (b) This statement is the contrapositive of (a).

Since it is sometimes difficult to establish the inequalities (8), the next result is frequently very useful.

Limit Comparison Test Suppose that $X := (x_n)$ and $Y := (y_n)$ are strictly positive sequences and suppose that the following limit exists in $\mathbb{R}$:

$$r := \lim_{n\to\infty} \left(\frac{x_n}{y_n}\right). \tag{9}$$

(a) If $r \neq 0$ then $\sum x_n$ is convergent if and only if $\sum y_n$ is convergent.

(b) If $r = 0$ and if $\sum y_n$ is convergent, then $\sum x_n$ is convergent.

(a) It follows from (9) that there exists $K \in \mathbb{N}$ such that $\frac{1}{2}r \leq \frac{x_n}{y_n} \leq 2r$ for $n \geq K$, whence

$$\left(\frac{1}{2}r\right) y_n \leq x_n \leq (2r)y_n \quad \text{for } n \geq K.$$

If we apply the Comparison Test twice, we obtain the assertion in (a). (b) If $r = 0$, then there exists $K \in \mathbb{N}$ such that

$$0 < x_n \leq y_n \quad \text{for } n \geq K,$$

so that Theorem 3.7.7(a) applies.

Example 6:

(a) The series $\sum_{n=1}^{\infty} \frac{1}{n^2+n}$ converges.

It is clear that the inequality

$$0 < \frac{1}{n^2+n} < \frac{1}{n^2} \quad \text{for } n \in \mathbb{N}$$

is valid. Since the series $\sum \frac{1}{n^2}$ is convergent , we can apply the Comparison Test to obtain the convergence of the given series.

(b) The series $\sum_{n=1}^{\infty} \frac{1}{n^2-n+1}$ is convergent.

If the inequality

$$\frac{1}{n^2-n+1} \leq \frac{1}{n^2} \tag{10}$$

were true, we could argue as in (a). However, (10) is false for all $n \in \mathbb{N}$. The reader can probably show that the inequality

$$0 < \frac{1}{n^2-n+1} \leq \frac{2}{n^2}$$

is valid for all $n \in \mathbb{N}$, and this inequality will work just as well. However, it might take some experimentation to think of such an inequality and then establish it.

Instead, if we take $x_n := \frac{1}{n^2-n+1}$ and $y_n := \frac{1}{n^2}$, then we have

$$\frac{x_n}{y_n} = \frac{n^2}{n^2-n+1} = \frac{1}{1-(1/n)+(1/n^2)} \to 1.$$

Therefore, the convergence of the given series follows from the Limit Comparison Test.

(c) The series $\sum_{n=1}^{\infty} \frac{1}{\sqrt{n+1}}$ is divergent.

This series closely resembles the series $\sum \frac{1}{\sqrt{n}}$ which is a p-series with $p = \frac{1}{2}$ which is divergent. If we let $x_n := \frac{1}{\sqrt{n+1}}$ and $y_n := \frac{1}{\sqrt{n}}$, then we have

$$\frac{x_n}{y_n} = \frac{\sqrt{n}}{\sqrt{n+1}} = \frac{1}{\sqrt{1+(1/n)}} \to 1.$$

Therefore, the Limit Comparison Test applies.

(d) The series $\sum_{n=1}^{\infty} \frac{1}{n!}$ is convergent.

It would be possible to establish this convergence by showing (by Induction) that $n^2 < n!$ for $n \geq 4$, whence it follows that

$$0 < \frac{1}{n!} < \frac{1}{n^2} \quad \text{for } n \geq 4.$$

Alternatively, if we let $x_n := \frac{1}{n!}$ and $y_n := \frac{1}{n^2}$, then (when $n \geq 4$) we have

$$\frac{x_n}{y_n} = \frac{n^2}{n!} = \frac{n}{1 \cdot 2 \cdots (n-1)} < \frac{1}{n-2} \to 0.$$

Therefore the Limit Comparison Test applies.

---

16 Limits of Functions

In this section, we will introduce the important notion of the limit of a function. The intuitive idea of the function f having a limit L at the point c is that the values $f(x)$ are close to L when x is close to (but different from) c. But it is necessary to have a technical way of working with the idea of "close to" and this is accomplished in the ϵ-δ definition given below.

In order for the idea of the limit of a function f at a point c to be meaningful, it is necessary that f be defined at points near c. It need not be defined at the point c, but it should be defined at enough points close to c to make the study interesting. This is the reason for the following definition.

Definition: Let $A \subseteq \mathbb{R}$. A point $c \in \mathbb{R}$ is a *cluster point* of A if for every $\delta > 0$ there exists at least one point $x \in A$, $x \neq c$ such that $|x - c| < \delta$.

Definition: Let $A \subseteq \mathbb{R}$, and let c be a cluster point of A. For a function $f : A \to \mathbb{R}$, a real number L is said to be a *limit* of f at c if, given any $\epsilon > 0$, there exists a $\delta > 0$ such that if $x \in A$ and $0 < |x - c| < \delta$, then $|f(x) - L| < \epsilon$.

Theorem: If $f : A \to \mathbb{R}$ and if c is a cluster point of A, then f can have only one limit at c.

Proof: Suppose that numbers L and L' satisfy Definition of the limit. For any $\epsilon > 0$, there exists $\delta(\epsilon/2) > 0$ such that if $x \in A$ and $0 < |x - c| < \delta(\epsilon/2)$, then $|f(x) - L| < \epsilon/2$. Also, there exists $\delta'(\epsilon/2)$ such that if $x \in A$ and $0 < |x - c| < \delta'(\epsilon/2)$, then $|f(x) - L'| < \epsilon/2$. Now let

$$\delta := \inf\{\delta(\epsilon/2), \delta'(\epsilon/2)\}.$$

Then if $x \in A$ and $0 < |x - c| < \delta$, the Triangle Inequality implies that

$$|L - L'| \leq |L - f(x)| + |f(x) - L'| < \epsilon/2 + \epsilon/2 = \epsilon.$$

Since $\epsilon > 0$ is arbitrary, we conclude that $L - L' = 0$, so that $L = L'$.)

Example 1: $\lim_{x \to c} b = b$.

To be more explicit, let $f(x) := b$ for all $x \in \mathbb{R}$. We want to show that $\lim_{x \to c} f(x) = b$.

If $\epsilon > 0$ is given, we let $\delta := 1$. (In fact, any strictly positive δ will serve the purpose.) Then if $0 < |x - c| < 1$, we have $|f(x) - b| = |b - b| = 0 < \epsilon$. Since $\epsilon > 0$ is arbitrary, we conclude that $\lim_{x \to c} f(x) = b$.

Example 2: $\lim_{x \to c} x = c$.

Let $g(x) := x$ for all $x \in \mathbb{R}$. If $\epsilon > 0$, we choose $\delta(\epsilon) := \epsilon$. Then if $0 < |x - c| < \delta(\epsilon)$, we have $|g(x) - c| = |x - c| < \epsilon$. Since $\epsilon > 0$ is arbitrary, we deduce that $\lim_{x \to c} g = c$.

Example 3: $\lim_{x \to c} x^2 = c^2$.

Let $h(x) := x^2$ for all $x \in \mathbb{R}$. We want to make the difference

$$|h(x) - c^2| = |x^2 - c^2|$$

less than a preassigned $\epsilon > 0$ by taking x sufficiently close to c. To do so, we note that $x^2 - c^2 = (x + c)(x - c)$. Moreover, if $|x - c| < 1$, then

$$|x| \leq |c| + 1 \quad \text{so that} \quad |x + c| \leq |x| + |c| \leq 2|c| + 1.$$

Therefore, if $|x - c| < 1$, we have

$$|x^2 - c^2| = |x + c||x - c| \leq (2|c| + 1)|x - c|. \tag{1}$$

Moreover, this last term will be less than ϵ provided we take $|x - c| < \epsilon/(2|c| + 1)$. Consequently, if we choose

$$\delta(\epsilon) := \inf\left\{1, \frac{\epsilon}{2|c| + 1}\right\},$$

then if $0 < |x-c| < \delta(\epsilon)$, it will follow first that $|x-c| < 1$ so that (1) is valid, and therefore, since $|x-c| < \epsilon/(2|c|+1)$ that

$$|x^2 - c^2| \leq (2|c| + 1)|x - c| < \epsilon.$$

Since we have a way of choosing $\delta(\epsilon) > 0$ for an arbitrary choice of $\epsilon > 0$, we infer that

$$\lim_{x \to c} h(x) = \lim_{x \to c} x^2 = c^2.$$

Example 4: $\lim_{x\to c} \frac{1}{x} = \frac{1}{c}$ if $c > 0$.

Let $\varphi(x) := \frac{1}{x}$ for $x > 0$ and let $c > 0$. To show that $\lim_{x\to c} \varphi = \frac{1}{c}$, we wish to make the difference

$$\left|\varphi(x) - \frac{1}{c}\right| = \left|\frac{1}{x} - \frac{1}{c}\right|$$

less than a preassigned $\epsilon > 0$ by taking x sufficiently close to $c > 0$. We first note that

$$\left|\frac{1}{x} - \frac{1}{c}\right| = \frac{1}{|cx|}|c - x| = \frac{1}{cx}|x - c|$$

for $x > 0$. It is useful to get an upper bound for the term $\frac{1}{cx}$ that holds in some neighborhood of c. In particular, if $|x - c| < \frac{1}{2}c$, then $\frac{1}{2}c < x < \frac{3}{2}c$ (why?), so that

$$0 < \frac{1}{cx} < \frac{2}{c^2} \quad \text{for} \quad |x - c| < \frac{1}{2}c.$$

Therefore, for these values of x we have

$$\left|\varphi(x) - \frac{1}{c}\right| \leq \frac{2}{c^2}|x - c|. \tag{2}$$

In order to make this last term less than ϵ, it suffices to take $|x - c| < \frac{1}{2}c^2\epsilon$. Consequently, if we choose

$$\delta(\epsilon) := \inf\left\{\frac{1}{2}c, \frac{1}{2}c^2\epsilon\right\},$$

then if $0 < |x-c| < \delta(\epsilon)$, it will follow first that $|x-c| < \frac{1}{2}c$ so that (2) is valid, and therefore, since $|x-c| < \frac{1}{2}c^2\epsilon$, that

$$\left|\varphi(x) - \frac{1}{c}\right| = \left|\frac{1}{x} - \frac{1}{c}\right| < \epsilon.$$

Since we have a way of choosing $\delta(\epsilon) > 0$ for an arbitrary choice of $\epsilon > 0$, we infer that $\lim_{x\to c} \varphi = \frac{1}{c}$.

Theorem (Sequential Criterion) Let $f : A \to \mathbb{R}$ and let c be a cluster point of A. Then the following are equivalent:

(i) $\lim_{x\to c} f = L$.

(ii) For every sequence (x_n) in A that converges to c such that $x_n \neq c$ for all $n \in \mathbb{N}$, the sequence $(f(x_n))$ converges to L.

Proof: (i) $\Rightarrow$ (ii). Assume f has limit L at c, and suppose (x_n) is a sequence in A with $\lim x_n = c$ and $x_n \neq c$ for all n. We must prove that the sequence $(f(x_n))$ converges to L. Let $\epsilon > 0$ be given. Then, there exists $\delta > 0$ such that if $x \in A$ satisfies $0 < |x - c| < \delta$, then $f(x)$ satisfies $|f(x) - L| < \epsilon$. We now apply the definition of convergent sequence for the given δ to obtain a natural number $K(\delta)$ such that if $n > K(\delta)$, then $|x_n - c| < \delta$. But for each such x_n, we have $|f(x_n) - L| < \epsilon$. Thus if $n > K(\delta)$, then $|f(x_n) - L| < \epsilon$. Therefore, the sequence $(f(x_n))$ converges to L.

(ii) $\Rightarrow$ (i). [The proof is a contrapositive argument.] If (i) is not true, then there exists an ϵ_0-neighborhood $V_{\epsilon_0}(L)$ such that no matter what δ-neighborhood of c we pick, there will be at least one number x_δ in $A \cap V_\delta(c)$ with

$x_\delta \neq c$ such that $f(x_\delta) \notin V_{\epsilon_0}(L)$. Hence for every $n \in \mathbb{N}$, the $(1/n)$-neighborhood of c contains a number x_n such that

$$0 < |x_n - c| < \frac{1}{n} \quad \text{and} \quad x_n \in A,$$

but such that

$$|f(x_n) - L| \geq \epsilon_0 \quad \text{for all } n \in \mathbb{N}.$$

We conclude that the sequence (x_n) in $A \setminus \{c\}$ converges to c, but the sequence $(f(x_n))$ does not converge to L. Therefore we have shown that if (i) is not true, then (ii) is not true. We conclude that (ii) implies (i).

Definition Let $A \subseteq \mathbb{R}$, let $f : A \to \mathbb{R}$, and let $c \in \mathbb{R}$ be a cluster point of A. We say that f is *bounded on a neighborhood of* c if there exists a δ-neighborhood $V_\delta(c)$ of c and a constant $M > 0$ such that we have $|f(x)| \leq M$ for all $x \in A \cap V_\delta(c)$.

Theorem: If $A \subseteq \mathbb{R}$ and $f : A \to \mathbb{R}$ has a limit at $c \in \mathbb{R}$, then f is bounded on some neighborhood of c.

Proof: If $L := \lim_{x\to c} f(x)$, then for $\epsilon = 1$, there exists $\delta > 0$ such that if $0 < |x - c| < \delta$, then $|f(x) - L| < 1$. Hence

$$|f(x)| - |L| \leq |f(x) - L| < 1.$$

Therefore, if $x \in A \cap V_\delta(c)$, $x \neq c$, then $|f(x)| \leq |L| + 1$. If $c \in A$ we take $M := \sup\{|f(c)|, |L| + 1\}$. If $c \notin A$, we take $M = |L| + 1$. It follows that if $x \in A \cap V_\delta(c)$, then $|f(x)| \leq M$. This shows that f is bounded on the neighborhood $V_\delta(c)$ of c.

Theorem Let $A \subseteq \mathbb{R}$, let f and g be functions on A to $\mathbb{R}$, and let $c \in \mathbb{R}$ be a cluster point of A. Further, let $b \in \mathbb{R}$.

(a) If $\lim_{x\to c} f = L$ and $\lim_{x\to c} g = M$, then:

$$\lim_{x\to c}(f + g) = L + M,$$

$$\lim_{x\to c}(f - g) = L - M,$$

$$\lim_{x\to c}(fg) = LM,$$

$$\lim_{x\to c}(bf) = bL.$$

(b) If $h : A \to \mathbb{R}$, if $h(x) \neq 0$ for all $x \in A$, and if $\lim_{x\to c} h = H \neq 0$, then:

$$\lim_{x\to c}\left(\frac{f}{h}\right) = \frac{L}{H}.$$

Example 5: $\lim_{x\to 2}(x^2 + 1)(x^3 - 4) = 20$.

It follows from the previous theorem that

$$\lim_{x\to 2}(x^2 + 1)(x^3 - 4) = \left(\lim_{x\to 2}(x^2 + 1)\right)\left(\lim_{x\to 2}(x^3 - 4)\right) = 5 \cdot 4 = 20.$$

Example 6: $\lim_{x\to 2} \frac{x^3-4}{x^2+1} = \frac{4}{5}$.

We have

$$\lim_{x\to 2} \frac{x^3 - 4}{x^2 + 1} = \frac{\lim_{x\to 2}(x^3 - 4)}{\lim_{x\to 2}(x^2 + 1)} = \frac{4}{5}.$$

Note that since the limit in the denominator $\left(\lim_{x\to 2}(x^2 + 1) = 5\right)$ is not equal to 0, then the previous theorem is applicable.

Example 7: $\lim_{x\to 2} \frac{x^2-4}{3x-6} = \frac{4}{3}$.

If we let $f(x) := x^2 - 4$ and $h(x) := 3x - 6$ for $x \in \mathbb{R}$, then we *cannot* use the previous theorem to evaluate $\lim_{x\to 2}\left(\frac{f(x)}{h(x)}\right)$ because

$$H = \lim_{x\to 2} h(x) = \lim_{x\to 2}(3x-6) = 3\cdot \lim_{x\to 2} x - 6 = 3\cdot 2 - 6 = 0.$$

However, if $x \neq 2$, then it follows that

$$\frac{x^2-4}{3x-6} = \frac{(x+2)(x-2)}{3(x-2)} = \frac{1}{3}(x+2).$$

Therefore we have

$$\lim_{x\to 2}\frac{x^2-4}{3x-6} = \lim_{x\to 2}\frac{1}{3}(x+2) = \frac{1}{3}\left(\lim_{x\to 2}(x+2)\right) = \frac{4}{3}.$$

Note that the function $g(x) = \frac{(x^2-4)}{(3x-6)}$ has a limit at $x = 2$ even though it is not defined there.

Example 8: If p is a polynomial function, then $\lim_{x\to c} p(x) = p(c)$.

Let p be a polynomial function on $\mathbb{R}$ so that

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

for all $x \in \mathbb{R}$. It follows from the fact that $\lim_{x\to c} x^k = c^k$, that

$$\begin{aligned}\lim_{x\to c} p(x) &= \lim_{x\to c}\left[a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0\right]\\ &= \lim_{x\to c}(a_n x^n) + \lim_{x\to c}(a_{n-1}x^{n-1}) + \cdots + \lim_{x\to c}(a_1 x) + \lim_{x\to c} a_0\\ &= a_n c^n + a_{n-1}c^{n-1} + \cdots + a_1 c + a_0\\ &= p(c).\end{aligned}$$

Hence $\lim_{x\to c} p(x) = p(c)$ for any polynomial function p.

Example 9: If p and q are polynomial functions on $\mathbb{R}$ and if $q(c) \neq 0$, then

$$\lim_{x\to c}\frac{p(x)}{q(x)} = \frac{p(c)}{q(c)}.$$

Since $q(x)$ is a polynomial function, it follows from a theorem in algebra that there are at most a finite number of real numbers $\alpha_1, \ldots, \alpha_m$ [the real zeroes of $q(x)$] such that $q(\alpha_j) = 0$ and such that if $x \notin \{\alpha_1, \ldots, \alpha_m\}$, then $q(x) \neq 0$. Hence, if $x \notin \{\alpha_1, \ldots, \alpha_m\}$, we can define

$$r(x) := \frac{p(x)}{q(x)}.$$

If c is not a zero of $q(x)$, then $q(c) \neq 0$, and it follows from part (f) that $\lim_{x\to c} q(x) = q(c) \neq 0$. Therefore we can conclude that

$$\lim_{x\to c}\frac{p(x)}{q(x)} = \frac{\lim_{x\to c} p(x)}{\lim_{x\to c} q(x)} = \frac{p(c)}{q(c)}.$$

Squeeze Theorem Let $A \subseteq \mathbb{R}$, let $f, g, h : A \to \mathbb{R}$, and let $c \in \mathbb{R}$ be a cluster point of A. If

$$f(x) \leq g(x) \leq h(x) \quad \text{for all} \quad x \in A, x \neq c,$$

and if

$$\lim_{x\to c} f = L = \lim_{x\to c} h,$$

then

$$\lim_{x\to c} g = L.$$

Examples 10:

(a) $\lim_{x\to 0} x^{3/2} = 0$ $(x > 0)$.

Let $f(x) := x^{3/2}$ for $x > 0$. Since the inequality $x < x^{1/2} \leq 1$ holds for $0 < x \leq 1$ (why?), it follows that $x^2 \leq f(x) = x^{3/2} \leq x$ for $0 < x \leq 1$. Since

$$\lim_{x\to 0} x^2 = 0 \quad \text{and} \quad \lim_{x\to 0} x = 0,$$

it follows from the Squeeze Theorem that $\lim_{x\to 0} x^{3/2} = 0$.

(b) $\lim_{x\to 0} \sin x = 0$.

We have that

$$-x \leq \sin x \leq x \quad \text{for all} \quad x \geq 0.$$

Since $\lim_{x\to 0}(\pm x) = 0$, it follows from the Squeeze Theorem that $\lim_{x\to 0} \sin x = 0$.

(c) $\lim_{x\to 0} \cos x = 1$.

We have that

$$1 - \frac{1}{2}x^2 \leq \cos x \leq 1 \quad \text{for all} \quad x \in \mathbb{R}.$$

Since $\lim_{x\to 0} \left(1 - \frac{1}{2}x^2\right) = 1$, it follows from the Squeeze Theorem that $\lim_{x\to 0} \cos x = 1$.

(d) $\lim_{x\to 0} \frac{\cos x - 1}{x} = 0$.

We have that

$$-\frac{1}{2}x \leq \frac{\cos x - 1}{x} \leq 0 \quad \text{for} \quad x > 0$$

and that

$$0 \leq \frac{\cos x - 1}{x} \leq -\frac{1}{2}x \quad \text{for} \quad x < 0.$$

Now let $f(x) := -x/2$ for $x \geq 0$ and $f(x) := 0$ for $x < 0$, and let $h(x) := 0$ for $x \geq 0$ and $h(x) := -x/2$ for $x < 0$. Then we have

$$f(x) \leq \frac{\cos x - 1}{x} \leq h(x) \quad \text{for} \quad x \neq 0.$$

Since it is readily seen that $\lim_{x\to 0} f = 0 = \lim_{x\to 0} h$, it follows from the Squeeze Theorem that

$$\lim_{x\to 0} \frac{\cos x - 1}{x} = 0.$$

(e) $\lim_{x\to 0} \left(\frac{\sin x}{x}\right) = 1$.

$$x - \frac{1}{6}x^3 \leq \sin x \leq x \quad \text{for} \quad x \geq 0$$

and that

$$x \leq \sin x \leq x - \frac{1}{6}x^3 \quad \text{for} \quad x \leq 0.$$

Therefore it follows (why?) that

$$1 - \frac{1}{6}x^2 \leq \left(\frac{\sin x}{x}\right) \leq 1 \quad \text{for all} \quad x \neq 0.$$

But since

$$\lim_{x \to 0} \left(1 - \frac{1}{6}x^2\right) = 1 - \frac{1}{6} \lim_{x \to 0} x^2 = 1,$$

we infer from the Squeeze Theorem that

$$\lim_{x \to 0} \left(\frac{\sin x}{x}\right) = 1.$$

16.1 Continuous Functions

Definition : Let $A \subseteq \mathbb{R}$, let $f : A \to \mathbb{R}$, and let $c \in A$. We say that f is **continuous at** c if, given any number $\epsilon > 0$, there exists $\delta > 0$ such that if x is any point of A satisfying $|x - c| < \delta$, then $|f(x) - f(c)| < \epsilon$.

If f fails to be continuous at c, then we say that f is **discontinuous at** c.

Sequential Criterion for Continuity A function $f : A \to \mathbb{R}$ is continuous at the point $c \in A$ if and only if for every sequence (x_n) in A that converges to c, the sequence $(f(x_n))$ converges to $f(c)$.

Discontinuity Criterion Let $A \subseteq \mathbb{R}$, let $f : A \to \mathbb{R}$, and let $c \in A$. Then f is discontinuous at c if and only if there exists a sequence (x_n) in A such that (x_n) converges to c, but the sequence $(f(x_n))$ does not converge to $f(c)$.

So far we have discussed continuity at a point. To talk about the continuity of a function on a set, we will simply require that the function be continuous at each point of the set.

Examples

(a) The constant function $f(x) := b$ is continuous on $\mathbb{R}$.

It was seen that if $c \in \mathbb{R}$, then $\lim_{x \to c} f(x) = b$. Since $f(c) = b$, we have $\lim_{x \to c} f(x) = f(c)$, and thus f is continuous at every point $c \in \mathbb{R}$. Therefore f is continuous on $\mathbb{R}$.

(b) $g(x) := x$ is continuous on $\mathbb{R}$.

It was seen that if $c \in \mathbb{R}$, then we have $\lim_{x \to c} g(x) = c$. Since $g(c) = c$, then g is continuous at every point $c \in \mathbb{R}$. Thus g is continuous on $\mathbb{R}$.

(c) $h(x) := x^2$ is continuous on $\mathbb{R}$.

It was seen that if $c \in \mathbb{R}$, then we have $\lim_{x \to c} h(x) = c^2$. Since $h(c) = c^2$, then h is continuous at every point $c \in \mathbb{R}$. Thus h is continuous on $\mathbb{R}$.

(d) $\varphi(x) := 1/x$ is continuous on $A := \{x \in \mathbb{R} : x > 0\}$.

It was seen that if $c \in A$, then we have $\lim_{x \to c} \varphi(x) = 1/c$. Since $\varphi(c) = 1/c$, this shows that φ is continuous at every point $c \in A$. Thus φ is continuous on A.

(e) $\varphi(x) := 1/x$ is not continuous at $x = 0$.

Indeed, if $\varphi(x) = 1/x$ for $x > 0$, then φ is not defined for $x = 0$, so it cannot be continuous there. Alternatively, it was seen that $\lim_{x \to 0} \varphi(x)$ does not exist in $\mathbb{R}$, so φ cannot be continuous at $x = 0$.

Let $A \subseteq \mathbb{R}$ and let f and g be functions that are defined on A to $\mathbb{R}$ and let $b \in \mathbb{R}$. In the definition, we defined the sum, difference, product, and multiple functions denoted by $f + g$, $f - g$, fg, bf. In addition, if $h : A \to \mathbb{R}$ is such that $h(x) \neq 0$ for all $x \in A$, then we defined the quotient function denoted by f/h.

Theorem Let $A \subseteq \mathbb{R}$, let f and g be functions on A to $\mathbb{R}$, and let $b \in \mathbb{R}$. Suppose that $c \in A$ and that f and g are continuous at c.

(a) Then $f + g$, $f - g$, fg, and bf are continuous at c.

(b) If $h : A \to \mathbb{R}$ is continuous at $c \in A$ and if $h(x) \neq 0$ for all $x \in A$, then the quotient f/h is continuous at c.

Proof. If $c \in A$ is not a cluster point of A, then the conclusion is automatic. Hence we assume that c is a cluster point of A.

(a) Since f and g are continuous at c, then

$$f(c) = \lim_{x \to c} f \quad \text{and} \quad g(c) = \lim_{x \to c} g.$$

Hence it follows that

$$(f+g)(c) = f(c) + g(c) = \lim_{x \to c}(f+g).$$

Therefore $f+g$ is continuous at c. The remaining assertions in part (a) are proved in a similar fashion.

(b) Since $c \in A$, then $h(c) \neq 0$. But since $h(c) = \lim_{x \to c} h$, it follows that

$$\frac{f}{h}(c) = \frac{f(c)}{h(c)} = \frac{\lim_{x\to c} f}{\lim_{x \to c} h} = \lim_{x \to c}\left(\frac{f}{h}\right).$$

Therefore f/h is continuous at c.

We now show that if the function $f : A \to \mathbb{R}$ is continuous at a point c and if $g : B \to \mathbb{R}$ is continuous at $b = f(c)$, then the composition $g \circ f$ is continuous at c. In order to assure that $g \circ f$ is defined on all of A, we also need to assume that $f(A) \subseteq B$.

Theorem Let $A, B \subseteq \mathbb{R}$ and let $f : A \to \mathbb{R}$ and $g : B \to \mathbb{R}$ be functions such that $f(A) \subseteq B$. If f is continuous at a point $c \in A$ and g is continuous at $b = f(c) \in B$, then the composition $g \circ f : A \to \mathbb{R}$ is continuous at c.

Proof. Let W be an ϵ-neighborhood of $g(b)$. Since g is continuous at b, there is a δ-neighborhood V of $b = f(c)$ such that if $y \in B \cap V$, then $g(y) \in W$. Since f is continuous at c, there is a γ-neighborhood U of c such that if $x \in A \cap U$, then $f(x) \in V$. Since $f(A) \subseteq B$, it follows that if $x \in A \cap U$, then $f(x) \in B \cap V$ so that $g \circ f(x) = g(f(x)) \in W$. But since W is an arbitrary ϵ-neighborhood of $g(b)$, this implies that $g \circ f$ is continuous at c.

Examples

(a) Let $g_1(x) := |x|$ for $x \in \mathbb{R}$. It follows from the Triangle Inequality that

$$|g_1(x) - g_1(c)| \leq |x - c|$$

for all $x, c \in \mathbb{R}$. Hence g_1 is continuous at $c \in \mathbb{R}$. If $f : A \to \mathbb{R}$ is any function that is continuous on A, then it implies that $g_1 \circ f = |f|$ is continuous on A. This gives another proof of the theorem.

(b) Let $g_2(x) := \sqrt{x}$ for $x \geq 0$. It follows that g_2 is continuous at any number $c \geq 0$. If $f : A \to \mathbb{R}$ is continuous on A and if $f(x) \geq 0$ for all $x \in A$, then it follows that $g_2 \circ f = \sqrt{f}$ is continuous on A. This gives another proof of the theorem.

(c) Let $g_3(x) := \sin x$ for $x \in \mathbb{R}$. We have seen that g_3 is continuous on $\mathbb{R}$. If $f : A \to \mathbb{R}$ is continuous on A, then it follows that $g_3 \circ f$ is continuous on A.

In particular, if $f(x) := 1/x$ for $x \neq 0$, then the function $g(x) := \sin(1/x)$ is continuous at every point $c \neq 0$. This shows that g cannot be defined at 0 in order to become continuous at that point.

Definition Let $A \subseteq \mathbb{R}$ and let $f : A \to \mathbb{R}$. We say that f has an **absolute maximum** on A if there is a point $x^* \in A$ such that

$$f(x^*) \geq f(x) \quad \text{for all } x \in A.$$

We say that f has an **absolute minimum** on A if there is a point $x_* \in A$ such that

$$f(x_*) \leq f(x) \quad \text{for all } x \in A.$$

We say that x^* is an **absolute maximum point** for f on A, and that x_* is an **absolute minimum point** for f on A, if they exist.

The next result is a generalization of the Location of Roots Theorem. It assures us that a continuous function on an interval takes on (at least once) any number that lies between two of its values.

Bolzano's Intermediate Value Theorem Let I be an interval and let $f : I \to \mathbb{R}$ be continuous on I. If $a, b \in I$ and if $k \in \mathbb{R}$ satisfies $f(a) < k < f(b)$, then there exists a point $c \in I$ between a and b such that $f(c) = k$.

Proof. Suppose that $a < b$ and let $g(x) := f(x) - k$; then $g(a) < 0 < g(b)$. By the Location of Roots Theorem there exists a point c with $a < c < b$ such that $0 = g(c) = f(c) - k$. Therefore $f(c) = k$.

If $b < a$, let $h(x) := k - f(x)$ so that $h(b) < 0 < h(a)$. Therefore there exists a point c with $b < c < a$ such that $0 = h(c) = k - f(c)$, whence $f(c) = k$.

Corollary Let $I = [a, b]$ be a closed, bounded interval and let $f : I \to \mathbb{R}$ be continuous on I. If $k \in \mathbb{R}$ is any number satisfying
$$\inf f(I) \leq k \leq \sup f(I),$$
then there exists a number $c \in I$ such that $f(c) = k$.

Proof. It follows from the Maximum-Minimum Theorem that there are points c_* and c^* in I such that

$$\inf f(I) = f(c_*) \leq k \leq f(c^*) = \sup f(I).$$

The conclusion now follows from Bolzano's Theorem.

16.2 Exercise

1. Suppose that $f(x)$ is continuous at $x = a$. Determine, with proof, a necessary and sufficient condition for $\frac{1}{f(x)}$ to be continuous at $x = a$.

2. Suppose that $f(x)$ and $g(x)$ are not continuous at $x = a$. Is it possible that $f(x) + g(x)$ is continuous at $x = a$?

3. Suppose that $f(x)$ is continuous at $x = a$, but $g(x)$ is not continuous at $x = a$. Is it possible that $f(x) + g(x)$ is continuous at $x = a$?

4. Suppose that $f(x)$ and $g(x)$ are not continuous at $x = a$. Is it possible that $f(x)g(x)$ is continuous at $x = a$?

5. Suppose that $f(x)$ is continuous at $x = a$, but $g(x)$ is not continuous at $x = a$. Is it possible that $f(x)g(x)$ is continuous at $x = a$?

6. Suppose f and g are functions such that $g \circ f$ is well-defined. Determine whether it is possible for $g(f(x))$ to be continuous at $x = a$ if

(a) $f(x)$ is discontinuous at $x = a$ but $g(y)$ is continuous at $y = f(a)$.

(b) $f(x)$ is continuous at $x = a$ but $g(y)$ is discontinuous at $y = f(a)$.

(c) $f(x)$ is discontinuous at $x = a$ and $g(y)$ is discontinuous at $y = f(a)$.

7. Define $f(x) = \sin \frac{1}{x}$ if $x \neq 0$ and $f(0) = 0$. Discuss the continuity of $f(x)$.
Note: For this problem, sequential approach is more useful than the $\epsilon - \delta$ approach.

8. Define $f(x) = x \sin \frac{1}{x}$ if $x \neq 0$ and $f(0) = 0$. Discuss the continuity of $f(x)$.
Note: For this problem, the $\epsilon - \delta$ approach is more useful than the sequential approach.

9. Let $A = [1, 2) \cup (2, 3]$. Define a function $f : A \to \mathbb{R}$ as follows: $f(x) = x + 1$ if $x \in [1, 2)$ and $3 - x$ if $x \in (2, 3]$. Can you draw the graph of $f(x)$ without lifting the pen? Is the function discontinuous at $x = 2$?

10. Let $A = [1, 2] \cup (3, 4]$. Define a function $f : A \to \mathbb{R}$ as follows: $f(x) = x + 1$ if $x \in [1, 2]$ and $3 - x$ if $x \in (3, 4]$. Can you draw the graph of $f(x)$ without lifting the pen? Determine whether the function is continuous on A or not.

16.3 Limits MCQ

1. $\lim_{x\to\infty} \frac{20+2\sqrt{x}+3\sqrt[3]{x}}{2+\sqrt{4x-3+\sqrt{8x-4}}}$ is

(A) 10;

(B) $\frac{3}{2}$;

(C) 1;

(D) 0.

2. $\lim_{x\to\infty} \left[x\sqrt{x^2+a^2}-\sqrt{x^4+a^4}\right]$ is

(A) ∞;

(B) $\frac{a^2}{2}$;

(C) a^2;

(D) 0.

3. The limit of $x^3\left[\sqrt{x^2+\sqrt{x^4+1}}-x\sqrt{2}\right]$ as $x\to\infty$

(A) exists and equals $\frac{1}{2\sqrt{2}}$;

(B) exists and equals $\frac{1}{4\sqrt{2}}$;

(C) does not exist;

(D) exists and equals $\frac{3}{4\sqrt{2}}$.

4. If $f(x)=\sqrt{\frac{x-\cos^2 x}{x+\sin x}}$, then the limit of $f(x)$ as $x\to\infty$ is

(A) 0;

(B) 1;

(C) ∞;

(D) none of 0, 1, or ∞.

5. Consider the function $f(x)=\tan^{-1}(2\tan\frac{x}{2})$, where $-\frac{\pi}{2}\le f(x)\le\frac{\pi}{2}$. ($\lim_{x\to\pi-0}$ means limit from the left at π and $\lim_{x\to\pi+0}$ means limit from the right.) Then

(A) $\lim_{x\to\pi-0} f(x)=\frac{\pi}{2}$, $\lim_{x\to\pi+0} f(x)=-\frac{\pi}{2}$;

(B) $\lim_{x\to\pi-0} f(x)=-\frac{\pi}{2}$, $\lim_{x\to\pi+0} f(x)=\frac{\pi}{2}$;

(C) $\lim_{x\to\pi} f(x)=\frac{\pi}{2}$;

(D) $\lim_{x\to\pi} f(x)=-\frac{\pi}{2}$.

6. The value of $\lim_{x\to a}\frac{x\sin a-a\sin x}{x-a}$ is

(A) non-existent;

(B) $\sin a+a\cos a$;

(C) $a\sin a-\cos a$;

(D) $\sin a-a\cos a$.

7. The limit $\lim_{x\to 0}\frac{\cos x-\sec x}{x^2(x+1)}$

(A) is 0;

(B) is 1;

(C) is -1;

(D) does not exist.

8. The limit $\lim_{x\to 0+} \frac{\tan x - x}{x - \sin x}$ equals

(A) -1;

(B) 0;

(C) 1;

(D) 2.

9. $\lim_{x\to 0} \frac{(1+x)^{\frac{1}{2}}-1}{(1+x)^{\frac{1}{3}}-1}$ is

(A) 1;

(B) 0;

(C) $\frac{3}{2}$;

(D) ∞.

10. A right circular cylindrical container closed on both sides is to contain a fixed volume of motor oil. Suppose its base has diameter d and overall surface area of the container is minimum when

(A) $h = \frac{3}{4}\pi d$;

(B) $h = 2d$;

(C) $h = d$;

(D) conditions other than the foregoing are satisfied.

11. $\lim_{x\to\infty}(\log x - x)$

(A) equals $+\infty$;

(B) equals e;

(C) equals $-\infty$;

(D) does not exist.

12. $\lim_{x\to 0} x \tan \frac{1}{x}$

(A) equals 0;

(B) equals 1;

(C) equals ∞;

(D) does not exist.

ANSWER KEY

1	2	3	4	5	6
C	B	B	B	A	D
7	8	9	10	11	12
C	D	C	C	C	D

17 Differentiability

17.1 Introduction

Definition 1: Suppose that $f : (a, b) \to \mathbb{R}$ and $a < c < b$. Then f is differentiable at c with derivative $f'(c)$ if

$$\lim_{h\to 0}\left[\frac{f(c+h)-f(c)}{h}\right] = f'(c).$$

The domain of f' is the set of points $c \in (a, b)$ for which this limit exists. If the limit exists for every $c \in (a, b)$ then we say that f is differentiable on (a, b).

Graphically, this definition says that the derivative of f at c is the slope of the tangent line to $y = f(x)$ at c, which is the limit as $h \to 0$ of the slopes of the lines through $(c, f(c))$ and $(c + h, f(c + h))$.

We can also write

$$f'(c) = \lim_{x\to c}\left[\frac{f(x)-f(c)}{x-c}\right],$$

since if $x = c + h$, the conditions $0 < |x - c| < \delta$ and $0 < |h| < \delta$ in the definitions of the limits are equivalent. The ratio

$$\frac{f(x)-f(c)}{x-c}$$

is undefined $(0/0)$ at $x = c$, but it doesn't have to be defined in order for the limit as $x \to c$ to exist.

Like continuity, differentiability is a local property. That is, the differentiability of a function f at c and the value of the derivative, if it exists, depend only the values of f in a arbitrarily small neighborhood of c. In particular if $f : A \to \mathbb{R}$

where $A \subset \mathbb{R}$, then we can define the differentiability of f at any interior point $c \in A$ since there is an open interval $(a, b) \subset A$ with $c \in (a, b)$.

Examples of derivatives Let us give a number of examples that illustrate differentiable and non-differentiable functions.

Example 1: The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is differentiable on $\mathbb{R}$ with derivative $f'(x) = 2x$ since

$$\lim_{h\to 0}\left[\frac{(c+h)^2-c^2}{h}\right] = \lim_{h\to 0}\frac{h(2c+h)}{h} = \lim_{h\to 0}(2c+h) = 2c.$$

Note that in computing the derivative, we first cancel by h, which is valid since $h \neq 0$ in the definition of the limit, and then set $h = 0$ to evaluate the limit. This procedure would be inconsistent if we didn't use limits.

Example 2: The function $f : \mathbb{R} \to \mathbb{R}$ defined by

$$f(x) = \begin{cases} x^2 & \text{if } x > 0, \\ 0 & \text{if } x \le 0. \end{cases}$$

is differentiable on $\mathbb{R}$ with derivative

$$f'(x) = \begin{cases} 2x & \text{if } x > 0, \\ 0 & \text{if } x \le 0. \end{cases}$$

For $x > 0$, the derivative is $f'(x) = 2x$ as above, and for $x < 0$, we have $f'(x) = 0$. For 0, we consider the limit

$$\lim_{h\to 0}\left[\frac{f(h)-f(0)}{h}\right] = \lim_{h\to 0}\frac{f(h)}{h}.$$

The right limit is

$$\lim_{h\to 0^+}\frac{f(h)}{h} = \lim_{h\to 0} h = 0,$$

and the left limit is

$$\lim_{h\to 0^-} \frac{f(h)}{h} = 0.$$

Since the left and right limits exist and are equal, the limit also exists, and f is differentiable at 0 with $f'(0) = 0$.

Next, we consider some examples of non-differentiability at discontinuities, corners, and cusps.

Example 3: The function $f : \mathbb{R} \to \mathbb{R}$ defined by

$$f(x) = \begin{cases} 1/x & \text{if } x \neq 0, \\ 0 & \text{if } x = 0, \end{cases}$$

is differentiable at $x \neq 0$ with derivative $f'(x) = -1/x^2$ since

$$\lim_{h\to 0} \left[\frac{f(c+h) - f(c)}{h}\right] = \lim_{h\to 0} \left[\frac{1/(c+h) - 1/c}{h}\right] = \lim_{h\to 0} \left[\frac{c - (c+h)}{hc(c+h)}\right] = -\lim_{h\to 0} \frac{1}{c(c+h)} = -\frac{1}{c^2}.$$

However, f is not differentiable at 0 since the limit

$$\lim_{h\to 0} \left[\frac{f(h) - f(0)}{h}\right] = \lim_{h\to 0} \left[\frac{1/h - 0}{h}\right] = \lim_{h\to 0} \frac{1}{h^2}$$

does not exist.

Example 4: The sign function $f(x) = \operatorname{sgn} x$, defined in Example 6.8, is differentiable at $x \neq 0$ with $f'(x) = 0$, since in that case $f(x+h) - f(x) = 0$ for all sufficiently small h. The sign function is not differentiable at 0 since

$$\lim_{h\to 0} \left[\frac{\operatorname{sgn} h - \operatorname{sgn} 0}{h}\right] = \lim_{h\to 0} \frac{\operatorname{sgn} h}{h}$$

and

$$\frac{\operatorname{sgn} h}{h} = \begin{cases} 1/h & \text{if } h > 0, \\ -1/h & \text{if } h < 0 \end{cases}$$

is unbounded in every neighborhood of 0, so its limit does not exist.

Example 5: The absolute value function $f(x) = |x|$ is differentiable at $x \neq 0$ with derivative $f'(x) = \operatorname{sgn} x$. It is not differentiable at 0, however, since

$$\lim_{h\to 0} \frac{f(h) - f(0)}{h} = \lim_{h\to 0} \frac{|h|}{h} = \lim_{h\to 0} \operatorname{sgn} h$$

does not exist. (The right limit is 1 and the left limit is -1.)

Example 6: The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = |x|^{1/2}$ is differentiable at $x \neq 0$ with

$$f'(x) = \frac{\operatorname{sgn} x}{2|x|^{1/2}}.$$

If $c > 0$, then using the difference of two squares to rationalize the numerator, we get

$$\begin{aligned}
\lim_{h\to 0} \left[\frac{f(c+h) - f(c)}{h}\right] &= \lim_{h\to 0} \frac{(c+h)^{1/2} - c^{1/2}}{h} \\
&= \lim_{h\to 0} \frac{(c+h) - c}{h\left[(c+h)^{1/2} + c^{1/2}\right]} \\
&= \lim_{h\to 0} \frac{1}{(c+h)^{1/2} + c^{1/2}} \\
&= \frac{1}{2c^{1/2}}.
\end{aligned}$$

If $c < 0$, we get the analogous result with a negative sign. However, f is not differentiable at 0, since

$$\lim_{h \to 0^+} \frac{f(h) - f(0)}{h} = \lim_{h \to 0^+} \frac{1}{h^{1/2}}$$

does not exist.

Left and right derivatives. For the most part, we will use derivatives that are defined only at the interior points of the domain of a function. Sometimes, however, it is convenient to use one-sided left or right derivatives that are defined at the endpoint of an interval.

Definition 2: Suppose that $f : [a, b] \to \mathbb{R}$. Then f is right-differentiable at $a \le c < b$ with right derivative $f'(c^+)$ if

$$\lim_{h \to 0^+} \left[\frac{f(c+h) - f(c)}{h} \right] = f'(c^+)$$

exists, and f is left-differentiable at $a < c \le b$ with left derivative $f'(c^-)$ if

$$\lim_{h \to 0^-} \left[\frac{f(c+h) - f(c)}{h} \right] = \lim_{h \to 0^+} \left[\frac{f(c) - f(c-h)}{h} \right] = f'(c^-).$$

A function is differentiable at $a < c < b$ if and only if the left and right derivatives at c both exist and are equal.

Example 7: If $f : [0, 1] \to \mathbb{R}$ is defined by $f(x) = x^2$, then

$$f'(0^+) = 0, \quad f'(1^-) = 2.$$

These left and right derivatives remain the same if f is extended to a function defined on a larger domain, say

$$f(x) = \begin{cases} x^2 & \text{if } 0 \le x \le 1, \\ 1 & \text{if } x > 1, \\ 1/x & \text{if } x < 0. \end{cases}$$

For this extended function we have $f'(1^+) = 0$, which is not equal to $f'(1^-)$, and $f'(0^-)$ does not exist, so the extended function is not differentiable at either 0 or 1.

17.2 Properties of Derivatives

Let us look at some properties of derivatives and the relation between differentiability and continuity.

Theorem: If $f : (a, b) \to \mathbb{R}$ is differentiable at $c \in (a, b)$, then f is continuous at c.

Proof. If f is differentiable at c, then

$$\begin{aligned} \lim_{h \to 0} f(c+h) - f(c) &= \lim_{h \to 0} \left[\frac{f(c+h) - f(c)}{h} \cdot h \right]. \\ &= \lim_{h \to 0} \left[\frac{f(c+h) - f(c)}{h} \right] \cdot \lim_{h \to 0} h \\ &= f'(c) \cdot 0 \\ &= 0, \end{aligned}$$

which implies that f is continuous at c.

For example, the sign function has a jump discontinuity at 0 so it cannot be differentiable at 0. The converse does not hold, and a continuous function needn't be differentiable.

The function $x^2 \sin(1/x)$ is differentiable on $\mathbb{R}$, but the derivative f' is not continuous at 0. Thus, while a function f has to be continuous to be differentiable, if f is differentiable its derivative f' need not be continuous. This leads to the following definition.

Definition: A function $f : (a, b) \to \mathbb{R}$ is continuously differentiable on (a, b), written $f \in C^1(a, b)$, if it is differentiable on (a, b) and $f' : (a, b) \to \mathbb{R}$ is continuous.

For example, the function $f(x) = x^2$ with derivative $f'(x) = 2x$ is continuously differentiable on $\mathbb{R}$, whereas the function $x^2 \sin(1/x)$ is not continuously differentiable at 0. As this example illustrates, functions that are differentiable but not continuously differentiable may behave in rather pathological ways. On the other hand, the behaviour of continuously differentiable functions, whose graphs have continuously varying tangent lines, is more-or-less consistent with what one expects.

Algebraic properties of the derivative. A fundamental property of the derivative is that it is a linear operation. In addition, we have the following product and quotient rules.

Theorem: If $f, g : (a, b) \to \mathbb{R}$ are differentiable at $c \in (a, b)$ and $k \in \mathbb{R}$, then kf, $f + g$, and fg are differentiable at c with

$$(kf)'(c) = kf'(c), \quad (f + g)'(c) = f'(c) + g'(c), \quad (fg)'(c) = f'(c)g(c) + f(c)g'(c).$$

Furthermore, if $g(c) \neq 0$, then f/g is differentiable at c with

$$\left(\frac{f}{g}\right)'(c) = \frac{f'(c)g(c) - f(c)g'(c)}{g^2(c)}.$$

Proof. The first two properties follow immediately from the linearity of limits stated.For the product rule, we write

$$\begin{aligned}(fg)'(c) &= \lim_{h\to 0}\left[\frac{f(c+h)g(c+h) - f(c)g(c)}{h}\right]\\ &= \lim_{h\to 0}\left[\frac{(f(c+h) - f(c))g(c+h) + f(c)(g(c+h) - g(c))}{h}\right]\\ &= \lim_{h\to 0}\left[\frac{f(c+h) - f(c)}{h}\right]\lim_{h\to 0} g(c+h) + f(c)\lim_{h\to 0}\left[\frac{g(c+h) - g(c)}{h}\right]\\ &= f'(c)g(c) + f(c)g'(c),\end{aligned}$$

where we have used the properties of limits, which implies that g is continuous at c. The quotient rule follows by a similar argument, or by combining the product rule with the chain rule, which implies that $(1/g)' = -g'/g^2$.

Example: We have $1' = 0$ and $x' = 1$. Repeated application of the product rule implies that x^n is differentiable on $\mathbb{R}$ for every $n \in \mathbb{N}$ with

$$(x^n)' = nx^{n-1}.$$

Alternatively, we can prove this result by induction: The formula holds for $n = 1$. Assuming that it holds for some $n \in \mathbb{N}$, we get from the product rule that

$$(x^{n+1})' = (x \cdot x^n)' = 1 \cdot x^n + x \cdot nx^{n-1} = (n + 1)x^n,$$

and the result follows. It also follows by linearity that every polynomial function is differentiable on $\mathbb{R}$, and from the quotient rule that every rational function is differentiable at every point where its denominator is nonzero. The derivatives are given by their usual formulae.

The chain rule The chain rule states that the composition of differentiable functions is differentiable. The result is quite natural if one thinks in terms of derivatives as linear maps. If f is differentiable at c, it scales lengths by a factor $f'(c)$, and if g is differentiable at $f(c)$, it scales lengths by a factor $g'(f(c))$. Thus, the composition $g \circ f$ scales lengths at c by a factor $g'(f(c)) \cdot f'(c)$. Equivalently, the derivative of a composition is the composition of the derivatives (regarded as linear maps).

We will prove the chain rule by showing that the composition of remainder terms in the linear approximations of f and g leads to a similar remainder term in the linear approximation of $g \circ f$. The argument is complicated by the fact that we have to evaluate the remainder of g at a point that depends on the remainder of f, but this complication should not obscure the simplicity of the final result.

Theorem (Chain rule). Let $f : A \to \mathbb{R}$ and $g : B \to \mathbb{R}$ where $A \subseteq \mathbb{R}$ and $f(A) \subseteq B$, and suppose that c is an interior point of A and $f(c)$ is an interior point of B. If f is differentiable at c and g is differentiable at $f(c)$, then $g \circ f : A \to \mathbb{R}$ is differentiable at c and

$$(g \circ f)'(c) = g'(f(c))f'(c).$$

Proof. Since f is differentiable at c, there is a function $r(h)$ such that

$$f(c+h) = f(c) + f'(c)h + r(h), \quad \lim_{h\to 0} \frac{r(h)}{h} = 0,$$

and since g is differentiable at $f(c)$, there is a function $s(k)$ such that

$$g(f(c)+k) = g(f(c)) + g'(f(c))k + s(k), \quad \lim_{k\to 0} \frac{s(k)}{k} = 0.$$

It follows that

$$\begin{aligned}
(g \circ f)(c+h) &= g(f(c+h)) = g(f(c) + f'(c)h + r(h)) \\
&= g(f(c)) + g'(f(c)) \cdot (f'(c)h + r(h)) + s(f'(c)h + r(h)) \\
&= g(f(c)) + g'(f(c))f'(c) \cdot h + t(h)
\end{aligned}$$

where

$$t(h) = g'(f(c)) \cdot r(h) + s(\phi(h)), \quad \phi(h) = f'(c)h + r(h).$$

Since $r(h)/h \to 0$ as $h \to 0$, we have

$$\lim_{h\to 0} \frac{t(h)}{h} = \lim_{h\to 0} \frac{s(\phi(h))}{h}.$$

We claim that this limit exists and is zero, and then it follows that $g \circ f$ is differentiable at c with

$$(g \circ f)'(c) = g'(f(c))f'(c).$$

To prove the claim, we use the facts that

$$\frac{\phi(h)}{h} \to f'(c) \text{ as } h \to 0, \quad \frac{s(k)}{k} \to 0 \text{ as } k \to 0.$$

Roughly speaking, we have $\phi(h) \sim f'(c)h$ when h is small and therefore

$$\frac{s(\phi(h))}{h} \sim \frac{s(f'(c)h)}{h} \to 0 \text{ as } h \to 0.$$

In detail, let $\epsilon > 0$ be given. We want to show that there exists $\delta > 0$ such that

$$\left|\frac{s(\phi(h))}{h}\right| < \epsilon \text{ if } 0 < |h| < \delta.$$

First, choose $\delta_1 > 0$ such that

$$\left|\frac{r(h)}{h}\right| < |f'(c)| + 1 \text{ if } 0 < |h| < \delta_1.$$

If $0 < |h| < \delta_1$, then

$$\begin{aligned}
|\phi(h)| &\le |f'(c)||h| + |r(h)| \\
&< |f'(c)||h| + (|f'(c)| + 1)|h| \\
&< (2|f'(c)| + 1)|h|.
\end{aligned}$$

Next, choose $\eta > 0$ so that

$$\left|\frac{s(k)}{k}\right| < \frac{\epsilon}{2|f'(c)| + 1} \text{ if } 0 < |k| < \eta.$$

(We include a "1" in the denominator on the right-hand side to avoid a division by zero if $f'(c) = 0$.) Finally, define $\delta_2 > 0$ by

$$\delta_2 = \frac{\eta}{2|f'(c)| + 1},$$

and let $\delta = \min(\delta_1, \delta_2) > 0$.

If $0 < |h| < \delta$ and $\phi(h) \neq 0$, then $0 < |\phi(h)| < \eta$, so

$$|s(\phi(h))| \leq \frac{\epsilon|\phi(h)|}{2|f'(c)| + 1} < \epsilon|h|.$$

If $\phi(h) = 0$, then $s(\phi(h)) = 0$, so the inequality holds in that case also. This proves that

$$\lim_{h \to 0} \frac{s(\phi(h))}{h} = 0.$$

17.3 Extreme Values

Definition: Suppose that $f : A \to \mathbb{R}$. Then f has a **global (or absolute) maximum** at $c \in A$ if

$$f(x) \leq f(c) \quad \text{for all } x \in A,$$

and f has a **local (or relative) maximum** at $c \in A$ if there is a neighborhood U of c such that

$$f(x) \leq f(c) \quad \text{for all } x \in A \cap U.$$

Similarly, f has a **global (or absolute) minimum** at $c \in A$ if

$$f(x) \geq f(c) \quad \text{for all } x \in A,$$

and f has a **local (or relative) minimum** at $c \in A$ if there is a neighborhood U of c such that

$$f(x) \geq f(c) \quad \text{for all } x \in A \cap U.$$

If f has a (local or global) maximum or minimum at $c \in A$, then f is said to have a **(local or global) extreme value** at c.

Theorem: Suppose that $f : A \to \mathbb{R}$ has a local extreme value at an interior point $c \in A$ and f is differentiable at c. Then $f(c) = 0$.

Proof: If f has a local maximum at c, then $f(x) \leq f(c)$ for all x in a δ-neighbourhood $(c - \delta, c + \delta)$ of c, so we have

$$\frac{f(c+h) - f(c)}{h} \leq 0 \quad \text{for all } 0 < h < \delta$$

which implies that

$$f'(c) = \lim_{h \to 0^+} \left[\frac{f(c+h) - f(c)}{h} \right] \leq 0$$

Moreover,

$$\frac{f(c+h) - f(c)}{h} \geq 0 \quad \text{for all } -\delta < h < 0$$

which implies that

$$f'(c) = \lim_{h \to 0^-} \left[\frac{f(c+h) - f(c)}{h} \right] \geq 0$$

It follows that $f(c) = 0$. If f has a local minimum at c, then the signs in these inequalities are reversed and we also conclude that $f(c) = 0$.

Definition: Suppose that $f : A \to \mathbb{R}$. An interior point $c \in A$ such that f is not differentiable at c or $f(c) = 0$ is called a critical point of f. An interior point where $f(c) = 0$ is called a stationary point of f or a critical point.

Theorem: Let $f : A \to \mathbb{R}$ be a function and let c be an interior point of A . Suppose that has a relative maximum (or minimum) at c . If is differentiable at c then c is a critical point of f, that is $f'(c) = 0$

Proof: Suppose f has a relative maxima at c. The case of relative minima will be the same as well. Observe that for $x \neq c$, we have $f(x) - f(c) \leq 0$ for $x \in (c - \delta, c + \delta)$ and for some $\delta > 0$. Consider the function $h : (c - \delta, c + \delta) \to \mathbb{R}$ defined by $h(x) = \frac{f(x)-f(c)}{x-c}$ for $x \neq c$ and $h(c) = f'(c)$. The function h is continuous at $c = 0$ because $\lim_{x\to c} h(x) = h(c)$.

Now for $x \in A = (c, c + \delta)$ it holds that $h(x) \leq 0$ and therefore $f'(c) = \lim_{x\to c} h(x) \leq 0$. Similarly for $x \in B = (c - \delta, c)$ it holds that $h(x) \geq 0$ and therefore $0 \leq f'(c)$. Thus we can conclude that $f'(c) = 0$

Theorem (Rolle's): Let $f : [a, b] \to \mathbb{R}$ be continuous on $[a, b]$ and differentiable on (a, b). If $f(a) = f(b)$ then there exists $c \in (a, b)$ such that $f'(c) = 0$

Proof: Since f is continuous on $[a, b]$ it achieves its maximum and minimum at some point x^* and x_* , respectively, that is $f(x_*) \leq f(x) \leq f(x^*)$ for all $x \in [a, b]$. If f is constant then $f'(x) = 0$ for all $x \in (a, b)$. If f is not constant then $f(x_*) < f(x^*)$. Since $f(a) = f(b)$ it follows that at least one of x^* and x_* is not contained in $\{a, b\}$, and hence there exists $c \in \{x_*, x^*\}$ such that $f'(c) = 0$.

Theorem (MVT): Let $f : [a, b] \to \mathbb{R}$ be continuous on $[a, b]$ and differentiable on (a, b) . Then there exists $c \in (a, b)$ such that $f'(c) = \frac{f(b)-f(a)}{b-a}$

Proof: If $f(a) = f(b)$ then the result follows from Rolle's Theorem (for some). Let $h : [a, b] \to \mathbb{R}$ be the line from $(a, f(a))$ to $(b, f(b)$, that is,

$$h(x) = f(a) + \frac{f(b) - f(a)}{(b - a)}(x - a)$$

and define the function $g(x) = f(x) - h(x)$ for $x \in [a, b]$. Then $g(a) = f(a) - f(a) = 0$ and $g(b) = f(b) - f(b) = 0$ and thus $g(a) = g(b)$. Clearly, g is continuous on $[a, b]$ and differentiable on (a, b) , and it is straightforward to verify that $g'(x) = f'(x) - \frac{f(b)-f(a)}{b-a}$. By Rolle's Theorem, there exists $c \in (a, b)$ such that $g'(c) = 0$ and therefore $f'(c) = \frac{f(b)-f(a)}{b-a}$

Theorem (Taylor): Let $n \in \mathbb{N}$ and let $I = [a, b]$. Let $f : I \to \mathbb{R}$ such that f and its n derivatives $f', f'', \cdots, f^{(n)}$ are continuous on I and that $f^{(n+1)}$ exists on (a, b). If $x_0 \in I$, then for any $x \in I$, there exists a point c in between x and x_0 such that

$$f(x) = f(x_0) + \sum_{k=1}^{n+1} f^{(k)}(x_0)\frac{(x - x_0)^k}{k!}$$

Example 1: (ISI-10) Let f be a real valued function on the real line such that the following limit exists and is finite

$$\lim_{x\to 0} \frac{f(x)}{x^2}$$

Then prove that $f'(0) = 0$

Solution: Observe that for the limit to exist we need $f(0) = 0$. Suppose the value of the limit is L, then we can say that

$$f'(0) = \lim_{x\to 0} \frac{f(x)}{x} = \lim_{x\to 0} x \left(\frac{f(x)}{x^2}\right) = \lim_{x\to 0} xL = 0$$

Example 1: (ISI-06) Let $f : \mathbb{R} \to \mathbb{R}$ be a function that is a function that is differentiable $n + 1$ times for some positive integer n . The i^{th} derivative of f is denoted by $f^{(i)}$. Suppose

$$f(1) = f(0) = f^{(1)}(0) = \cdots = f^{(n)}(0) = 0$$

Prove that $f^{(n+1)}(x) = 0$ for some $x \in (0, 1)$

Solution:

Example 1: (ISI-21) Let $g : (0, \infty) \to (0, \infty)$ be a differentiable function whose derivative is continuous, and such that $g(g(x)) = x$ for all $x > 0$. If g is not the identity function, prove that g must be strictly decreasing.

Solution: g is differentiable. So, differentiating both sides of the given equation, we get

$$g'(g(x)) \cdot g'(x) = 1 \qquad \forall\ x > 0$$

Now, $g'(x) = 0$ is impossible for any x, because if not, then we shall get $0 = 1$.

So, we must have either $g'(x) > 0$ for all x, or $g'(x) < 0$ for all x. But, observe that both of them can't hold together because if $\exists\ a > b > 0$ such that WLOG $g'(a) > 0 > g'(b)$, then due to the continuity of g', there'll be $c \in (b, a)$ such that $g'(c) = 0$ by Intermediate Value Theorem, which can never hold

So, suppose we have $g'(x) > 0$ for all $x > 0$. Then, g is strictly increasing. Now, it is given that g is not the identity function, so there exists some $h > 0$ such that $g(h) \neq h$. If $g(h) < h$, then

$$h = g(g(h)) < g(h) < h$$

which is a contradiction. If $g(h) > h$, then

$$h = g(g(h)) > g(h) > h$$

which is a contradiction too. Thus, we obtain that $g'(x) > 0$ for all $x > 0$ is impossible. So, the we are left with the only option that $g'(x) < 0$, i.e. g must be a strictly decreasing function

Example 4: (ISI-17) Suppose $f : \mathbb{R} \to \mathbb{R}$ is a function given by

$$f(x) = \begin{cases} 1 & \text{if } x = 1 \\ e^{(x^{10}-1)} + (x-1)^2 \sin \frac{1}{x-1} & \text{if } x \neq 1 \end{cases}$$

(a) Find $f'(1)$

(b) Evaluate $\displaystyle \lim_{u \to \infty} \left[100u - u \sum_{k=1}^{100} f\left(1 + \frac{k}{u}\right) \right]$.

Solution: Observe that for the first part we have

$$\begin{aligned} f'(1) &= \lim_{x \to 1} \frac{f(x) - f(1)}{x - 1} \\ &= \lim_{x \to 1} \frac{e^{x^{10}-1} + (x-1)^2 \sin\left(\frac{1}{x-1}\right) - 1}{x - 1} \\ &= \lim_{x \to 1} \frac{e^{x^{10}-1} - 1}{x - 1} + (x-1) \sin\left(\frac{1}{x-1}\right) \\ &= \lim_{x \to 1} \frac{e^{x^{10}-1} - 1}{x - 1} + \lim_{x \to 1} (x-1) \sin\left(\frac{1}{x-1}\right) \\ &= \lim_{x \to 1} \frac{e^{x^{10}-1} - 1}{x^{10} - 1} \cdot \frac{x^{10} - 1}{x - 1} + \lim_{x \to 1} (x-1) \sin\left(\frac{1}{x-1}\right) \\ &= 1 \cdot 10 + 0 \\ &= 10. \end{aligned}$$

$$
\begin{aligned}
\lim_{u\to\infty}\left[100u - u\sum_{k=1}^{100} f\left(1+\frac{k}{u}\right)\right] &= \lim_{u\to\infty}\sum_{k=1}^{100} u\left[1 - f\left(1+\frac{k}{u}\right)\right] \\
&= \sum_{k=1}^{100}\lim_{u\to\infty} u\left[1 - f\left(1+\frac{k}{u}\right)\right] \\
&= \sum_{k=1}^{100} k\lim_{u\to\infty}\frac{1-f\left(1+\frac{k}{u}\right)}{\frac{k}{u}} \\
&= \sum_{k=1}^{100} k\lim_{h\to 0}\frac{f(1)-f(1+h)}{h} \\
&= \sum_{k=1}^{100} k(-f'(1)) \\
&= -f'(1)\sum_{k=1}^{100} k \\
&= -10\times 5050 \\
&= -50500.
\end{aligned}
$$

17.4 Some Harder Problems

1. Find all integers a and b such that $0 < a < b$ and $a^b = b^a$.

2. Which number is larger π^e or e^π

3. Prove that there are no positive real numbers x, y such that

$$x2^y + y2^{-x} = x + y$$

4. Find with proof if there are any differentiable functions $\varphi : \mathbb{R} \to \mathbb{R}$ such that $\varphi(x)$ and $\varphi'(x)$ are integers and only if x is an integer

5. Let $f : [a, b] \to \mathbb{R}$ be a differentiable function. Prove that for any positive integer n, there are numbers $\theta_1 < \theta_2 < \cdots < \theta_n$ such that

$$\frac{f(b) - f(a)}{b - a} = \frac{1}{n} \sum_{k=1}^{n} f'(\theta_k)$$

6. Let $f, g : \mathbb{R} \to \mathbb{R}$ be differentiable functions with continuous derivatives such that

$$f(x) + g(x) = f'(x) - g'(x)$$

Prove that if x_1, x_2 are two consecutive real solutions of the equation $f(x) - g(x) = 0$, then the equation $f(x) + g(x) = 0$ has at least one solution in the interval (x_1, x_2).

7. Let $\varphi : \mathbb{R} \to \mathbb{R}$ be a differentiable function at the origin and satisfying $\varphi(0) = 0$. Evaluate the following

$$\lim_{x \to 0} \left[\varphi(x) + \varphi\left(\frac{x}{2}\right) + \cdots + \varphi\left(\frac{x}{n}\right) \right]$$

8. Let a be a positive real number. Prove that there is a unique positive real number μ such that

$$\frac{\mu^x}{x^\mu} \geq a^{\mu - x} \text{ for all } x > 0$$

9. Let $f : [a, b] \to \mathbb{R}$ be a twice differentiable function on $[a, b]$ such that $f(a) = f(b)$ and $f'(a) = f'(b)$. Prove that for any real number λ the equation

$$f''(x) - \lambda(f'(x))^2 = 0$$

has a least one solution in the interval (a, b)

17.5 Differentiation MCQ

1. Let f and g be two functions defined on an interval I such that $f(x) \geq 0$ and $g(x) \leq 0$ for all $x \in I$, and f is strictly decreasing on I while g is strictly increasing on I. Then

(A) the product function fg is strictly increasing on I;

(B) the product function fg is strictly decreasing on I;

(C) the product function fg is increasing but not necessarily strictly increasing on I;

(D) nothing can be said about the monotonicity of the product function fg.

2. Given that f is a real-valued differentiable function such that $f(x)f'(x) < 0$ for all real x, it follows that

(A) $f(x)$ is an increasing function;

(B) $f(x)$ is a decreasing function;

(C) $|f(x)|$ is an increasing function;

(D) $|f(x)|$ is a decreasing function.

3. Let x and y be positive numbers. Which of the following always implies $x^y \geq y^x$?

(A) $x \leq e \leq y$;

(B) $y \leq e \leq x$;

(C) $x \leq y \leq e$ or $e \leq y \leq x$;

(D) $y \leq x \leq e$ or $e \leq x \leq y$.

4. Let f be the function $f(x) = \cos x - 1 + \frac{x^2}{2}$. Then

(A) $f(x)$ is an increasing function on the real line;

(B) $f(x)$ is a decreasing function on the real line;

(C) $f(x)$ is an increasing function in the interval $-\infty < x \leq 0$ and decreasing in the interval $0 \leq x < \infty$;

(D) $f(x)$ is a decreasing function in the interval $-\infty < x \leq 0$ and increasing in the interval $0 \leq x < \infty$.

5. Consider the function $f(n)$ defined for all positive integers as follows:

$$f(n) = \begin{cases} n+1 & \text{if } n \text{ is odd,} \\ \frac{n}{2} & \text{if } n \text{ is even.} \end{cases}$$

Let $f^{(k)}$ denote f applied k times; e.g., $f^{(1)}(n) = f(n)$, $f^{(2)}(n) = f(f(n))$ and so on. Then

(A) there exists one integer k_0 such that for all $n \geq 2$, $f^{(k_0)}(n) = 1$;

(B) for each $n \geq 2$, there exists an integer k (depending on n) such that $f^{(k)}(n) = 1$;

(C) for each $n \geq 2$, there exists an integer k (depending on n) such that $f^{(k)}(n)$ is a multiple of 4;

(D) for each n, $f^{(k)}(n)$ is a decreasing function of k.

6. Let $p_n(x)$, $n = 0, 1, \ldots$ be polynomials defined by $p_0(x) = 1$, $p_1(x) = x$ and $p_n(x) = xp_{n-1}(x) - p_{n-2}(x)$ for $n \geq 2$. Then $p_{10}(0)$ equals

(A) 0;

(B) 10;

(C) 1;

(D) -1.

7. Consider the function $f(x) = x(x-1)(x+1)$ from $\mathbb{R}$ to $\mathbb{R}$, where $\mathbb{R}$ is the set of all real numbers. Then,

(A) f is one-one and onto;

(B) f is neither one-one nor onto;

(C) f is one-one but not onto;

(D) f is not one-one but onto.

8. For all integers $n \geq 2$, define $f_n(x) = (x+1)^{1/n} - x^{1/n}$, where $x > 0$. Then, as a function of x

(A) f_n is increasing for all n;

(B) f_n is decreasing for all n;

(C) f_n is increasing for n odd and f_n is decreasing for n even;

(D) f_n is decreasing for n odd and f_n is increasing for n even.

9. Let

$$g(x) = \int_{-10}^{x} t f'(t)\, dt \quad \text{for } x \geq -10,$$

where f is an increasing function. Then

(A) $g(x)$ is an increasing function of x;

(B) $g(x)$ is a decreasing function of x;

(C) $g(x)$ is increasing for $x > 0$ and decreasing for $-10 < x < 0$;

(D) none of the foregoing conclusions is necessarily true.

10. Let

$$f(x) = \begin{cases} x^3 - x + 3 & \text{for } 0 < x \leq 1, \\ 2x + 1 & \text{for } 1 < x \leq 2, \\ x^2 + 1 & \text{for } 2 < x \leq 3. \end{cases}$$

Then

(A) $f(x)$ is differentiable at $x = 1$ and at $x = 2$;

(B) $f(x)$ is differentiable at $x = 1$ but not at $x = 2$;

(C) $f(x)$ is differentiable at $x = 2$ but not at $x = 1$;

(D) $f(x)$ is differentiable neither at $x = 1$ nor at $x = 2$.

11. If the function

$$f(x) = \begin{cases} \frac{x^2 - 2x + A}{\sin x} & \text{when } x \neq 0, \\ B & \text{when } x = 0, \end{cases}$$

is continuous at $x = 0$, then

(A) $A = 0, B = 0$;

(B) $A = 0, B = -2$;

(C) $A = 1, B = 1$;

(D) $A = 1, B = 0$.

12. The function

$$f(x) = \begin{cases} \frac{1 - \cos 4x}{x^2} & \text{if } x < 0, \\ a & \text{if } x = 0, \\ \frac{2\sqrt{x}}{\sqrt{16 + \sqrt{x}} - 4} & \text{if } x > 0, \end{cases}$$

is continuous at $x = 0$ for

(A) $a = 8$;

(B) $a = 4$;

(C) $a = 16$;

(D) no value of a.

13. Consider the function

$$f(x) = \begin{cases} 0 & \text{if } x \text{ is rational,} \\ x^2 & \text{if } x \text{ is irrational.} \end{cases}$$

Then only one of the following statements is true. Which one is it?

(A) f is differentiable at $x = 0$ but not continuous at any other point.

(B) f is not continuous anywhere.

(C) f is continuous but not differentiable at $x = 0$.

(D) None of the foregoing statements is true.

14. Let $f(x) = x \sin \frac{1}{x}$ if $x \neq 0$, and let $f(x) = 0$ if $x = 0$. Then f is

(A) not continuous at 0;

(B) continuous but not differentiable at 0;

(C) differentiable at 0 and $f'(0) = 1$;

(D) differentiable at 0 and $f'(0) = 0$.

15. Let $f(x)$ be the function defined on the interval $(0, 1)$ by

$$f(x) = \begin{cases} x & \text{if } x \text{ is rational,} \\ 1 - x & \text{otherwise.} \end{cases}$$

Then f is continuous

(A) at no point in $(0, 1)$;

(B) at exactly one point in $(0, 1)$;

(C) at more than one, but finitely many points in $(0, 1)$;

(D) at infinitely many points in $(0, 1)$.

16. The function $f(x) = \lfloor x \rfloor + \sqrt{x - \lfloor x \rfloor}$, where $\lfloor x \rfloor$ denotes the largest integer smaller than or equal to x, is

(A) continuous at every real number x;

(B) continuous at every real number x except at negative integer values;

(C) continuous at every real number x except at integer values;

(D) continuous at every real number x except at $x = 0$.

17. For any positive real number x and any positive integer n, we can uniquely write

$$x = mn + r,$$

where m is an integer (positive, negative, or zero) and $0 \leq r < n$. With this notation we define

$$x \mod n = r.$$

For example, $13.2 \mod 3 = 1.2$. The number of discontinuity points of the function

$$f(x) = (x \mod 2)^2 + (x \mod 4)$$

in the interval $0 < x < 9$ is

(A) 0;

(B) 2;

(C) 4;

(D) 6.

18. Let $f(x)$ and $g(x)$ be defined as follows:

$$f(x) = \begin{cases} x & \text{if } x \geq 0, \\ 0 & \text{if } x < 0, \end{cases} \quad \text{and} \quad g(x) = \begin{cases} x^2 & \text{if } x \geq 0, \\ 0 & \text{if } x < 0. \end{cases}$$

Then

(A) f and g are both differentiable at $x = 0$;

(B) f is differentiable at $x = 0$ but g is not;

(C) g is differentiable at $x = 0$ but f is not;

(D) neither f nor g is differentiable at $x = 0$.

19. The number of points at which the function

$$f(x) = \begin{cases} \min\{\lfloor x \rfloor, x^2\} & \text{if } -\infty < x < 1, \\ \min\{2x-1, x^2\} & \text{otherwise}, \end{cases}$$

is not differentiable is

(A) 0;

(B) 1;

(C) 2;

(D) more than 2.

20. If $f(x) = (\sin x)(\sin 2x) \cdots (\sin nx)$, then $f'(x)$ is

(A) $\sum_{k=1}^{n} (k \cos kx) f(x)$;

(B) $(\cos x)(2 \cos 2x)(3 \cos 3x) \cdots (n \cos nx)$;

(C) $\sum_{k=1}^{n} (k \cos kx)(\sin kx)$;

(D) $\sum_{k=1}^{n} (k \cot kx) f(x)$.

ANSWER KEY

1	2	3	4	5	6	7	8	9	10
A	D	D	D	B	D	D	B	C	B
11	12	13	14	15	16	17	18	19	20
B	D	A	B	B	A	C	C	B	D

18 Riemann Integration

You might have heard that $\int_a^b f(x)dx$ denotes the area under the graph of $f(x)$ from $x = a$ to $x = b$. But what does that really mean? Recall how we learnt the concept of area since childhood. First we define a certain shape, suppose a square, to have a 'unit area'. Then for any rectangle, we measure the sides in that unit and say that area of the rectangle is length times breadth ($l \times b$), which essentially means that the area of the rectangle is lb times the unit area. For a triangle, we perform a similar procedure (we compare its area with a rectangle). But how to define area of some arbitrary shape? Intuition says that we should try to cover up the shape using those unit squares and find out how many of the unit squares are needed. Let us now try to make this intuition precise.

Given a function f defined on $[a, b]$, we wish to define the quantity $\int_a^b f(x)dx$ such that it represents the signed area of the region in the xy-plane that is bounded by the graph of f, the x-axis and the vertical lines $x = a$ and $x = b$. The area above the x-axis adds to the total and that below the x-axis subtracts from the total.

For the time being, assume that the graph of $f(x)$ is 'simple', like the ones shown here. In order to approximate the area (as noted above), we divide the interval $[a, b]$ into some disjoint sub-intervals, suppose using the points $a = x_0 < x_1 < \cdots < x_{n-1} < x_n = b$, and pick a point t_i in each $[x_{i-1}, x_i]$ such that $f(t_i)$ would be height of a suitable rectangle that approximates the area under the curve within that sub-interval. Then we can use the sum of the areas of these rectangles to approximate the desired area.

However, there is a little problem. How do we choose those t_i's? Choosing t_i to be one of the endpoints might not always serve the purpose. Let us consider two extreme cases: when t_i is chosen such that $f(t_i)$ is the minimum or the maximum value of f within the sub-interval $[x_{i-1}, x_i]$. We know that if f is continuous on a closed bounded interval (like $[x_{i-1}, x_i]$) then it attains a minimum and a maximum within that interval. But not every bounded function f has this property we should use sup and inf instead of max and min, respectively.

For each $1 \le i \le n$, we define

$$M_i = \sup\{f(t) : x_{i-1} \le t \le x_i\}, \quad \text{and} \quad m_i = \inf\{f(t) : x_{i-1} \le t \le x_i\}.$$

Then, for any choice of t_i's, we have

$$\sum_{i=1}^{n} m_i(x_i - x_{i-1}) \le \sum_{i=1}^{n} f(t_i)(x_i - x_{i-1}) \le \sum_{i=1}^{n} M_i(x_i - x_{i-1}). \tag{1}$$

Given the partition $P = \{a = x_0 < x_1 < \cdots < x_{n-1} < x_n = b\}$, the LHS of (1) is the worst under-estimate of the desired area with this partition (worst over all possible choices of t_i) and the RHS is the worst over-estimate. Keeping aside the t_i's for the moment, we might also write

$$\sum_{i=1}^{n} m_i(x_i - x_{i-1}) \le \text{desired area} \le \sum_{i=1}^{n} M_i(x_i - x_{i-1}). \tag{2}$$

Note that these under-estimate and over-estimate depend only on the partition P (and on f of course!), so we can denote them by $L(P, f)$ and $U(P, f)$, respectively. The quantity in the middle of (1) is called a Riemann-sum approximation of the desired area.

Example 1.1. Let us consider the function $f(x) = x$ on $[0, 1]$. Take the partition P that divides $[0, 1]$ into n intervals of equal length, i.e., $P_n = \{0, 1/n, 2/n, \ldots, 1\}$. Write $x_i = i/n$ for $0 \le i \le n$. Note that for $x \in [x_{i-1}, x_i]$, the maximum possible value of $f(x)$ is $M_i = f(x_i)$ and the minimum possible value is $m_i = f(x_{i-1})$. Hence,

$$U(P_n, f) = \sum_{i=1}^{n} M_i(x_i - x_{i-1}) = \frac{1}{n}\sum_{i=1}^{n} f(x_i) = \frac{1}{n}\sum_{i=1}^{n} \frac{i}{n} = \frac{n(n+1)}{2n^2}$$

and

$$L(P_n, f) = \sum_{i=1}^{n} m_i(x_i - x_{i-1}) = \frac{1}{n}\sum_{i=1}^{n} f(x_{i-1}) = \frac{1}{n}\sum_{i=1}^{n} \frac{i-1}{n} = \frac{n(n-1)}{2n^2}.$$

In this simple example, we already know what the area should be, because the region under the curve $y = f(x) = x$ for $x \in [0, 1]$ (and bounded below by the x-axis) is just a triangle which has area $1/2$. Observe that $U(P_n, f)$ is a slight over-estimate, while $L(P_n, f)$ is a slight under-estimate, which is exactly what we expect. In fact, letting $n \to \infty$, we see that both $U(P_n, f)$ and $L(P_n, f)$ converges to $1/2$.

Note that in the above example, we just considered a specific sequence of partitions. But there always is a plethora of partitions to choose from! Then how to develop a general notion of the area? Let us go back to equation (1) once again. The Riemann-sum approximation $\sum_{i=1}^{n} f(t_i)(x_i - x_{i-1})$ is always an estimate of the area, regardless of how we choose the t_i's. Intuition says that if the sub-intervals are made smaller and smaller, then this approximation will get closer and closer to the actual area. Keeping this in mind, let us try to perceive the following definition of integrals given by Riemann:

Definition 1.1 (Riemann's definition of integrability).
We say that f is (Riemann-)integrable on $[a, b]$ if there exists a real number A such that for every $\epsilon > 0$ there exists $\delta > 0$ such that whenever a partition $P = \{a = x_0 < x_1 < \cdots < x_n = b\}$ of $[a, b]$ has the property that the length of each sub-interval is less than δ, then it holds that

$$\left|\sum_{i=1}^{n} f(t_i)(x_i - x_{i-1}) - A\right| < \epsilon,$$

irrespective of the choice of the points t_i's where $t_i \in [x_{i-1}, x_i]$. If the above holds, we write

$$\int_a^b f(x)dx = A.$$

Informally, the above definition says that by making the length of each sub-interval sufficiently small, we can ensure the Riemann-sum approximation to be as close to $\int_a^b f(x)dx$ as we please. In particular, if we take n sub-intervals of equal length (i.e., each of length $\frac{b-a}{n}$) and let $n \to \infty$, we get the following theorem:

Theorem 1.1. If f is integrable on $[a, b]$, then it holds that

$$\lim_{n\to\infty} \frac{b-a}{n}\sum_{k=1}^{n} f\left(a + k \cdot \frac{b-a}{n}\right) = \int_a^b f(x)dx.$$

On one hand, this theorem can be used to calculate integrals of very simple functions (e.g., $x, x^2, e^x, \sin x$ etc.), while on the other hand, it can be used to calculate certain limits which can be expressed as the limit in the above LHS. This latter idea is extensively used for creating and solving competition problems. We shall see some interesting examples soon!

Corollary 1.1. If f is integrable on $[0, 1]$ then

$$\lim_{n\to\infty} \frac{1}{n}\sum_{k=1}^{n} f\left(\frac{k}{n}\right) = \int_0^1 f(x)dx.$$

Question 1. If $\lim_{n\to\infty} \frac{1}{n}\sum_{k=1}^{n} f\left(\frac{k}{n}\right) = \ell$, does it always imply that $\int_0^1 f(x)dx = \ell$?

It is undeniable that even understanding the statement of Definition 1.1 takes a lot of effort, let alone the struggle of learning how to use it to prove that a given function is integrable. This is where Darboux's alternate definition (of Riemann integral) comes to our rescue. We consider all possible partitions of $[a, b]$ and try to find what are the best under-estimate and over-estimate of the desired area ,best over the choice of P, i.e., over the class of all partitions of $[a, b]$. Intuition suggests that best under-estimate is the largest one among all such under-estimates

$L(P, f)$ and best over-estimate is the smallest one among all such over-estimates $U(P, f)$. Again, here a smallest or a largest one may not exist, so we use inf and sup :

$$\text{best over-estimate} = \inf U(P, f), \quad \text{best under-estimate} = \sup L(P, f)$$

where the infimum and the supremum are taken over P, i.e., over all possible partitions of $[a, b]$. Note that $\inf U(P, f)$ exists because for any partition P, the quantity $L(P, f)$ is a lower bound on the set of all possible values of $U(P, f)$. A similar argument shows why $\sup L(P, f)$ exists. Also note that the best over-estimate is always greater than or equal to the best under-estimate, but if the former is strictly bigger than the later, then how can we define the area? Having this notion in mind, we settle for the following definition of the area/integral:

Definition 1.2 (Darboux's definition of Riemann-integrability). *We say that f is Riemann-integrable on $[a, b]$ if the 'best over-estimate' and the 'best under-estimate', as defined in (3) are equal and their common value is denoted by $\int_a^b f(x)dx$.*

The reader who is not lost yet might wonder, how can there be two definitions of the same thing? Of course this is not the first time it is happening in this Calculus course, we already had seen two equivalent definitions of continuity ($\epsilon - \delta$ definition and sequential definition). What we just need here is a proof that shows the above two definitions to be equivalent. There are such proofs, but let us skip that for now, since it will obviously be very much involved. If you are interested, you can look it up in any undergraduate-level textbook on Real Analysis.

It should however be noted that the above definition only attaches a *meaning* to the symbol $\int_a^b f(x)dx$, it does not give any method to calculate it. Moreover, the set of all partitions is so huge that even for very simple functions, it is notoriously difficult to verify the above definition, i.e., to show that $\inf U(P, f)$ and $\sup L(P, f)$ are equal. However, there is a result that is very handy when one tries to prove that a given function is integrable, which is as follows.

Result 1.1. *A function f is integrable on $[a, b]$ if and only if for every $\epsilon > 0$ there exists a partition P of $[a, b]$ such that $U(P, f) - L(P, f) < \epsilon$ holds.*

We shall not prove this result here either. However, let us use this result to find out some common classes of functions that are Riemann-integrable.

Result 1.2. *If f is monotone on $[a, b]$ then it is integrable on $[a, b]$ as well.*

Result 1.3. *If f is continuous on $[a, b]$ then it is integrable on $[a, b]$ as well.*

Proof of Result 1.2. Without loss of generality, we may assume that f is increasing. Then, for any partition $P = \{a = x_0 < x_1 < \cdots < x_{n-1} < x_n = b\}$, we have

$$U(P, f) = \sum_{i=1}^{n} f(x_i)(x_i - x_{i-1}), \quad L(P, f) = \sum_{i=1}^{n} f(x_{i-1})(x_i - x_{i-1}).$$

Hence, if we choose P such that the length of each sub-interval $[x_{i-1}, x_i]$ is small, say less than δ, then

$$U(P, f) - L(P, f) = \sum_{i=1}^{n} (f(x_i) - f(x_{i-1}))(x_i - x_{i-1}) \leq \sum_{i=1}^{n} (f(x_i) - f(x_{i-1})) \cdot \delta = (f(b) - f(a)) \cdot \delta.$$

So by choosing $\delta > 0$ such that $\delta \cdot (f(b) - f(a)) \leq \epsilon$, we are through. $\square$

Proof of Result 1.3. Since f is continuous, it attains a maximum and a minimum value in each sub-interval. Now, we wish to make the sub-intervals very small such that in each of them the difference between the maximum and minimum value of f is small enough. To achieve this, uniform continuity would help.

Since f is continuous on this closed and bounded interval $[a, b]$, we know that f must be uniformly continuous on $[a, b]$. Hence, for every $\epsilon > 0$ there exists $\delta > 0$ such that for any $x, y \in [a, b]$ such that $|x - y| < \delta$ we have $|f(x) - f(y)| < \epsilon$. Now, if we choose the partition P such that length of each sub-interval is less than this δ, then we know that $M_i - m_i$ is less than ϵ, for each i. Hence

$$U(P, f) - L(P, f) = \sum_{i=1}^{n} (M_i - m_i)(x_i - x_{i-1}) < \epsilon \sum_{i=1}^{n} (x_i - x_{i-1}) = \epsilon(b - a),$$

which completes the proof. (We could have started with $\epsilon' = \epsilon/(b-a)$ instead.) $\square$

We shall assume the following results without proof. A curious reader can locate the proofs in any UG-level textbook on Real Analysis.

Result 1.4. *If f and g are integrable on $[a,b]$, then so are $f \pm g$, cf (where c is a constant).*

Result 1.5. *If f is integrable on $[a,b]$, and g is continuous on the range of f, then $g \circ f$ is integrable.*

You are encouraged to use whatever learnt till now to answer the following questions.

Question 2. *If f is integrable on $[a,b]$, is it necessary that $|f|$ is also integrable?*

Question 3. *Suppose that f and g are integrable on $[a,b]$. Is it necessary that their product fg is also integrable on $[a,b]$? What about $\max\{f,g\}$ and $\min\{f,g\}$?*

Till now we have not seen any function which is not integrable. Following is a classical example of such kind.

Example 1.2 (Dirichlet function). Let $f : [0,1] \to \mathbb{R}$ be a function defined as

$$f(x) = \begin{cases} 0 & \text{if } x \in \mathbb{Q}, \\ 1 & \text{if } x \notin \mathbb{Q}. \end{cases}$$

Take any partition P. In each sub-interval, there is at least one rational and at least one irrational number, which implies that $M_i = 1$ and $m_i = 0$ holds for each i. Therefore,

$$U(P,f) = \sum_{i=1}^{n} 1 \cdot (x_i - x_{i-1}) = 1 \cdot (1-0) = 1, \quad L(P,f) = \sum_{i=1}^{n} 0 \cdot (x_i - x_{i-1}) = 0,$$

for any partition P. Hence we can say that f is not integrable on $[0,1]$, by noting that f does not meet the requirements in Darboux's definition.

Remark 1.1. *If we change the value of f at just one point, that does not have any influence on the integrability of f or on the value of the integral. Hence, if a function f is continuous everywhere except at just one point inside $[a,b]$, then f would be integrable, provided f is bounded. (It requires a proof though, which we skip for now.)*

Remark 1.2. *Note that from the very beginning we have imposed a condition that f must be bounded. How to define integrals of functions such as $f(x) = \log x$ on the interval $[0,1]$ or $g(x) = \tan x$ on the interval $[0,\pi]$ (with $f(0)$ and $g(\pi/2)$ being defined something forcibly)? Integral of such functions are called improper integrals and will be discussed later. For now you can just keep in mind that they are defined using limits, e.g.,*

$$\int_0^1 \log x \, dx \stackrel{\text{def}}{=} \lim_{a \to 0^+} \int_a^1 \log x \, dx.$$

Question 4. *If f is continuous on $[a,b]$ except only at 10^{10} many points, will f be necessarily integrable?*

Question 5. *Is it possible to have a function f which is integrable but discontinuous at infinitely many points?*

If you know the distinction between countably infinite and uncountably infinite, try to answer the following question.

Question 6. *If we change the value of f at countably many points, will it have any influence on the integrability of f?*

Some properties of Integrals

Result 2.1. *If f,g are integrable on $[a,b]$ then $\int_a^b (f+g) = \int_a^b f + \int_a^b g$.*

Proof. As we mentioned earlier, there is a result which says that $f+g$ is integrable if f,g are integrable. Hence we can use Theorem 1.1 to get

$$\int_a^b (f+g) = \lim_{n\to\infty} h_n \sum_{k=1}^{n} (f(a+kh_n) + g(a+kh_n)) \quad (\text{where } h_n = \frac{b-a}{n})$$

$$= \lim_{n\to\infty} h_n \sum_{k=1}^{n} f(a+kh_n) + \lim_{n\to\infty} h_n \sum_{k=1}^{n} g(a+kh_n)$$
$$= \int_a^b f + \int_a^b g$$
where in the last step we used Theorem 1.1 again.

In a similar manner we can prove the following results using Theorem 1.1 (and the reader is strongly encouraged to write their proofs, before proceeding further).

Result 2.2. *Let f, g be integrable on $[a,b]$. Then, $\int_a^b (\alpha f + \beta g) = \alpha \int_a^b f + \beta \int_a^b g$, for any constants α, β.*

Result 2.3. *Let f be integrable on $[a,b]$. Then, $\left|\int_a^b f(x)dx\right| \leq \int_a^b |f(x)|dx$.*

Result 2.4. *If f is integrable on $[a,b]$ and $f(x) \geq 0$ for all $x \in [a,b]$ then $\int_a^b f(x)dx \geq 0$.*

However, the proof of the following result involves $U(P,f)$ and $L(P,f)$, so we skip its proof for now.

Result 2.5. *Suppose that f is integrable on $[a,c]$ and on $[c,b]$. Then f must be integrable on $[a,b]$ and $\int_a^b f(x)dx = \int_a^c f(x)dx + \int_c^b f(x)dx$.*

Some solved Examples

Example 1 (MVT for integrals) *Let f be continuous and g be integrable on $[a,b]$ and assume that g is positive. Show that there exists $c \in [a,b]$ such that*

$$\int_a^b f(x)g(x)dx = f(c)\int_a^b g(x)dx.$$

Solution. Since f is continuous on $[a,b]$, we know that f attains a minimum and a maximum on $[a,b]$, say $f(m) \leq f(x) \leq f(d)$ for every $x \in [a,b]$. Since g is positive, we have

$$f(m)g(x) \leq f(x)g(x) \leq f(d)g(x), \text{ for every } x \in [a,b],$$

and hence
$$f(m)\int_a^b g(x)dx \leq \int_a^b f(x)g(x)dx \leq f(d)\int_a^b g(x)dx.$$
Now the conclusion follows from the intermediate value property of f. $\square$

Question 7. *Suppose that f is integrable and non-negative on $[a,b]$. If $\int_a^b f(x)dx = 0$, is it necessary that f must be identically zero on $[a,b]$?*

As you might have guessed, the answer to the above question is in the negative (try to find a counter-example then). However, if we impose an additional assumption that f must be continuous, then the following result holds.

Example 2: *Let f be continuous and non-negative on $[a,b]$. If $\int_a^b f(x)dx = 0$, then show that f must be identically zero on $[a,b]$.*

Intuition says that if f is strictly positive at some point, then there will be a part of the curve $y = f(x)$ that lies strictly above the x-axis, which implies that the area under the curve can not be zero. Let us now try to write a rigorous proof, with the help of ϵ and δ.

Solution. Let, if possible, there be a point $c \in (a,b)$ such that $f(c) > 0$. By continuity, for $\epsilon = f(c)/2$, there exists a $\delta > 0$ such that $|f(x) - f(c)| < \epsilon$ for every $|x - c| < \delta$. Note that

$$|f(x) - f(c)| < \epsilon \implies \epsilon > |f(c)| - |f(x)| \implies f(x) > f(c)/2.$$

Since $f \geq 0$ on $[a, b]$, we have

$$\int_a^b f = \int_a^{c-\delta} f + \int_{c-\delta}^{c+\delta} f + \int_{c+\delta}^b f \geq \int_{c-\delta}^{c+\delta} f(x)dx \geq \int_{c-\delta}^{c+\delta} f(c)/2\, dx = f(c) \cdot \delta > 0$$

which violates the given condition that $\int_a^b f = 0$. Therefore, for $\int_a^b f(x)dx = 0$, we need $f(x) = 0$ for all $x \in (a, b)$.

Finally, the continuity of f ensures that $f(a) = 0 = f(b)$. $\square$

Example 3: *Suppose that $f : \mathbb{R} \to \mathbb{R}$ is continuous and satisfies*

$$\int_0^1 f(x)(1 - f(x))dx = \frac{1}{4}.$$

What can you say about f?

Solution. First note that

$$\int_0^1 f(x)(1 - f(x))dx = \frac{1}{4} \implies \int_0^1 (f(x) - 1/2)^2 dx = 0.$$

Since the function $g(x) = (f(x) - 1/2)^2$ is continuous and non-negative, this implies that $g(x) = 0$, i.e., $f(x) = 1/2$ for every $x \in [0, 1]$. However, having no information on f outside the interval $[0, 1]$, we are unable to conclude anything about f beyond $[0, 1]$. $\square$

Example 4. (Cauchy-Schwarz inequality) *Let f, g be integrable on $[a, b]$. Prove that*

$$\left(\int_a^b f(x)^2 dx\right)\left(\int_a^b g(x)^2 dx\right) \geq \left(\int_a^b f(x)g(x)dx\right)^2.$$

Furthermore, if f, g are continuous, then equality holds if and only if $f(x) = \lambda g(x)$ for some constant λ and for all $x \in [a, b]$.

One way to prove this is to use Theorem 1.1, which I encourage you to write down. This proof, however, fails to provide a justification for the equality case here. So we shall give another proof below, which essentially mimics the proof of C-S inequality for real numbers.

Solution. For $t \in \mathbb{R}$ define

$$h(t) = \int_a^b (f(x) - tg(x))^2 dx = At^2 - 2Bt + C,$$

where

$$A = \int_a^b g(x)^2 dx, \quad B = \int_a^b f(x)g(x)dx, \quad C = \int_a^b f(x)^2 dx.$$

Now, $h(t)$ is a quadratic in t, which is always non-negative, with leading coefficient $A > 0$ (the case $A = 0$ is trivial, in view of the Result 3.2). Hence it follows that the discriminant $4B^2 - 4AC$ must be non-positive, i.e.,

$$B^2 \leq AC.$$

This is precisely the C-S inequality that we wanted to show. For equality to hold, we must have discriminant equal to zero, which says that the function $h(t)$ has a real root, say $t = \lambda$. After a little algebra, this is seen to be same as saying that

$$h(\lambda) = \int_a^b (f(x) - \lambda g(x))^2 dx = 0.$$

Since the function $(f(x) - \lambda g(x))^2$ is continuous and non-negative, Result 3.2 implies that $f(x) - \lambda g(x)$ must be identically zero on $[a, b]$. $\square$

18.1 Exercise 1

1. Define $f(x) = \int_0^x |t - x| dt$, for $x \in \mathbb{R}$. Sketch the graph of $f(x)$. What is the minimum value of $f(x)$?

2. For any positive integer n, let $C(n)$ denote the number of points which have integer coordinates and lie inside the circle $x^2 + y^2 = n^2$. Show that the limit

$$\lim_{n\to\infty} \frac{C(n)}{n^2}$$

exists and also evaluate this limit. Can you explain the result intuitively?

3. Let f, g be polynomials of degree n such that $\int_0^1 x^k f(x)dx = \int_0^1 x^k g(x)dx$ holds for each $k = 0, 1, \ldots, n$. Show that $f = g$.

4. Let f, g be continuous and positive functions defined on $[0, 1]$ satisfying

$$\int_0^1 f(x)dx = \int_0^1 g(x)dx.$$

Define $y_n = \int_0^1 \left(\frac{f(x)}{g(x)}\right)^{n+1} dx$, for every integer $n \geq 0$. Show that $\{y_n\}_{n\geq 0}$ is an increasing sequence.

5. Suppose that f is integrable on $[a, b]$. Define

$$F(x) = \int_a^x f(t)dt, \text{ for } a \leq x \leq b.$$

Then, (i) if F is continuous on $[a, b]$, and (ii) if f is continuous at $c \in [a, b]$, then F will be differentiable at c, with $F'(c) = f(c)$.

6. If f is differentiable on $[a, b]$, such that f' is continuous on $[a, b]$, then

$$\int_a^b f'(x)dx = f(b) - f(a).$$

7. If f is continuous on $[a, b]$, show that

$$\int_a^b f(t)dt = f(c)(b - a) \text{ must hold for some } c \in (a, b).$$

8. Let $f : [0, 1] \to \mathbb{R}$ be a continuous function such that

$$\int_0^1 f(x)dx = 1.$$

Show that there exists a point $c \in (0, 1)$ such that $f(c) = 3c^2$.

9. Prove the inequalities:

$$\frac{\pi^2}{9} \leq \int_{\pi/6}^{\pi/2} \frac{x}{\sin x} dx \leq \frac{2\pi^2}{9}.$$

18.2 Fundamental Theorem of Calculus

Connection with derivatives

It would not be much of an overstatement if we say that derivatives and integrals are the two main pillars of the whole of Calculus. Derivatives represent the rate of change of a function and integrals represent the area under the curves. In this section we shall try to find the connection between these two seemingly different concepts.

Suppose that f is differentiable on $[a,b]$. Let us take a partition of $[a,b]$, say $P = \{a = x_0 < x_1 < \cdots < x_{n-1} < x_n = b\}$. Observe that we can write

$$f(b) - f(a) = \sum_{i=1}^{n}(f(x_i) - f(x_{i-1})) = \sum_{i=1}^{n} \frac{f(x_i) - f(x_{i-1})}{x_i - x_{i-1}} \cdot (x_i - x_{i-1}). \tag{1}$$

Now Lagrange's Mean Value Theorem tells us that for each sub-interval $[x_{i-1}, x_i]$, there exists $t_i \in (x_{i-1}, x_i)$ such that

$$\frac{f(x_i) - f(x_{i-1})}{x_i - x_{i-1}} = f'(t_i).$$

Therefore we can write from (1) that

$$\sum_{i=1}^{n} f'(t_i) \cdot (x_i - x_{i-1}) = f(b) - f(a).$$

If we now assume that f' is integrable, then making the partition finer and finer makes the above LHS closer and closer to

$$\int_a^b f'(x)dx.$$

In fact, Theorem 1.3 applies here and tells us that the LHS converge to $\int_a^b f'(x)dx$ if the maximum length of any sub-interval for P goes to zero.

Hence we have the following theorem.

Theorem 1.1 : FTC-integral of a derivative If f is differentiable on $[a,b]$ such that f' is integrable on $[a,b]$, then

$$\int_a^b f'(x)dx = f(b) - f(a).$$

The above theorem is known as a Fundamental Theorem of Calculus. It tells us what will be the integral of a derivative. There is one more fundamental theorem (given below) which tells us what will be the derivative of an integral.

The importance of the above theorem lies in the fact that it allows us to calculate the integral of a function g provided we have another function f such that $f' = g$. Such a function f is called an anti-derivative of g. Why 'an'? Because it is not unique: if $f(x)$ is an anti-derivative of $g(x)$, then so is $f(x) + c$, for any constant c. Does integrable functions always have anti-derivatives? In general the answer is 'No' (we'll see such examples). However, if we impose continuity, then we get a positive answer, as given in the following theorem.

Theorem 1.2 : FTC-derivative of an integral Suppose that f is integrable on $[a,b]$. Define

$$F(x) = \int_a^x f(t)dt, \text{ for } a \leq x \leq b.$$

Then, (i) F is continuous on $[a,b]$, and (ii) if f is continuous at $c \in [a,b]$, then F will be differentiable at c, with $F'(c) = f(c)$.

Before proving this theorem, let us understand what it really says and why that should be true. The theorem says that if we 'slide' x from a to b, the (signed) area $\int_a^x f(t)dt$ changes continuously (as a function of x) and if f is continuous at c, then the rate of this change in area (at c) is same as value of f at that point.

However, it might not be very clear why the rate of the change in area is same as the value of f at that point. For this, consider the diagram on the right. If we take h small enough, then the change in area from x to $x+h$, which is $F(x+h)-F(x)$, can be very well approximated by the area of the rectangle that has height $f(x)$ and width h. Hence, the rate of change in area is approximately $f(x)$. We shall next prove (rigorously) that as $h \to 0$, this rate of change converges to $f(x)$, which is exactly what the theorem tells us.

Proof of Theorem 1.2. Since integrals are defined for bounded functions only, let us take $M > 0$ such that $|f(x)| < M$ holds for all $x \in [a,b]$. Then, for any $x \in [a,b]$ and $h > 0$ (such that $x+h \in [a,b]$ as well) we have

$$|F(x+h)-F(x)| = \left|\int_x^{x+h} f(t)dt\right| \leq \int_x^{x+h} |f(t)|dt \leq \int_x^{x+h} M dt = Mh.$$

Similarly, for $h < 0$, we have

$$|F(x+h)-F(x)| \leq \int_x^{x+h} M dt = M(-h).$$

Combining these, we may write $|F(x+h)-F(x)| \leq M|h|$, which implies that F is (uniformly) continuous on $[a,b]$.

To prove the other part, let f be continuous at c. Observe that for $h > 0$,

$$\left|\frac{F(c+h)-F(c)}{h} - f(c)\right| = \left|\frac{1}{h}\int_c^{c+h} f(t)dt - hf(c)\right| = \left|\frac{1}{h}\int_c^{c+h} (f(t)-f(c))dt\right| \leq \frac{1}{h}\int_c^{c+h} |f(t)-f(c)|dt.$$

Now, since f is continuous at c, so for any $\epsilon > 0$ there exists $\delta > 0$ such that $|f(t)-f(c)| \leq \epsilon$ holds for every $t \in [a,b]$ such that $|t-c| \leq \delta$. Hence, if we take $0 < h < \delta$, then we have

$$\left|\frac{F(c+h)-F(c)}{h} - f(c)\right| \leq \frac{1}{h}\int_c^{c+h} |f(t)-f(c)|dt \leq \frac{\epsilon}{h}\int_c^{c+h} dt = \epsilon.$$

Similar result holds for $h < 0$. Combining them, we can say that for every $\epsilon > 0$ there exists $\delta > 0$ such that

$$\left|\frac{F(c+h)-F(c)}{h} - f(c)\right| < \epsilon \text{ holds for } 0 < |h| < \delta.$$

Therefore, from the definition of derivative, we conclude that $F'(c) = f(c)$. $\square$

When I first learned the above two theorems (Theorems 1.1 and 1.2), I had the following thought:

> If f is continuous and I want to find $\int_a^b f(x)dx$, then Theorem 1.1 says that I need an anti-derivative F of f, and Theorem 1.2 provides one such anti-derivative. So in this manner, I can find $\int_a^b f(x)dx$ for any continuous function f!

Unfortunately, this is a very stupid idea. To see why, take any continuous f, say $f(x) = x^2$. Then, note that the anti-derivative of $f(x) = x^2$ provided by Theorem 1.2 is

$$F(x) = \int_0^x t^2 dt.$$

and then Theorem 1.1 would help us calculate the integral as

$$\int_1^2 x dx = F(2) - F(1).$$

But how to get the values of $F(2)$ and $F(1)$? The way F is defined, we have to calculate an integral which is essentially the same as the original one – we are back to square one!

Thus, although Theorem 1.2 guarantees the existence of an anti-derivative of any continuous function, it does not provide us a way to calculate it. And without an anti-derivative how can we find the integral using Theorem 1.1!

This is why students are first taught how to guess an anti-derivative, under the name of 'indefinite integration'. All the chapters on indefinite integration actually teach us how to cleverly guess an anti-derivative for a given function. For example, we learn that an anti-derivative of x is $x^2/2$, and we write

$$\int x dx = x^2/2 + c,$$

to mean that a function F is an anti-derivative of $f(x) = x$ if and only if $F(x) = x^2/2 + c$ for some constant c. The notation

$$\int x dx$$

is simply a placeholder for 'an anti-derivative of $f(x) = x$', it does not directly relate to an area in any way. From a computational perspective, finding an anti-derivative for a given function g is not easy (at least not as easy as finding the derivative of a function). That is why we develop different ways to guess anti-derivatives, e.g., substitution, integration by parts, reduction formulae etc. I assume that the reader has already seen a fair amount of indefinite integration (or, will see them in due course of time), here we shall mainly focus on the theory of (definite) integrals that relate to area under the curves!

The following examples illustrate why one must check the conditions before applying the above theorems.

Example 1.1. Define $f(x) = x^2 \sin \frac{1}{x^2}$ if $x \neq 0$ and $f(0) = 0$. Note that f is differentiable on $[-1, 1]$. For $x \neq 0$,

$$f'(x) = 2x \sin \frac{1}{x^2} - 2 \cos \frac{1}{x} \cdot \frac{1}{x^2}$$

and $f'(0) = 0$. Yet, it is incorrect to write that

$$\int_{-1}^{1} f'(x)dx = f(1) - f(-1) = 0.$$

Why? Because f' being unbounded near $x = 0$, the above integral is an improper integral, so we cannot directly apply FTC here. In fact, it turns out that the above integral does not exist, even in the improper sense. To see why, let $g(x) = 2\cos(1/x^2)$ and note that $\cos(1/x^2) \geq 1/2$ for $|x| < \sqrt{3/\pi} = a$, hence

$$\int_0^a \frac{2}{x} \cos\left(\frac{1}{x^2}\right) dx \geq \int_0^a \frac{1}{x} dx = \lim_{\epsilon \to 0^+} \int_\epsilon^a \frac{1}{x} dx = \lim_{\epsilon \to 0^+} (\log a - \log \epsilon) = +\infty.$$

Similarly, you can show that $\int_0^a g(x)dx = -\infty$. Hence $\int_{-a}^a g(x)dx$ does not exist, even though it is tempting to write $\int_{-a}^a g(x)dx = \int_0^a (g(t) + g(-t))dt = 0$.

Example 1.2. Take $f(x) = \lfloor x \rfloor, 0 \leq x \leq 2$. This function has discontinuity only at $x = 1$ and $x = 2$, so it is integrable. Define

$$F(x) = \int_0^x f(t)dt, 0 \leq x \leq 2.$$

Observe that $F(x) = 0$ for $0 \leq x \leq 1$ and $F(x) = x - 1$ for $1 \leq x \leq 2$. Hence, F is not differentiable at $x = 1$. Does it contradict FTC? No, because f is not continuous at $x = 1$.

(In fact, this function f cannot have an anti-derivative. Because, if there were any function F such that $F' = f$, then F must have the Intermediate Value Property (derivatives always have IVP). But our f does not have IVP.)

Question 1. In Example 1, if f is differentiable but the derivative is not integrable, while in Example 2, f is integrable but the integral is not differentiable. Now, if f is integrable on $[a, b]$ and the integral from a to x is differentiable w.r.t. x, is it necessary that F' equals f?

The answer to the above question is again in the negative, as shown by the following example.

Example 1.3. Consider $f : [0, 2] \to \mathbb{R}$ as $f(x) = x$ for $x \neq 1$, and set $f(1) = 2$. Define

$$F(x) = \int_0^x f(t)dt, 0 \leq x \leq 2.$$

Clearly, F is differentiable, but $F'(1) \neq f(1)$.

Theorem 1.3 If f is integrable on $[a, b]$, then it holds that

$$\lim_{n\to\infty} \frac{b-a}{n} \sum_{k=1}^{n} f\left(a + k \cdot \frac{b-a}{n}\right) = \int_a^b f(x)dx.$$

Some Solved Examples

Example 1: *Let $f : \mathbb{R} \to \mathbb{R}$ be continuous. Define $g(x) = \int_0^x (x-t)f(t)dt$ for every $x \in \mathbb{R}$. Show that $g'' = f$.*

Solution. First we write $g(x)$ as:

$$g(x) = x\int_0^x f(t)dt - \int_0^x tf(t)dt.$$

Since f is continuous on $\mathbb{R}$, by the fundamental theorem of calculus (FTC) we know that $F(x) = \int_0^x f(t)dt$ is differentiable at each $x \in \mathbb{R}$ and $F' = f$. Also, since $h(t) = tf(t)$ is continuous on $\mathbb{R}$, by FTC we know that

$$H(x) = \int_0^x tf(t)dt$$

is differentiable at each $x \in \mathbb{R}$ and $H'(x) = h(x) = xf(x)$. Therefore $g(x) = xF(x) - H(x)$ is differentiable and

$$g'(x) = F(x) + xF'(x) - xF'(x) = F(x).$$

Hence g' is also differentiable and $g''(x) = F'(x) = f(x)$.

Example 2: *Let $f : \mathbb{R} \to \mathbb{R}$ be continuous and periodic with period $T > 0$. Prove that for every $a \in \mathbb{R}$,*

$$\int_a^{a+T} f(x)dx = \int_0^T f(x)dx.$$

Solution. Define $F(x) = \int_0^x f(t)dt$ for any $x \in \mathbb{R}$. Also, let

$$g(a) = \int_a^{a+T} f(x)dx = F(a+T) - F(a).$$

Since f is continuous on $\mathbb{R}$, by FTC, we know that $F'(x) = f(x)$ at every $x \in \mathbb{R}$. Hence

$$\frac{d}{da}g(a) = \frac{d}{da}(F(a+T) - F(a)) = f(a+T) - f(a) = 0.$$

Hence g is a constant function, and therefore $g(a) = g(0)$, i.e., for every $a \in \mathbb{R}$,

$$\int_a^{a+T} f(x)dx = \int_0^T f(x)dx$$

which is exactly what we had to show.

Example 3 (Leibniz Rule) *Let f be continuous on $[a, b]$, and u and v be differentiable functions from $[c, d]$ to $[a, b]$. Prove that,*

$$\frac{d}{dx}\int_{u(x)}^{v(x)} f(t)dt = f(v(x))v'(x) - f(u(x))u'(x).$$

Solution. Define $F(y) = \int_a^y f(t)dt$ for every $y \in [a, b]$. Now for $x \in [c, d]$,

$$I(x) = \int_{u(x)}^{v(x)} f(t)dt = F(v(x)) - F(u(x)).$$

Since f is continuous, we know that $F' = f$. Hence, by chain rule of differentiation,

$$I'(x) = F'(v(x))v'(x) - F'(u(x))u'(x) = f(v(x))v'(x) - f(u(x))u'(x)$$

for every $x \in [c, d]$.

Example 4: *Let $a_0 = 0 < a_1 < a_2 < \cdots < a_n$ be real numbers. Suppose that $p(t)$ is a real-valued polynomial of degree n such that*

$$\int_{a_j}^{a_{j+1}} p(t)dt = 0, \text{ for each } 0 \le j \le n-1.$$

Prove that the polynomial $p(t)$ must have exactly n real roots.

Solution. Define $F(x) = \int_0^x p(t)dt$, for any $x > 0$. For each $0 \le j \le n-1$,

$$\int_{a_j}^{a_{j+1}} p(t)dt = F(a_{j+1}) - F(a_j) = 0.$$

Since $p(t)$ is continuous everywhere, we have $F'(x) = p(x)$. By applying Rolle's theorem on $F(x)$, we get a root of $p(x) = F'(x)$ in each (a_j, a_{j+1}).

18.3 Exercise 2

1. (a) For each positive integer n, define a function f_n on $[0,1]$ by $f_n(x) = x^n$. Evaluate

$$\lim_{n\to\infty}\left(\int_0^1 f_n(x)dx\right) \quad \text{and} \quad \int_0^1 \left(\lim_{n\to\infty} f_n(x)\right) dx.$$

(b) Repeat the above exercise with $f_n(x) = nx^n$ for $0 \le x < 1$, and $f_n(1) = 0$.

2. Suppose that f has an anti-derivative F on an interval I, i.e., $F'(x) = f(x)$ for all $x \in I$. Let $x_0 \in I$ such that $\lim_{x\to x_0^+} f(x) = a$. Prove that $f(x_0) = a$.

3. Let f be continuous on $[a,b]$. Suppose that $\int_a^c f(x)dx = 0$ holds for every $a \le c \le b$. Show that f must be identically zero on $[a,b]$.

4. Let f be continuous on $\mathbb{R}$. Suppose that for some $T > 0$,

$$\int_a^{a+T} f(x)dx = \int_0^T f(x)dx$$

holds for every $a \in \mathbb{R}$. Show that $f(x+T) = f(x)$ for every $x \in \mathbb{R}$.

5. Define $I_n = \int_0^1 \frac{x^n}{\sqrt{x^2+1}}dx$, for every $n \in \mathbb{N}$. Prove that, $\lim_{n\to\infty} nI_n = \frac{1}{\sqrt{2}}$.

6. Prove the inequality: $0.4 < \int_0^1 x^{\sin x + \cos x} dx < 0.5$.

7. Find a $\alpha \in \mathbb{R}$ which maximises the value of the following integral

$$\int_{a-1}^{a+1} \frac{1}{1+x^8} dx.$$

8. Let $f : [0,\infty) \to \mathbb{R}$ be a non-decreasing function. Then show that the following inequality holds for all x, y, z such that $0 \le x < y < z$.

$$(z-x)\int_y^z f(u)du \ge (z-y)\int_x^z f(u)du.$$

9. Let $f(u)$ be a continuous function and, for any real number u, let $[u]$ denote the greatest integer less than or equal to u. Show that for any $x > 1$,

$$\int_1^x [u]([u]+1)f(u)du = 2\sum_{n=1}^{[x]} n \int_n^x f(u)du.$$

18.4 Applications of the Fundamental Theorems of Calculus

Integrating by parts

Suppose that f, g are differentiable functions, such that their derivatives are integrable on $[a,b]$. Since $(fg)' = f'g + fg'$, we can write

$$\int_a^b (f(x)g'(x))\,dx = \int_a^b \big((f(x)g(x))' - f'(x)g(x)\big)\,dx.$$

Now applying FTC, we get

$$\int_a^b f(x)g'(x)\,dx = f(x)g(x)\Big|_a^b - \int_a^b f'(x)g(x)\,dx.$$

This formula is commonly known as integrating by parts. It is particularly useful when it is difficult to find an anti-derivative of fg', but easy to do the same for $f'g$. For example, if $f(x) = \tan^{-1} x$ and $g(x) = x$, then note that it is difficult to directly find an anti-derivative of $f(x)g'(x) = \tan^{-1} x$, but for $f'(x)g(x) = \frac{x}{1+x^2}$ we immediately see that $\frac{1}{2}\log(1+x^2)$ is an anti-derivative. This is the key idea behind integration by parts: we split fg' into two parts, namely $(fg)'$ and $f'g$, each of which are easier to integrate.

An alternate form of integration by parts is found in Indian textbooks. Suppose that $g(x)$ is an anti-derivative of some function $h(x)$. Note that,

$$\int_a^b f(x)h(x)\,dx = \int_a^b f(x)g'(x)\,dx = f(x)g(x)\Big|_a^b - \int_a^b f'(x)g(x)\,dx.$$

Since g is an anti-derivative of h, we may write $g(x) = \int h(x)\,dx$. Then, the above equation takes the form

$$\int_a^b f(x)h(x)\,dx = \left(f(x)\int h(x)\,dx\right)\Big|_a^b - \int_a^b f'(x)\left(\int_a^x h(x)\,dx\right)dx. \tag{1}$$

Here I emphasize on the fact that $\int h(x)\,dx$ is just a short-hand notation for an anti-derivative of h; it does not represent any area or anything like that. This is why it will be wrong to write that

$$\int_a^b f(x)h(x)\,dx = \left(f(x)\int_a^b h(x)\,dx\right)\Big|_a^b - \left(\int_a^b f'(x)\int_a^b h(x)\,dx\right)dx.$$

even though the by parts formula for indefinite integration reads

$$\int f(x)h(x)\,dx = \left(f(x)\int h(x)\,dx\right) - \int \left(f'(x)\int h(x)\,dx\right)dx.$$

Remark 1.1. While calculating the indefinite integral of h in (1), we need not put an arbitrary constant c, because it would get cancelled out (can you see why?).

Example 1.1. Calculate $\int_0^1 \log x\,dx$.

Solution. Note that this is actually an improper integral, since log is unbounded near 0. So let us instead calculate $\int_a^1 \log x\,dx$ first, and then we will take a limit at $a \to 0^+$. To evaluate the last integral, we integrate by parts. Set $f(x) = \log x$ and $g(x) = x$ and write

$$\int_a^1 \log x\,dx = \int_a^1 fg' = f(x)g(x)\Big|_a^1 - \int_a^1 f'g = x\log x\Big|_a^1 - \int_a^1 \frac{x}{x}\,dx = -a\log a + a - 1.$$

Now we can show that $\lim_{a\to 0^+} a\log a = 0$. Hence $\int_0^1 \log x\,dx = -1$. $\square$

Substitution formula

Suppose that f, g are differentiable functions such that $(f \circ g)(x) = f(g(x))$ is well-defined, say for $x \in [a, b]$. Then the chain rule of differentiation states that

$$\frac{d}{dx} f(g(x)) = f'(g(x))g'(x).$$

Integrating this equation from $x = a$ to b, we obtain (using FTC)

$$\int_a^b f'(g(x))g'(x)\,dx = \int_a^b (f \circ g)'(x)\,dx = f(g(b)) - f(g(a)) = \int_{g(a)}^{g(b)} f'(u)\,du.$$

This is exactly the substitution formula that you are possibly aware of, from high-school textbooks. Usually in high-school, our teachers tell the same thing in a slightly different manner. They say the following:

Substitute $u = g(x)$, so that $du = g'(x)\,dx$. Now $u = g(a)$ when $x = a$, and $u = g(b)$ when $x = b$. Hence

$$\int_a^b f'(g(x))g'(x)\,dx = \int_{g(a)}^{g(b)} f'(u)\,du.$$

While the above is sufficient for a first course in Calculus, it is now a good time to learn rigorously when the above holds, and when it does not. If you are still under the impression that the above holds always, let me weaken your confidence for a moment, by giving the following example.

Example 1.2. Let $\phi(\theta) = \tan\theta$ and $f(x) = 1/(1 + x^2)$. Observe that

$$\int_0^\pi f(\phi(\theta))\phi'(\theta)\,d\theta = \int_0^\pi \frac{\sec^2\theta}{1 + \tan^2\theta}\,d\theta = \int_0^\pi d\theta = \pi.$$

Now, if we blindly apply the substitution formula, we get

$$\int_0^\pi f(\phi(\theta))\phi'(\theta)\,d\theta = \int_{\phi(0)}^{\phi(\pi)} f(x)\,dx = \int_0^0 f(x)\,dx = 0.$$

But this is absurd, because it yields that $\pi = 0$. Where is the mistake?

You should try yourself finding out what's wrong in the above example, I shall answer it later (in this note though). By now you should be convinced that we need to check some conditions before applying the substitution formula. The following theorem answers that, by putting minimal conditions on the function for the substitution (here, $u = \phi(t)$).

Theorem 1.1. Let $\phi : [a, b] \to I$ be a differentiable function, where $I \subseteq \mathbb{R}$ is an interval. Suppose that ϕ' is integrable on $[a, b]$. Let $f : I \to \mathbb{R}$ be a continuous function. Then,

$$\int_a^b f(\phi(t))\phi'(t)\,dt = \int_{\phi(a)}^{\phi(b)} f(x)\,dx.$$

Proof. Choose any $c \in I$ and define

$$F(y) = \int_c^y f(x)\,dx, \quad y \in I.$$

Since f is continuous, we can apply FTC-I (or the Leibniz rule) which tells us that $F(y)$ must be differentiable w.r.t. y on I, with $F'(y) = f(y)$. Hence, using the chain rule of differentiation,

$$\int_a^b f(\phi(t))\phi'(t)\,dt = \int_a^b F'(\phi(t))\phi'(t)\,dt = \int_a^b (F \circ \phi)'(t)\,dt.$$

Applying FTC-II here, we can say that

$$\int_a^b (F \circ \phi)'(t)\,dt = F(\phi(b)) - F(\phi(a)) = \int_{\phi(a)}^{\phi(b)} f(x)\,dx.$$

The last equality follows from the definition of F.

There is another formulation of the substitution formula, where we don't restrict f to be continuous (we just need f to be integrable); however we need to pay it off by restricting ϕ to be bijective. This version is stated in the following theorem.

Theorem 1.2. Let $\phi : [a,b] \to I$ be a differentiable, bijective function, where $I \subseteq \mathbb{R}$ is an interval. Suppose that ϕ' is integrable on $[a,b]$. Let $f : I \to \mathbb{R}$ be an integrable function. Then,

$$\int_a^b f(\phi(t))\phi'(t)\,dt = \int_{\phi(a)}^{\phi(b)} f(x)\,dx.$$

Proof of the last theorem is not as simple as the first one, let us skip it for now. Let us now go through some more examples.

Example 1.3. Suppose we want to calculate $\int_0^2 x\cos(x^2+1)\,dx$. Here we make the substitution $u = \phi(x) = x^2+1$. The substitution formula gives

$$\int_0^2 x\cos(t^2+1)\,dt = \int_0^2 \frac{1}{2}\cos(\phi(t))\phi'(t)\,dt = \frac{1}{2}\int_{\phi(0)}^{\phi(2)} \cos\,dx = \frac{\sin 5 - \sin 1}{2}.$$

Note that in this example we used the substitution formula from left to right.

Example 1.4. Suppose we want to calculate $\int_0^1 \sqrt{1-x^2}\,dx$. As usual, we substitute $x = \sin\theta$ here. So, $f(x) = \sqrt{1-x^2}$ and $x = \sin\theta = \phi(\theta)$. Using the substitution formula, we get

$$\int_0^1 \sqrt{1-x^2}\,dx = \int_{\phi(0)}^{\phi(\pi/2)} f(x)\,dx = \int_0^{\pi/2} f(\phi(t))\phi'(t)\,dt = \int_0^{\pi/2} \cos^2 u\,du = \frac{\pi}{4}.$$

The last integral is calculated using $2\cos^2 u = 1 + \cos 2u$. Note that in this example we used the substitution formula from right to left. Note that this example actually gives us a proof of the fact that area of a circle is πr^2 where r is the radius of the circle.

Using the substitution formula, we can prove the following simple results, which are frequently used to manipulate definite integrals.

1. $\int_a^b f(x)\,dx = \int_a^b f(a+b-x)\,dx$.
2. $\int_a^b f(x)\,dx = \int_a^b f(a-x)\,dx$.
3. $\int_0^{2a} f(x)\,dx = \int_0^a (f(x) + f(2a-x))\,dx$.
4. $\int_{-a}^a f(x)\,dx = \int_0^a (f(x)+f(-x))\,dx = \begin{cases} 0 & \text{if } f \text{ is an odd function} \\ 2\int_0^a f(x)\,dx & \text{if } f \text{ is an even function} \end{cases}$

Example 1.2 (continuing from p. 3). One reason why the substitution formula failed in this example is that $\phi(\theta) = \tan\theta$ is not really a function from $[0,\pi]$ to an interval $I \subseteq \mathbb{R}$, because $\tan(\pi/2)$ is undefined. If instead you first break the integral into two parts, one from $(0,\pi/2)$ and another from $(\pi/2,\pi)$, then we have no conflict:

$$\begin{aligned}
\pi &= \int_0^\pi \frac{\sec^2\theta}{1+\tan^2\theta}\,d\theta = \int_0^\pi f(\phi(\theta))\phi'(\theta)\,d\theta \\
&= \lim_{a\to(\pi/2)^-} \int_0^a f(\phi(\theta))\phi'(\theta)\,d\theta + \lim_{b\to(\pi/2)^+} \int_b^\pi f(\phi(\theta))\phi'(\theta)\,d\theta \\
&= \lim_{a\to(\pi/2)^-} \int_{\phi(0)}^{\phi(a)} f(u)\,du + \lim_{b\to(\pi/2)^+} \int_{\phi(b)}^{\phi(\pi)} f(u)\,du \\
&= \lim_{a\to(\pi/2)^-} \left[\tan^{-1}(u)\right]_{\phi(0)}^{\phi(a)} + \lim_{b\to(\pi/2)^+} \left[\tan^{-1}(u)\right]_{\phi(b)}^{\phi(\pi)} \\
&= \lim_{a\to(\pi/2)^-} \tan^{-1}(a) - \lim_{b\to(\pi/2)^+} \tan^{-1}(b) = \pi/2 - (-\pi/2) = \pi.
\end{aligned}$$

If you are still wondering exactly where did the proof fail, take $F(x) = \tan^{-1}(x)$ so that $F' = f$, and note that the following equality, the second equality fails here.

$$\int_0^\pi F'(g(x))g'(x)\,dx = \int_0^\pi (F \circ g)'(x)\,dx = F(g(\pi)) - F(g(0)) = \int_{g(0)}^{g(\pi)} F'(u)\,du.$$

Why does that fail? FTC does not apply here since the integrand is not even continuous at $t = \pi/2$, as

$$(F \circ \phi)(t) = \tan^{-1}(\tan(t)) = \begin{cases} t & \text{if } 0 \le t \le \pi/2 \\ t - \pi & \text{if } \pi/2 \le t \le \pi. \end{cases}$$

Some solved examples

Problem 2.1. Determine, with proof, the value of $\lim_{n\to\infty} \sqrt[n]{n!}/n$.

Solution. Observe that

$$\lim_{n\to\infty} \log\left(\sqrt[n]{n!}/n\right) = \lim_{n\to\infty} \frac{1}{n}\sum_{k=1}^{n} \log\frac{k}{n} = \int_0^1 \log x\,dx.$$

We calculated this integral in the Example 1 in today's class. Thus

$$\lim_{n\to\infty} \frac{1}{n}\sum_{k=1}^{n} \log\frac{k}{n} = \int_0^1 \log x\,dx = -1.$$

Finally, since $x \mapsto e^x$ is continuous we conclude that the desired limit is e^{-1}. (Ans.)

Problem 2.2. Let $f(x)$ be a continuous function, whose first and second derivatives are continuous on $[0, 2\pi]$ and $f''(x) \ge 0$ for all $x \in [0, 2\pi]$. Show that

$$\int_0^{2\pi} f(x)\cos x\,dx \ge 0.$$

Solution. The key idea is to integrate by parts.

$$\begin{aligned}\int_0^{2\pi} f(x)\cos x\,dx &= \left[f(x)\int \cos x\,dx\right]_0^{2\pi} - \int_0^{2\pi} f'(x)\left(\int \cos x\,dx\right)dx \\ &= -\int_0^{2\pi} f'(x)\sin x\,dx. \quad (*)\end{aligned}$$

(Integrating by parts again)

$$\begin{aligned}\int_0^{2\pi} f(x)\cos x\,dx &= -\left[f'(x)\int \sin x\,dx\right]_0^{2\pi} + \int_0^{2\pi} f''(x)\left(\int \sin x\,dx\right)dx \\ &= f'(2\pi) - f'(0) - \int_0^{2\pi} f''(x)\cos x\,dx \\ &= \int_0^{2\pi} f''(x)\,dx - \int_0^{2\pi} f''(x)\cos x\,dx.\end{aligned}$$

In the last step we could use Fundamental Theorem of Calculus since f'' is continuous (and hence integrable). Now observe that

$$\cos x \le 1 \implies f''(x)\cos x \le f''(x) \implies \int_0^{2\pi} f''(x)\cos x\,dx \le \int_0^{2\pi} f''(x)\,dx.$$

This gives us the desired inequality. $\square$

Why is the continuity of f'' crucial in the above solution? Because otherwise we cannot use

$$\int_a^b g'(x)\,dx = g(b) - g(a)$$

with $g = f'$. By blindly using the above formula one may end up into horribly wrong results, such as:

$$\int_{-1}^{1} \frac{1}{x^2}\,dx = -2.$$

(This is wrong, since integral of a positive function cannot be negative! By the way, can you give a correct evaluation of this integral?)

It turns out that here one can also give an alternate solution that does not rely upon the continuity of f''. We can write from $*$ that

$$\int_0^{2\pi} f(x)\cos x\,dx = -\int_0^{2\pi} f'(x)\sin x\,dx = -\int_\pi^{2\pi} f'(x)\sin x\,dx - \int_0^{\pi} f'(x)\sin x\,dx.$$

Now, substitute $x = y + \pi$ in the first integral above, to arrive at

$$\begin{aligned}\int_0^{2\pi} f(x)\cos x\,dx &= -\int_0^{\pi} f'(y+\pi)\sin(y+\pi)\,dy - \int_0^{\pi} f'(x)\sin x\,dx\\ &= \int_0^{\pi} f'(y+\pi)\sin y\,dy - \int_0^{\pi} f'(x)\sin x\,dx\\ &= \int_0^{\pi} \big(f'(x+\pi) - f'(x)\big)\sin x\,dx \geq 0.\\ &\geq 0 \quad \text{since } f'' \geq 0.\end{aligned}$$

This completes the proof. $\square$

Problem 2.3. Suppose that $f : [0,1] \to \mathbb{R}$ is a continuous function satisfying $xf(y) + yf(x) \leq 1$ for every $x, y \in [0,1]$. Show that

$$\int_0^1 f(x)\,dx \leq \pi/4. \quad (2)$$

Find a function satisfying the given condition for which equality is attained here.

Solution. Substituting $x = \sin\theta$ in the integral, and using $\int_0^a f(x)\,dx = \int_0^a f(a-x)\,dx$, we obtain

$$\begin{aligned}\int_0^1 f(x)\,dx &= \int_0^{\pi/2} f(\sin\theta)\cos\theta\,d\theta\\ &= \int_0^{\pi/2} f\left(\sin\left(\frac{\pi}{2}-\theta\right)\right)\cos\left(\frac{\pi}{2}-\theta\right)\,d\theta = \int_0^{\pi/2} f(\cos\theta)\sin\theta\,d\theta.\end{aligned}$$

Adding up these two expressions for the same integral,

$$2\int_0^1 f(x)\,dx = \int_0^{\pi/2} \left(f(\sin\theta)\cos\theta + f(\cos\theta)\sin\theta\right)d\theta \leq \int_0^{\pi/2} 1\,d\theta = \frac{\pi}{2}$$

which gives the desired inequality (2). For equality to hold, it is sufficient to have

$$f(\sin\theta)\cos\theta + f(\cos\theta)\sin\theta = 1$$

which holds for $f(x) = \sqrt{1-x^2}$. How to check that this function does satisfy the given condition for all $x, y \in [0,1]$? Well, we can apply the Cauchy-Schwarz inequality to conclude that for any $0 \leq x, y \leq 1$,

$$xf(y) + yf(x) = x\sqrt{1-y^2} + y\sqrt{1-x^2} \leq \sqrt{(1-y^2+y^2)(x^2+1-x^2)} = 1.$$

This completes the proof that $f(x) = \sqrt{1-x^2}$ is indeed a function satisfying the given condition for which equality is attained in (2). $\square$

Problem 2.4. Suppose f is a differentiable function such that $f(f(x)) = x$ holds for all $x \in [0,1]$. Also, $f(0) = 1$. For any $n \in \mathbb{N}$, find the value of

$$\int_0^1 (x - f(x))^{2n}\, dx.$$

Solution. Since f is one-one and continuous, it must be monotone. And $f(0) = 1$ implies $f(1) = f(f(0)) = 0$. Therefore, f is monotonically decreasing and range of f is $[0,1]$. So we can apply the substitution formula, with $\phi = f$ (i.e. substituting $x = f(t)$) and get

$$\begin{aligned} I = \int_0^1 (x - f(x))^{2n}\, dx &= -\int_{f(1)}^{f(0)} (x - f(x))^{2n}\, dx \\ &= -\int_0^1 (f(t) - f(f(t)))^{2n} f'(t)\, dt. \end{aligned}$$

Next, using $f(f(t)) = t$, we can write the last integral as $\int_0^1 (f(t) - t)^{2n} f'(t)\, dt$. Therefore,

$$I = \int_0^1 (x - f(x))^{2n}\, dx = -\int_0^1 (f(x) - x)^{2n} f'(x)\, dx.$$

Adding up these two alternate expressions for I, we get

$$2I = \int_0^1 (f(x) - x)^{2n} \left(1 - f'(x)\right) dx.$$

Since this integrand is just the derivative of $\frac{(f(x)-x)^{2n+1}}{2n+1}$, we apply FTC to obtain

$$2I = \frac{1}{2n+1} (f(x) - x)^{2n+1} \Big|_{x=1}^{x=0} = \frac{2}{2n+1}$$

which implies that

$$\int_0^1 (x - f(x))^{2n}\, dx = \frac{1}{2n+1}.$$

(Ans.)

Problem 2.5. For $n = 1,2,3,4$, define $I_n = \int_0^{n\pi} \frac{\sin x}{1+x}\, dx$. Arrange I_1, I_2, I_3, I_4 in increasing order.

Solution. We can roughly sketch the graph of $y = \frac{\sin x}{1+x}$ and using it we can guess the ordering. (The actual graph is shown in Figure 1.)

Once we have guessed that the desired ordering is $I_1 > I_3 > I_4 > I_2$, it remains to show each of these inequalities one by one. First note that for any integer m,

$$\int_{m\pi}^{(m+1)\pi} \frac{\sin x}{1+x}\, dx = \int_0^\pi \frac{(-1)^m \sin y}{1 + y + m\pi}\, dy.$$

(This can be seen by substituting $y = x - m\pi$.) Hence,

$$I_4 - I_2 = \int_{3\pi}^{4\pi} \frac{\sin x}{1+x}\, dx + \int_{2\pi}^{3\pi} \frac{\sin x}{1+x}\, dx = \int_0^\pi \left(\frac{\sin y}{1 + 2\pi + y} - \frac{\sin y}{1 + 3\pi + y} \right) dy > 0.$$

In the last step, we used the fact that integral of a positive and continuous function is positive. Similarly,

$$I_3 - I_2 = \int_{2\pi}^{3\pi} \frac{\sin x}{1+x}\, dx + \int_{\pi}^{2\pi} \frac{\sin x}{1+x}\, dx = \int_0^\pi \left(\frac{\sin y}{1 + 2\pi + y} - \frac{\sin y}{1 + \pi + y} \right) dy < 0.$$

Finally,

$$I_3 - I_4 = -\int_{3\pi}^{4\pi} \frac{\sin x}{1+x}\, dx = \int_0^\pi \left(\frac{\sin y}{1 + 3\pi + y} - \frac{\sin y}{1 + 4\pi + y} \right) dy > 0.$$

18.5 Excercise 3

1. Evaluate the following limits:

(a) $\lim_{n\to\infty} \frac{1^k+2^k+\cdots+n^k}{n^{k+1}} \quad (k \in \mathbb{N})$

(b) $\lim_{n\to\infty} \frac{1}{n}\sqrt{(n+1)(n+2)\cdots(n+n)}$

(c) $\lim_{n\to\infty} n^2\left(\frac{1}{n^3+1^3}+\frac{1}{n^3+2^3}+\cdots+\frac{1}{n^3+n^3}\right)$

(d) $\lim_{n\to\infty} \frac{1}{n}\log\binom{2n}{n}$

2. Evaluate the following integrals:

(a) $\int_{1/e}^{e} |\log x|\,dx$

(b) $\int_0^{\pi/2} \frac{1}{1+\tan^2 x}\,dx$

(c) $\int_0^{\pi/4} \frac{\sin x}{\sin x+\cos x}\,dx$

(d) $\int_0^{\pi} \frac{x\sin x}{1+\cos^2 x}\,dx$

3. Suppose f is continuous on $[0,1]$. Prove that

$$\int_0^{\pi} xf(\sin x)\,dx = \pi\int_0^{\pi/2} f(\sin x)\,dx$$

Hence (or otherwise) calculate

$$\int_0^{\pi} \frac{x\sin^{2n} x}{\sin^{2n} x+\cos^{2n} x}\,dx.$$

4. Prove the following inequality

$$\int_0^{\pi} \frac{\sin nx}{x}\,dx \geq \frac{2}{\pi}\left(1+\frac{1}{2}+\cdots+\frac{1}{n}\right).$$

5. For every positive integer n, evaluate the integrals

(a) $\int_0^{\pi/2} \sin^n x\,dx$

(b) $\int_0^{\pi/2} \cos^n x\,dx$

(c) $\int_0^{\pi/4} \tan^{2n} x\,dx$

(d) $\int_0^{\pi/2} \frac{\sin(2n+1)x}{\sin x}\,dx$

6. For any $n \in \mathbb{N}$, evaluate the integral $\int_0^1 (1-x^2)^n dx$ and hence calculate the following sum

$$\sum_{k=0}^{\infty}\left(\frac{1}{1}\binom{n}{0}-\frac{1}{3}\binom{n}{1}+\frac{1}{5}\binom{n}{2}-\cdots+(-1)^n\frac{1}{2n+1}\binom{n}{n}\right).$$

7. Let $f:[1,\infty)\to\mathbb{R}$ be defined by $f(x)=\int_1^x \frac{\log t}{1+t}\,dt$. Find all $x\in\mathbb{R}$ that satisfies the equation

$$f(x)+f(1/x)=2.$$

8. Let f be continuous on $\mathbb{R}$. If $\int_{-a}^{a} f(x)\,dx = 0$ holds for every $a\in\mathbb{R}$, show that f must be an odd function.

9. Let $f:\mathbb{R}\to(0,\infty)$ be a continuously differentiable function which satisfies $f'(t)\geq\sqrt{f(t)}$ for all $t\in\mathbb{R}$. Show that for every $x\geq 1$,

$$f(x)\geq\sqrt{f(1)}+\frac{1}{2}(x-1).$$

10. Let $f : [1, \infty) \to \mathbb{R}$ be a function satisfying $f(1) = 1$, and

$$f'(x) = \frac{1}{x^2 + f(x)^2}$$

for every $x \geq 1$. Prove that $\lim_{x\to\infty} f(x)$ exists and this limit is less than $1 + \pi/4$.

11. Let $f(x) = x^3 - \frac{3}{2}x^2 + x + \frac{1}{4}$. For every $n \in \mathbb{N}$ let f^n denote f composed n-times, i.e.,

$$f^n(x) = f \circ f \circ \cdots \circ f(x).$$

Evaluate

$$\int_0^1 f^{2020}(x)\,dx.$$

12. Suppose that $f : [0, \infty) \to \mathbb{R}$ is continuous. Define $a_n = \int_0^1 f(x+n)\,dx$, for every $n \geq 0$. Suppose also that $\lim_{n\to\infty} a_n = a$. Find the limit

$$\lim_{n\to\infty} \int_0^1 f(nx)\,dx.$$

13. Let $f : [a, b] \to \mathbb{R}$ be a continuously differentiable function. Prove that,

$$\lim_{n\to\infty} \int_a^b f(x) \sin nx\,dx = 0.$$

18.6 Integration MCQ

1. If $[x]$ stands for the largest integer not exceeding x, then the integral $\int_{-1}^{2}[x]\,dx$ is

(A) 3; (B) 0; (C) 1; (D) 2.

2. For any real number x, let $[x]$ denote the greatest integer m such that $m \le x$. Then

$$\int_{-2}^{2}[x^2-1]\,dx$$

equals

(A) $2(3-\sqrt{3}-\sqrt{2})$; (B) $2(5-\sqrt{3}-\sqrt{2})$; (C) $2(1-\sqrt{3}-\sqrt{2})$; (D) none of these.

3. Let $f(x)$ be a continuous function such that its first two derivatives $f'(x), f''(x)$ are continuous. The tangents to the graph of $f(x)$ at the points with abscissa $x=a$ and $x=b$ make with the X-axis angles $\frac{\pi}{3}$ and $\frac{\pi}{4}$ respectively. Then the value of the integral $\int_a^b f'(x)f''(x)\,dx$ equals

(A) $1-\sqrt{3}$; (B) 0; (C) 1; (D) -1

4. The integral $\int_0^{100} e^{x-\lfloor x\rfloor}dx$ is

(A) $\frac{e^{100}-1}{100}$; (B) $e^{100}-1$; (C) $100(e-1)$; (D) $e^{-\frac{1}{100}}$.

5. If $S=\int_0^1 \frac{e^t}{t+1}dt$ then $\int_a^{a-1} \frac{e^t}{t+1}dt$ is

(A) Se^a; (B) Se^{-a}; (C) $-Se^{-a}$; (D) $-Se^a$.

6. If the value of the integral $\int_1^e e^{x^2}dx$ is α, then the value of $\int_e^{e^4}\sqrt{\log x}dx$ is

(A) $e^4-e-\alpha$; (B) $2e^4-e-\alpha$;

(C) $2(e^4-e)-\alpha$; (D) none of the foregoing quantities.

7. The value of the integral $\int_0^{\pi}|1+2\cos x|dx$ is

(A) $\frac{\pi}{3}+\sqrt{3}$; (B) $\frac{\pi}{3}+2\sqrt{3}$; (C) $\frac{\pi}{3}+4\sqrt{3}$; (D) $\frac{2\pi}{3}+4\sqrt{3}$.

8. The value of the integral $\int_0^{\pi}\sqrt{1+\sin\frac{x}{2}}dx$, where $0\le u\le \pi$, is

(A) $4+4(\sin\frac{u}{4}-\cos\frac{u}{4})$; (B) $4+4(\cos\frac{u}{4}-\sin\frac{u}{4})$;

(C) $4+\frac{1}{4}(\sin\frac{u}{4}-\cos\frac{u}{4})$; (D) $4+\frac{1}{4}(\sin\frac{u}{4}-\cos\frac{u}{4})$.

9. The definite integral $\int_0^{\pi/2}\frac{dx}{1+(\tan x)^{101}}$ equals

(A) π; (B) $\frac{\pi}{2}$; (C) 0; (D) $\frac{\pi}{4}$.

10. If $f(x)$ is a nonnegative continuous function such that $f(x)+f(\frac{1}{2}+x)=1$ for all $x, 0\le x\le\frac{1}{2}$, then $\int_0^1 f(x)dx$ is equal to

(A) $\frac{1}{2}$; (B) $\frac{1}{4}$; (C) 1; (D) 2.

11. The value of the integral $\int_0^{\pi/4} \log_e(1+\tan\theta)d\theta$ is

(A) $\frac{\pi}{8}$; (B) $\frac{\pi}{8}\log_e 2$; (C) 1; (D) $2\log_e 2 - 1$.

12. Define the real-valued function f on the set of real numbers by

$$f(x) = \int_0^x \frac{t^2+t^2}{2-t}dt.$$

Consider the curve $y = f(x)$. It represents

(A) a straight line; (B) a parabola; (C) a hyperbola; (D) an ellipse.

13. $\lim_{n\to\infty} \frac{1}{n}\sum_{r=0}^{n-1} \cos\left(\frac{\pi r}{2n}\right)$

(A) is 1; (B) is 0; (C) is $\frac{2}{\pi}$; (D) does not exist.

14. $\lim_{n\to\infty} \frac{\sqrt{1}+\sqrt{2}+\cdots+\sqrt{n}}{n\sqrt{n}}$ is equal to

(A) $\frac{1}{2}$; (B) $\frac{1}{3}$; (C) $\frac{2}{3}$; (D) 0.

15. The value of

$$\lim_{n\to\infty} \sum_{i=1}^{n} \frac{1}{n}\left\lfloor \sqrt{4i/n} \right\rfloor,$$

where $\lfloor x \rfloor$ is the largest integer smaller than or equal to x, is

(A) 3; (B) $\frac{3}{4}$; (C) $\frac{4}{3}$; (D) none of the foregoing numbers.

16. Let $\alpha = \lim_{n\to\infty} \frac{12^2+22^2+\cdots+n^2}{n^3}$ and $\beta = \lim_{n\to\infty} \frac{(1^3-1^2)+(2^3-2^2)+\cdots+(n^3-n^2)}{n^4}$. Then

(A) $\alpha = \beta$; (B) $\alpha < \beta$; (C) $4\alpha - 3\beta = 0$; (D) $3\alpha - 4\beta = 0$.

17. The value of the integral

$$\int_{-4}^{4} |x-3|dx$$

is

(A) 13; (B) 8; (C) 25; (D) 24.

18. The value of $\int_{-2}^{2} |x(x-1)|dx$ is

(A) $\frac{11}{3}$; (B) $\frac{13}{3}$; (C) $\frac{16}{3}$; (D) $\frac{17}{3}$.

19. $\int_{-1}^{3/2} |x \sin \pi x|dx$ is equal to

(A) $\frac{3\pi+1}{\pi^2}$; (B) $\frac{\pi+1}{\pi^2}$; (C) $\frac{1}{\pi^2}$; (D) $\frac{3\pi-1}{\pi^2}$.

20. The set of values of a for which the integral $\int_0^2 (|x-a| - |x-1|)dx$ is nonnegative, is

(A) all numbers $a \geq 1$; (B) all real numbers; (C) all numbers a with $0 \leq a \leq 2$; (D) all numbers $a \leq 1$.

ANSWER KEY

1	2	3	4	5	6	7	8	9	10
B	A	D	C	C	B	B	A	D	A
11	12	13	14	15	16	17	18	19	20
B	B	C	C	A	D	C	D	A	B

18.7 Some Harder Problems

Example 1: Let $f : \mathbb{R} \to \mathbb{R}$ be a continuous function such that for all $x \in \mathbb{R}$,

$$\int_0^1 f(xt)dt = 0.$$

Show that $f \equiv 0$.

Solution: We have, for any $x \neq 0$,

$$\int_0^1 f(x)dx = \int_0^x f(u)\frac{du}{x} = \frac{1}{x}\int_0^x f(u)du.$$

Hence

$$\int_0^x f(u)du = 0 \quad \text{for all } x \in \mathbb{R}.$$

This shows that

$$\frac{d}{dx}\int_0^x f(u)du = 0,$$

which shows that $f(x) = 0$ for all $x \in \mathbb{R}$.

Example 2: Let p, q be positive numbers. Prove that

$$\int_0^1 (1-x^p)^{1/q}dx = \int_0^1 (1-x^q)^{1/p}dx.$$

Solution: More generally, assume that f is a decreasing continuous function on $[a, b]$. Then its inverse function g exists in $[f(b), f(a)]$ and is also decreasing and continuous. Hence

$$\int_{f(b)}^{f(a)} g(y)dy = \int_a^b g(f(t))f'(t)dt = \int_b^a tf'(t)dt = af(a) - bf(b) + \int_a^b f(t)dt.$$

If additionally we have $f(a) = b$ and $f(b) = a$, then

$$\int_a^b g(t)dt = \int_b^a f(t)dt.$$

The functions $f(x) = (1-x^q)^{1/p}$ and $g(x) = (1-x^p)^{1/q}$ represent in $[0, 1]$ a special case of this situation.

Example 3: Let $f : [0, 1] \to [0, \infty)$ be a continuous function such that

$$f^2(t) \leq 1 + 2\int_0^t f(s)ds, \quad \forall t \in [0, 1].$$

Prove that $f(t) \leq 1 + t$, for all $t \in [0, 1]$.

Solution. Let

$$g(t) = 1 + 2\int_0^t f(s)ds.$$

Then $g'(t) = 2f(t) \le 2\sqrt{g(t)}$, so

$$\sqrt{g(t)} - 1 = \int_0^t \frac{g'(s)}{2\sqrt{g(s)}} ds \le \int_0^t ds = t.$$

Hence $f(t) \le \sqrt{g(t)} \le 1 + t$.

Example 4: Let $f : [1, \infty) \to \mathbb{R}$ be such that $f(1) = 1$ and

$$f'(x) = \frac{1}{x^2 + f^2(x)}.$$

Prove that $\lim_{x\to\infty} f(x)$ exists and this limit is less than $1 + \frac{\pi}{4}$.

Solution. Since $f' > 0$, our function f is increasing, so $f(t) > f(1) = 1$, $\forall t > 1$. Hence

$$f'(t) = \frac{1}{t^2 + f^2(t)} < \frac{1}{t^2 + 1}, \quad \forall t > 1.$$

It follows that

$$f(x) = 1 + \int_1^x f'(t)dt < 1 + \int_1^x \frac{1}{t^2+1} dt < 1 + \int_1^\infty \frac{1}{t^2+1} dt = 1 + \frac{\pi}{4}.$$

Thus, $\lim_{x\to\infty} f(x)$ exists and is at most $1 + \frac{\pi}{4}$. This inequality is strict because

$$\lim_{x\to\infty} f(x) = 1 + \int_1^\infty f'(t)dt < 1 + \int_1^\infty \frac{1}{t^2+1} dt = 1 + \frac{\pi}{4}.$$

---

1. Let $f:[0,1]\to\mathbb{R}$ be an integrable function such that

$$\int_0^1 f(x)dx = \int_0^1 xf(x)dx = 1.$$

Prove that $\int_0^1 f^2(x)dx \geq 4$.

2. Let $f:[0,1]\to\mathbb{R}$ be a continuous function with the property that $xf(y)+yf(x)\leq 1$, for all $x,y\in[0,1]$. Show that

$$\int_0^1 f(x)dx \leq \frac{\pi}{4}.$$

Find a function satisfying the condition for which there is equality.

3. Let $f:[0,1]\to(0,\infty)$ be a nonincreasing function. Prove that

$$\frac{\int_0^1 xf^2(x)\,dx}{\int_0^1 xf(x)\,dx} \leq \frac{\int_0^1 f^2(x)\,dx}{\int_0^1 f(x)\,dx}.$$

4. Evaluate the definite integral

$$\int_{-\pi}^{\pi} \frac{\sin nx}{(1+2^x)\sin x}\,dx,$$

where n is a natural number.

5. Let n be a positive integer. Compute

$$\int_0^{\pi} \frac{2+2\cos x-\cos(n-1)x-2\cos nx-\cos(n+1)x}{1-\cos 2x}\,dx.$$

6. Let $f,g:\mathbb{R}\to\mathbb{R}$ be continuous functions such that $f(x+1)=f(x)$ and $g(x+1)=g(x)$, for all $x\in\mathbb{R}$. Prove that

$$\lim_{n\to\infty}\int_0^1 f(x)g(nx)\,dx = \left(\int_0^1 f(x)\,dx\right)\left(\int_0^1 g(x)\,dx\right).$$

9. Let $f:[0,1]\to\mathbb{R}$ be a differentiable function such that

$$\sup_{x\in(0,1)}\left|f'(x)\right| = M < \infty.$$

Let n be a positive integer. Prove that

$$\left|\sum_{j=0}^{n-1}\frac{f(j/n)}{n} - \int_0^1 f(x)\,dx\right| \leq \frac{M}{2n}.$$

---

19 Combinatorics

You have already seen basic combinatorics problems in your daily life. For example "What is the number of ways you can do something" or "Shat is the number of ways of choosing something". These all involve the following counting principles which have an underlying set theoretic principle.

19.1 Basic Counting Principles

Addition Principle: Suppose you have a collection of disjoint sets $S_1, \cdots, S_k$ such that $S_i \cap S_j = \phi$. Then we can say that

$$\left|\bigcup_{i=1}^{k} S_i\right| = \sum_{i=1}^{k} |S_i|$$

But the question is how do we use this in a counting problem. Whenever we have an "or" logic we use the addition principle. Suppose we have three ways of travelling from A to B via road and 4 ways of travelling from A to B via air then what is the total number of ways of travelling from A to B?

The answer is easy. Its 8 right? This question is so natural that we don't even think the underlying principle. The idea is the total no of ways S is the union of the roadways S_1 and no of airways S_2 and hence $S = S_1 \cup S_2$ which is why the total number of ways $|S| = 8$. If you think about it the logic is an "or" logic as you can choose a road way "or" an airway.

Multiplication Principle: Suppose we have two sets S_1, S_2 and we look at the cartesian product of these sets

$$S_1 \times S_2 = \{(s_1, s_2) : s_1 \in S_1, s_2 \in S_2\}$$

Then we can say that $|S_1 \times S_2| = |S_1| \times |S_2|$ We use the multiplication principle whenever we have an "and" logic. For example we have the following route that you need to travel $A \to B \to C$ where there are three ways of travelling from $A \to B$ and two ways of travelling from $B \to C$ then the total number of ways of travelling from $A \to C$. This is because any route from $A \to C$ is an ordered pair (r_1, r_2) where r_1 is one route from $A \to B$ and r_2 is some route from B to C hence we are looking from the cartesian product which has a size 6 in this case.

Example 1: Find the number of 2-digit numbers which are even and have different digits.

Solution: Since the number $10x + y$ is to be even, its units digit y must be even: 0, 2, 4, 6, 8. So, y can be chosen in 5 ways. Also, the tens digit x must be non-zero and different from the units digit. Hence we have 2 mutually exclusive cases: (a) Let $y = 0$. Then x can be chosen in 9 ways. This gives 9 numbers. (b) Let y be non-zero. Then y can be chosen in 4 ways and x can be chosen in 8 ways. This gives, by the multiplication principle, $4 \times 8 = 32$. Hence, by the addition principle, the total number of required numbers is $9 + 32 = 41$. Note that if we *first* choose x from $\{1, 2, \ldots, 9\}$, then we have to proceed differently. In fact, we then have the following 2 mutually exclusive cases: (i) x odd (ii) x even. In case (i), x can be chosen in 5 ways and y in 5 ways giving in all $5 \times 5 = 25$ numbers and in case (ii), x can be chosen in 4 ways and y in 4 ways giving in all $4 \times 4 = 16$ numbers. Hence, by the addition principle, the total number of required numbers is again $25 + 16 = 41$.

Example 2: Let $X = \{1, 2, \ldots, 100\}$ and let

$$S = \{(a, b, c) \mid a, b, c \in X, a < b \text{ and } a < c\}.$$

Find $|S|$.

Solution. The problem may be divided into disjoint cases by considering $a = 1, 2, \ldots, 99$.

For $a = k \in \{1, 2, \ldots, 99\}$, the number of choices for b is $100 - k$ and that for c is also $100 - k$. Thus the number of required ordered triples (k, b, c) is $(100 - k)^2$, by (MP). Since k takes on the values 1, 2, ..., 99, by applying (AP), we have

$$|S| = 99^2 + 98^2 + \cdots + 1^2.$$

Using the formula $\sum_{k=1}^{n} k^2 = \frac{1}{6}n(n+1)(2n+1)$, we finally obtain

$$|S| = \frac{1}{6} \times 99 \times 100 \times 199 = 328350.$$

Principle of Inclusion and Exclusion

Bijection Principle : If two finite sets S and T can be put into one-to-one correspondence with each other, then they contain the same number of elements, i.e. $|S| = |T|$. So a natural question is when do we use this? What happens is that sometimes some "Scenario" or some "Counting Principle" is difficult to count so what we do is show is that there is a bijection from "Scenario" say S_1 to another "Scenario" S_2 which is slightly easier to count.

For example we want to count the number of n-length binary strings. Now what is a n-length binary string? It a string of length n

$$S = a_1 a_2 \cdots a_n \text{ where } a_i \in \{0, 1\}$$

Now even though this a pretty simple problem let us illustrate the Bijection Principle. Suppose we consider a set $S = \{x_1, \cdots, x_n\}$ and consider subsets $X \subseteq S$. Now since the set S has n elements, whenever we look at a subset $X_i \subseteq S$, we will a binary string $s_i = a_1 \cdots a_n$ according to this following rule

$$a_i = \begin{cases} 0 & x_i \notin X_i \\ 1 & x_i \in X_i \end{cases}$$

It is easy to see that this gives us a n-length binary string and corresponding to every subset we get an unique binary string. Hence there is a bijection. Thus the no of n-length binary string should be the same as the no of subsets of a set of size n which is 2^n.

Example 3: There are 7 boys and 3 girls in a gathering. In how many ways can they be arranged in a row so that

1. the 3 girls form a single block (i.e. there is no boy between any two of the girls)?
2. the two end-positions are occupied by boys and no girls are adjacent?

Solution.

(i) Since the 3 girls must be together, we can treat them as a single entity. The number of ways to arrange 7 boys together with this entity is $(7 + 1)!$. As the girls can permute among themselves within the entity in 3! ways, the desired number of ways is, by the multiplication principle (MP),

$$8! \times 3!.$$

(ii) We first consider the arrangements of boys and then those of girls. There are 7! ways to arrange the boys. Fix an arbitrary one of the arrangements. Since the end-positions are occupied by boys, there are only 6 spaces available for the 3 girls G_1, G_2 and G_3.

G_1 has 6 choices. Since no two girls are adjacent, G_2 has 5 choices and G_3 has 4. Thus by (MP), the number of such arrangements is

$$7! \times 6 \times 5 \times 4.$$

19.2 Exercise 1.1

1. A new club flag is to be designed with 6 vertical stripes using some or all of the colours yellow, green, blue, and red. In how many ways can this be done so that no two adjacent stripes have the same colour?

2. - How many different five-digit numbers are there (leading zeros, e.g., 00144, not allowed)?
   - How many even 5-digit numbers are there?
   - How many 5-digit numbers are there with exactly one 3?
   - How many 5-digit numbers are there that are the same when the order of their digits is inverted (e.g., 14341)?

3. How many times is the digit 0 written when listing all numbers from 1 to 3333?

4. How many times is the digit 5 written when listing all numbers from 1 to 10^5?

5. How many non-empty collections of letters can be formed from three A's and five B's?

6. Show that the number of ways of making a non-empty collection by choosing some or all of $n_1 + n_2 + \cdots + n_k$ objects where n_1 are alike of one kind, n_2 alike of a second kind, ..., n_k alike of a kth kind, is

$$(n_1 + 1)(n_2 + 1) \cdots (n_k + 1) - 1.$$

7. Show that the total number of subsets of a set S with n elements is 2^n.

8. How many positive integers are factors of 30030?

9. Let $A = \{1, 2, \ldots, m\}$ and $B = \{1, 2, \ldots, n\}$ where m, n are positive integers. How many functions are there from A to B? How many one-to-one functions are there from A to B?

10. $A = \{a_1, a_2, a_3, \ldots, a_n\}$ and $B = \{b_1, b_2\}$. Find the number of onto functions that can be defined from A to B.

19.3 Permutation and Combinations

Now we talk about two scenarios, one where we just choose some objects from a set and the second case when we choose and then arrange the objects.

For example we can talk about having a set of 5 people from which we have to choose 3 people and then these people stand in some line. So as you can see in this case both the choice of the people and the way they stand in the line matters. These are known as Permutations.

On the other hand suppose I have 6 subjects that I need to study and on a particular day I decide I am going to study only 3 subjects and then at the end of the day I ask which are the subjects I covered the ordering in which I studied those subjects doesn't matter. What matters is the ones I studied so in this case only the choice matters and not the order. These are known as combinations. Let us now define them formally

Theorem 1. The number of r-permutations of a set S containing n different objects is denoted by $P(n,r)$ or ${}^nP_r$ and is given by

$$ {}^nP_r = n(n-1)(n-2)\cdots(n-r+1) = \frac{n!}{(n-r)!}. $$

By an r-combination of a set $S = \{1, 2, \ldots, n\}$, we mean an unordered selection of r of the n elements of S.

Theorem 2. The number of r-combinations of an n-element set is denoted by $\binom{n}{r}$ or ${}^nC_r$ or $C(n,r)$ and is given by

$$ {}^nC_r = \frac{n!}{r!(n-r)!}. $$

Theorem 3 (Binomial Theorem). For every positive integer n, we have

$$ (x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} $$

Proof: To evaluate the product

$$ (x+y)^n = (x+y)(x+y)\cdots(x+y) \quad \text{[n factors]} $$

we have to add the 2^n monomials obtained thus: a monomial is formed by choosing one term from each factor and multiplying them together. Now if we choose y from r of the factors and x from the remaining $n-r$ factors, then we get the monomial $x^{n-r}y^r$. Here r takes values from 0 to n to account for all possible monomials. But r of the n factors (from which we take y) can be chosen in $\binom{n}{r}$ ways. Hence the monomial $x^{n-r}y^r$ occurs $\binom{n}{r}$ times. Therefore the simplified expansion of the above product is given by

$$ (x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \cdots + \binom{n}{r}x^{n-r}y^r + \cdots + \binom{n}{n}y^n. $$

Theorem 4. For any positive integers n, r $(r \le n)$, we have

(a) $\binom{n}{r} = \binom{n}{n-r}$, if $0 \le r \le n$.

(b) $\binom{n}{r} + \binom{n}{r-1} = \binom{n+1}{r}$, if $1 \le r \le n$.

(c) $\binom{n}{r} = \frac{n}{r} \times \binom{n-1}{r-1}$, if $1 \le r \le n$.

(d) $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$.

(e) $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots = 2^{n-1}$.

(f) $\sum_{r=0}^{k} \binom{n}{r}\binom{m}{k-r} = \binom{m+n}{k}$.

(g) $\binom{n}{k}\binom{k}{m} = \binom{n}{m}\binom{n-m}{k-m}$.

Example 4: Evaluate
$$\binom{n}{0}+\binom{n}{3}+\binom{n}{6}+\cdots$$

Solution: We note that
$$(1+x)^n=\binom{n}{0}+\binom{n}{1}x+\binom{n}{2}x^2+\cdots+\binom{n}{n}x^n.$$

Put $x=1$,
$$2^n=\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{n}.$$

Put $x=\omega=\frac{-1+i\sqrt{3}}{2}$,
$$(1+\omega)^n=\binom{n}{0}+\binom{n}{1}\omega+\binom{n}{2}\omega^2+\cdots$$

Put $x=\omega^2=\frac{-1-i\sqrt{3}}{2}$,
$$(1+\omega^2)^n=\binom{n}{0}+\binom{n}{1}\omega^2+\binom{n}{2}(\omega^2)^2+\cdots$$

Adding the equations for $x=1,\omega,\omega^2$, we get,
$$2^n+(1+\omega)^n+(1+\omega^2)^n=3\left[\binom{n}{0}+\binom{n}{3}+\binom{n}{6}+\cdots\right]$$

using $1+\omega+\omega^2=0$. But
$$1+\omega=-\omega^2=\frac{1+i\sqrt{3}}{2}=\cos 60^\circ+i\sin 60^\circ,\quad\text{and}$$
$$1+\omega^2=-\omega=\frac{1-i\sqrt{3}}{2}=\cos 60^\circ-i\sin 60^\circ.$$

Hence
$$2^n+(1+\omega)^n+(1+\omega^2)^n=2^n+(\cos 60^\circ+i\sin 60^\circ)^n+(\cos 60^\circ-i\sin 60^\circ)^n=2^n+2\cos(n\cdot 60^\circ)$$

But $\cos(n\cdot 60^\circ)=\begin{cases}1 & \text{if } n=6k,\\ \frac{1}{2} & \text{if } n=6k\pm 1,\\ -\frac{1}{2} & \text{if } n=6k\pm 2,\\ -1 & \text{if } n=6k+3.\end{cases}$

This gives
$$\binom{n}{0}+\binom{n}{3}+\binom{n}{6}+\cdots=\begin{cases}\frac{2^n+2}{3} & \text{if } n=6k,\\ \frac{2^n+1}{3} & \text{if } n=6k\pm 1,\\ \frac{2^n-1}{3} & \text{if } n=6k\pm 2.\end{cases}$$

Example 5: In a group of 15 boys, there are 7 scout-boys. In how many ways can 12 boys be selected so as to include (i) exactly 6 scout-boys (ii) at least 6 scout-boys?

Solution.

(i) (a) 6 scout-boys out of 7 can be chosen in $\binom{7}{6}$ ways and (b) 6 other boys out of 8 others can be chosen in $\binom{8}{6}$ ways. Now any 6-combination from (a) can be combined with any 6-combination from (b) to make a required type of group of 12 boys. So, by MP, the total number of ways is $\binom{7}{6}\times\binom{8}{6}=196$.

(ii) The 12-combination can include either 6 or 7 scout-boys. As in (i), there are $\binom{7}{6}\times\binom{8}{6}$ 12-combinations with exactly 6 scout-boys. Also, if we include all the 7 scout-boys, then the remaining 5 boys can be chosen from the other 8 boys in $\binom{8}{5}$ ways. So there are $\binom{8}{5}$ 12-combinations with exactly 7 scout-boys. Hence, by AP, the total number of ways is $\binom{7}{6}\times\binom{8}{6}+\binom{8}{5}$.

Circular permutations

By a *circular permutation* of the set $S = \{1, 2, \ldots, n\}$, we mean an ordered arrangement of the n elements of S around a circle.

Theorem 5: The number of circular permutations of n different objects is $(n-1)!$.

Complement Principle: Sometimes it is easier to count the complement of the scenario. In this case what we do is we count the complement and the total and then their difference is the required number of ways.

$$|S| = |U| - |S^c|$$

Example 6: In how many ways can 5 boys and 3 girls be seated around a table if

1. there is no restriction?
2. boy B_1 and girl G_1 are not adjacent?
3. no girls are adjacent?

Solution

(i) The number of ways is $Q_8^8 = 7!$.

(ii) The 5 boys and 2 girls not including G_1 can be seated in $(7-1)!$ ways. Given such an arrangement , G_1 has 5(= 7 - 2) choices for a seat not adjacent to B_1. Thus the desired number of ways is

$$6! \times 5 = 3600.$$

Now, the number of ways to arrange the 5 boys and 3 girls around a table so that boy B_1 and girl G_1 are adjacent (treating $\{B_1, G_1\}$ as an entity) is

$$(7-1)! \times 2 = 1440.$$

Thus the desired number of ways is by (CP),

$$7! - 1440 = 3600.$$

(iii) We first seat the 5 boys around the table in $(5-1)!$ ways. Given such an arrangement, there are 5 ways to seat girl G_1. As no girls are adjacent, G_2 and G_3 have 4 and 3 choices respectively. Thus the desired number of ways is

$$4! \times 5 \times 4 \times 3 = 1440.$$

Example 7: In how many ways can a committee of 5 be formed from a group of 11 people consisting of 4 teachers and 7 students if

1. there is no restriction in the selection?
2. the committee must include exactly 2 teachers?
3. the committee must include at least 3 teachers?
4. a particular teacher and a particular student cannot be both in the committee?

Solution:

1. The number of ways is $\binom{11}{5} = \frac{11!}{5!6!} = 462$.
2. We first select 2 teachers from 4 and then $5-2$ students from 7. The number of ways is

$$\binom{4}{2}\binom{7}{3} = 6 \times 35 = 210.$$

3. There are two cases: either 3 teachers or 4 teachers are in the committee. In the former case, the number of ways is
$$\binom{4}{3}\binom{7}{2} = 4 \times 21 = 84,$$
while in the latter, the number of ways is
$$\binom{4}{4}\binom{7}{1} = 7.$$
Thus by (AP), the desired number of ways is $84 + 7 = 91$.

4. Let T be the particular teacher and S the particular student. We first find the number of ways to form a committee of 5 which includes both T and S. Evidently, such a committee of 5 can be formed by taking the union of $\{T, S\}$ and a subset of 3 from the remaining 9 people. Thus the number of ways to form a committee of 5 including T and S is $\binom{9}{3} = 84$.

   Hence the number of ways to form a committee of 5 which does not include both T and S is by (CP):
$$\binom{11}{5} - \binom{9}{3} = 462 - 84 = 378, \quad \text{by (i)}.$$

Example 8 (IMO, 1989/3) Let n and k be positive integers and let S be a set of n points in the plane such that

(i) no three points of S are collinear, and

(ii) for any point P of S, there are at least k points of S equidistant from P.

Prove that $k < \frac{1}{2} + \sqrt{2n}$.

Solution: For convenience, we call a line segment in the plane an *edge* if it joins up any two points in S. Let ℓ be the number of edges in the plane. We shall consider the quantity ℓ.

First, since there are n distinct points in S and any two of them determine an edge, we have,
$$\ell = \binom{n}{2}. \tag{1}$$

Next, for each point P of S, by condition (ii), one can draw a circle with centre P whose circumference $C(P)$ contains at least $\binom{k}{2}$ edges. As there are n points P in S, the total number of these edges, counted with repetition, is at least $n\binom{k}{2}$.

Now, let us look at those edges which are counted more than once. An edge is counted more than once when and only when it is a common chord of at least 2 circles. Since two circles can have at most one common chord and there are n such circles, the number of common chords, counted with repetition, is at most $\binom{n}{2}$. Thus,
$$\ell \geq n\left(\binom{k}{2} - \binom{n}{2}\right). \tag{2}$$

Combining (1) with (2), we have
$$n\left(\binom{k}{2} - \binom{n}{2}\right) \leq \binom{n}{2}$$
or
$$n\binom{k}{2} \leq 2\binom{n}{2},$$
which implies that
$$k^2 - k - 2(n-1) \leq 0.$$

Hence,

$$k \le \frac{1+\sqrt{1+8(n-1)}}{2} < \frac{1}{2} + \frac{1}{2}\sqrt{8n} = \frac{1}{2} + \sqrt{2n},$$

as required.

Example 9: In how many ways can 6 people be seated

1. around two tables?
2. around three tables?

(We assume that the tables are indistinguishable.)

Solution.

1. For 2 tables, there are 3 cases to consider according to the numbers of people to be seated around the 2 respective tables, namely,

   - $5+1$
   - $4+2$
   - $3+3$

   Case (1). There are $\binom{6}{5}$ ways to divide the 6 people into 2 groups of sizes 5 and 1 each. By formula (1.3.2), the 5 people chosen can be seated around a table in $(5-1)!$ ways and the 1 chosen in $0!$ way around the other. Thus by (MP), the number of ways in this case is

   $$\binom{6}{5} \times 4! \times 0! = 144.$$

   Case (2). There are $\binom{6}{4}$ ways to divide the 6 people into 2 groups of size 4 and 2 each. Thus, again, the number of ways in this case is

   $$\binom{6}{4} \times 3! \times 1! = 90.$$

   Case (3). We have to be careful in this case. The number of ways to divide the 6 people into 2 groups of size 3 each is $\frac{1}{2}\binom{6}{3}$ (why?). Thus the number of arrangements is

   $$\frac{1}{2}\binom{6}{3} \times 2! \times 2! = 40.$$

   Hence by (AP), the desired number of arrangements is $144 + 90 + 40 = 274$.

2. For 3 tables, there are also 3 cases to consider depending on the number of people distributed to the 3 respective tables, namely,

   - $4+1+1$
   - $3+2+1$
   - $2+2+2$

   The number of arrangements in these cases are given below:

   - $\frac{1}{2}\binom{6}{4}\binom{2}{1} \times 3! \times 0! \times 0! = 90$;
   - $\binom{6}{3}\binom{3}{2} \times 2! \times 1! = 120$;
   - $\frac{1}{3!}\binom{6}{2}\binom{4}{2} \times 1! \times 1! \times 1! = 15$.

   Hence by (AP), the desired number of arrangements is $90 + 120 + 15 = 225$.

19.4 Exercise 1.2

1. How many ways can 12 identical white and 12 identical black pawns be placed on the black squares of an 8×8 chessboard?
2. How many ways are there to place 2 identical rooks in a common row or column of an 8×8 chessboard?
3. How many ways are there to place 2 identical kings on an 8×8 chessboard so that the kings are not in adjacent squares? On an $n \times m$ chessboard?
4. How many necklaces can be made using 7 beads of which 5 are identical red beads and 2 are identical blue beads?
5. There are 12 members in a committee who sit around a table. There is one place specially designated for the chairman. Besides the chairman, there are 3 people who constitute a subcommittee. Find the number of seating arrangements if
   - the subcommittee sit together as a block, and
   - no two of the subcommittee sit next to each other.
6. Prove that the number of ways of arranging p 1's and q 0's in a line such that no two 1's are adjacent is
$$\binom{q+1}{p}.$$
7. Prove that the number of r-subsets of the set $S = \{1, 2, \ldots, n\}$ that do not contain a pair of consecutive integers is
$$\binom{n-r+1}{r}.$$

19.5 Permutation with Repetitions

Theorem 6: Suppose there are n objects, of which n_1 are identical of first type, n_2 are identical of second type, $\ldots$, n_k are identical of k-th type so that $n = n_1 + n_2 + \cdots + n_k$. Then the number of permutations of these n objects, taken all at a time, is denoted by $P(n; n_1, n_2, \ldots, n_k)$ and is given by

$$P(n; n_1, n_2, \ldots, n_k) = \frac{n!}{n_1! n_2! \cdots n_k!}.$$

Theorem 6: Let S be a set having n different objects. Then the number of r-combinations of S, with repetitions allowed, is

$$\binom{n-1+r}{r}.$$

Corollary 1: Let n, r be given positive integers. Then the number $A_{n,r}$ of non-negative integer solutions $(x_1, x_2, \ldots, x_n)$ of the equation

$$x_1 + x_2 + \cdots + x_n = r,$$

is

$$\binom{n-1+r}{r}.$$

Proof: Let $S = \{a_1, \ldots, a_n\}$ be a set with n distinct elements. Given any r-combination t of S, with repetitions allowed, (say, $t = a_2a_2a_2a_5a_7$, $n = 7, r = 5$) let x_i be the number of times a_i occurs in t. Then t corresponds to the solution $(x_1, x_2, \ldots, x_n)$ of equation (1) in non-negative integers. (Thus the above 5-combination $t = a_2a_2a_2a_5a_7$ corresponds to the solution $(0, 3, 0, 0, 1, 0, 1)$ of the equation $x_1 + x_2 + \cdots + x_7 = 5$).

Conversely, every non-negative integer solution of (1) corresponds to a unique r-combination of S, with repetitions allowed. Hence, by the above theorem,

$$A_{n,r} = \binom{n-1+r}{r}.$$

Corollary 2: Let $r \geq n > 0$ be integers. The number $B_{n,r}$ of solutions $(x_1, x_2, \ldots, x_n)$ of equation (1) in positive integers is

$$\binom{r-1}{n-1}.$$

Proof : Given any solution $(y_1, \ldots, y_n)$ of (1) in positive integers, let $x_i = y_i - 1$. Then substituting in (1), we get

$$x_1 + \cdots + x_n = y_1 + \cdots + y_n - n = r - n,$$

so that $(x_1, x_2, \ldots, x_n)$ is a non-negative integer solution of (2). Conversely, every non-negative integer solution of (2) corresponds to a unique positive integer solution $(y_1, \ldots, y_n)$ of (1) with $y_i = x_i + 1$. Hence,

$$B_{n,r} = \binom{n-1+r-n}{r-n} = \binom{r-1}{n-1}.$$

Corollary 3: Let $r, n > 0$ be integers. Let $a_1, \ldots, a_n$ be given integers. Then the number of integer solutions of equation (1) such that $x_i > a_i$, $1 \leq i \leq n$, is

$$\binom{r - a_1 - \cdots - a_n - 1}{n-1}.$$

Proof : Given any solution $(y_1, \ldots, y_n)$ of (1) in integers, such that $y_i > a_i$, $1 \leq i \leq n$, so that $y_1 + \cdots + y_n = r$. Let $x_i = y_i - a_i$. Then substituting for y's we get

$$x_1 + \cdots + x_n = r - (a_1 + \cdots + a_n),$$

so that $(x_1, x_2, \ldots, x_n)$ is a positive integer solution of the last equation conversely. So, the number of required solutions is $\binom{r-a_1-\cdots-a_n-1}{n-1}$.

Example 10: If n identical dice are rolled, how many different outcomes can be recorded?

Solution: Since the dice are identical, the order in which the n scores appear is not important. So we want the number of n-combinations, with repetition, of the set $\{1, 2, 3, 4, 5, 6\}$ and it is

$$\binom{6-1+n}{n}.$$

Example 11: Given integers 1, 2, ..., 11, two groups (not necessarily disjoint) are selected; the first group contains 5 integers and the second group contains 2 integers. In how many ways, allowing repetitions, can the selection be made if

(i) there are no further conditions?

(ii) each group contains either all odd integers or all even integers?

Solution:

(i) The first group G_1 of 5 integers from the 11 integers can be chosen in

$$\binom{11-1+5}{5} = \binom{15}{5}$$

ways. Similarly, the group G_2 of 2 integers from the 11 integers can be chosen in

$$\binom{11-1+2}{2} = \binom{12}{2}$$

ways. Therefore the two groups G_1 and G_2 can be chosen in

$$\binom{15}{5} \times \binom{12}{2}$$

ways.

(ii) We have 4 mutually exclusive cases:

(a) G_1 all odd, G_2 all odd

(b) G_1 all odd, G_2 all even

(c) G_1 all even, G_2 all odd

(d) G_1 all even, G_2 all even

Hence the total number of ways is

$$\binom{10}{5}\binom{6}{2} + \binom{10}{5}\binom{7}{2} + \binom{9}{5}\binom{7}{2} + \binom{9}{5}\binom{6}{2}.$$

Example 12: Find the number of integer solutions of $x_1 + x_2 + x_3 + x_4 = 48$ with the conditions $x_1 > 5$, $x_2 > 6$, $x_3 > 7$, $x_4 > 8$.

Solution: If $y_1, \ldots, y_4$ is a solution of the required type, put $x_1 = y_1 - 5$, $x_2 = y_2 - 6$, $x_3 = y_3 - 7$ and $x_4 = y_4 - 8$. Then $y_1 + \cdots + y_4 = 48$ becomes $x_1 + \cdots + x_4 = 48 - 26 = 22$ and we want positive integer solutions. So the number of solutions is

$$\binom{22-1}{4-1}.$$

19.6 Some Harder Problems

Example 1: Let $S = \{1, 2, \ldots, n\}$ and let T be the set of all ordered triples of subsets of S, say (A_1, A_2, A_3), such that $A_1 \cup A_2 \cup A_3 = S$. Determine, in terms of n,

$$\sum_{(A_1,A_2,A_3)\in T} |A_1 \cap A_2 \cap A_3|$$

where $|X|$ denotes the number of elements in the set X. (For example, if $S = \{1, 2, 3\}$ and $A_1 = \{1, 2\}, A_2 = \{2, 3\}, A_3 = \{3\}$ then one of the elements of T is $(\{1, 2\}, \{2, 3\}, \{3\})$.

Solution: Let $X = (A_1, A_2, A_3) \in T$ and let $i \in A_1 \cap A_2 \cap A_3$. The number of times the element i occurs in the required sum is equal to the number of ordered tuples $(A_1 - \{i\}, A_2 - \{i\}, A_3 - \{i\})$ such that

$$A_1 - \{i\} \cup A_2 - \{i\} \cup A_3 - \{i\} = S - \{i\} \quad (*)$$

For every element of $S - \{i\}$, there are eight possibilities - whether the element belongs to or does not belong to A_i for $i = 1, 2, 3$. Out of these, the case when the element does not belong to any of the three subsets violates $(*)$. Therefore, each element can satisfy the requirement in 7 ways. The number of tuples is, therefore, 7^{n-1} and the sum is $n \cdot 7^{n-1}$.

Example 2: All the squares of a 2024×2024 board are coloured white. In one move, Mohit can select one row or column whose every square is white, choose exactly 1000 squares in this row or column, and colour all of them red. Find the maximum number of squares that Mohit can colour red in a finite number of moves.

Solution: Let $n = 2024$ and $k = 1000$. We claim that the maximum number of squares that can be coloured in this way is $k(2n - k)$, which evaluates to 3048000.

Indeed, call a row/column *bad* if it has at least one red square. After the first move, there are exactly $k + 1$ bad rows and columns: if a row was picked, then that row and the k columns corresponding to the chosen squares are all bad. Any subsequent move increases the number of bad rows/columns by at least 1. Since there are only $2n$ rows and columns, we can make at most $2n - (k + 1)$ moves after the first one, and so at most $2n - k$ moves can be made in total. Thus we can have at most $k(2n - k)$ red squares.

To prove this is achievable, let's choose each of the n columns in the first n moves, and colour the top k cells in these columns. Then, the bottom $n - k$ rows are still uncoloured, so we can make $n - k$ more moves, colouring $k(n + n - k)$ cells in total.

Example 3: Suppose 100 points in the plane are coloured using two colours, red and white, such that each red point is the centre of a circle passing through at least three white points. What is the least possible number of white points?

Solution: Let n be the number of white points. Then we can draw at most $\binom{n}{3}$ circles. Thus the number of white and red points together is at most $n + \binom{n}{3}$. We observe that

$$9 + \binom{9}{3} = 93, \quad 10 + \binom{10}{3} = 130.$$

Thus $n \geq 10$. We show that $n = 10$ works.

Take any 10 points such that no three are collinear and no four are concyclic. Then we get $\binom{10}{3} = 120$ points as centres of distinct circles. Among these, there may be some points from the original 10 points. Even if we leave out these 10 points, we have at least 110 points which are centres of circles formed by the ten points we have chosen. Choose any 90 points from them and colour them red and colour the original 10 points white. We get 100 points of which 10 are white and remaining 90 are red. Each of these 90 red points is the centre of a circle passing through some three white points.

Example 4: Consider n^2 unit squares in the xy-plane centred at point (i, j) with integer coordinates, $1 \leq i \leq n, 1 \leq j \leq n$. It is required to colour each unit square in such a way that whenever $1 \leq i < j \leq n$ and

$1 \leq k < l \leq n$, the three squares with centres at $(i,k),(j,k),(j,l)$ have distinct colours. What is the least possible number of colours needed?

Solution: We first show that at least $2n-1$ colours are needed. Observe that squares with centres (i,i) must all have different colours for $1 \leq i \leq n$; let us call them $C_1, C_2, \ldots, C_n$. Besides, the squares with centres (n,j), for $2 \leq j \leq n$ must have different colours and these must be different from $C_1, C_2, \ldots, C_n$. Thus we need at least $n + (n-1) = 2n-1$ colours. The following diagram shows that $2n-1$ colours will suffice.

n	$n+1$	$n+2$		$2n-2$	$2n-1$
$n-1$	n	$n+1$		$2n-3$	$2n-2$

3	4	5		$n+1$	$n+2$
2	3	4		n	$n+1$
1	2	3		$n-1$	n

Example 5: Find the number of all 6-digit natural numbers having exactly three odd digits and three even digits.

Solution: First we choose 3 places for even digits. This can be done in $\binom{6}{3} = 20$ ways. Observe that the other places for odd digits get automatically fixed. There are 5 even digits and 5 odd digits. Any of these can occur in their proper places. Hence there are 5^6 ways of selecting 3 even and 3 odd digits for a particular selection of place for even digits. Hence we get 20×5^6 such numbers. But this includes all those numbers having the first digit equal to 0. Since we are looking for 6-digit numbers, these numbers have to be removed from our counting. If we fix 0 as the first digit, we have 2 places for even numbers and 3 places for odd numbers. We can choose 2 places for even numbers in $\binom{5}{2} = 10$ ways. As earlier, for any such choice of places for even digits, we can choose even digits in 5^2 ways and odd digits in 5^3 ways. Hence the number of ways of choosing 3 even and 3 odd digits with 0 as the first digit is 10×5^5. Therefore the number of 6-digit numbers with 3 even digits and 3 odd digits is

$$20 \times 5^6 - 10 \times 5^5 = 10 \times 5^5(10-1) = 281250.$$

Example 6: There are 100 countries participating in an olympiad. Suppose n is a positive integer such that each of the 100 countries is willing to communicate in exactly n languages. If each set of 20 countries can communicate in at least one common language, and no language is common to all 100 countries, what is the minimum possible value of n?

Solution: We show that $n = 20$. We first show that $n = 20$ is possible. Call the countries $C_1, \cdots, C_{100}$. Let $1, 2, \cdots, 21$ be languages and suppose the country C_i $(1 \leq i \leq 20)$ communicates exactly in the languages $\{j : 1 \leq j \leq 20, j \neq i\}$. Suppose each of the countries $C_{21}, \cdots, C_{100}$ communicates in the languages $1, 2, \cdots, 20$. Then, clearly every set of 20 countries have a common language of communication.

Now, we show that $n \geq 20$. If $n < 20$, look at any country A communicating in the languages $L_1, \cdots, L_n$. As no language is common to all 100 countries, for each L_i, there is a country A_i not communicating in L_i. Then, the $n + 1 \leq 20$ countries $A, A_1, A_2, \cdots, A_n$ have no common language of communication. This contradiction shows $n \geq 20$.

Example 7: (ISI-23) There is a rectangular plot of size $1 \times n$. This has to be covered by three types of tiles - red, blue and black. The red tiles are of size 1×1, the blue tiles are of size 1×1 and the black tiles are of size 1×2. Let t_n denote the number of ways this can be done. For example, clearly $t_1 = 2$ because we can have either a red or a blue tile. Also $t_2 = 5$ since we could have tiled the plot as: two red tiles, two blue tiles, a red tile on the left and a blue tile on the right, a blue tile on the left and a red tile on the right, or a single black tile.

a. Prove that $t_{2n+1} = t_n(t_{n-1} + t_{n+1})$ for all $n > 1$.

b. Prove that $t_n = \sum_{d\geq 0} \binom{n-d}{d} 2^{n-2d}$ for all $n > 0$.

Here,

$$\binom{m}{r} = \begin{cases} \frac{m!}{r!(m-r)!} & \text{if } 0 \leq r \leq m, \\ 0 & \text{otherwise} \end{cases}$$

for integers m, r.

Solution: (a): Suppose t_n are the number of ways to tile the plot.

Consider a plot of dimension $1 \times 2n+1$. For that, if the tile between $n-1$ and $n+2$ tile is not covered with black then there are $t_n \cdot t_{n+1}$ ways to cover the plot. And if the tile between $n-1$ and $n+2$ is covered by a black tile then we notice first $n-1$ tiles can be covered in t_{n-1} ways and rest tiles from $n+2$ to $2n+1$ can be covered in t_n ways. Hence in total we have $t_{2n+1} = t_n(t_{n+1} + t_{n-1})$.

(b): Consider the plot is covered by d number of black tiles. Then $n - 2d$ number of 1×1 tiles are left to tile. Suppose x_1 number of 1×1 tiles are before 1st black tile, x_2 number of tiles are there between black tile 1 and black tile 2, $\cdots$, x_d be the number of tiles between $d-1$ and d-th black tile and x_{d+1} number of tiles after black tile d.

So we have $x_1 + x_2 + \cdots + x_{d+1} = n - 2d$. We have to solve this equation in non-negative integers. Solutions to this equation are $\binom{n-2d+d+1-1}{d+1-1} = \binom{n-d}{d}$. And for each 1×1 tile we have 2 ways to fill it with a red tile or blue tile.

Hence,

$$t_n = \sum_{d\geq 0} \binom{n-d}{d} 2^{n-2d}$$

Example 8 (ISI-22) Consider a board having 2 rows and n columns. Thus there are $2n$ cells in the board. Each cell is to be filled in by 0 or 1.

a. In how many ways can this be done such that each row sum and each column sum is even?

b. In how many ways can this be done such that each row sum and each column sum is odd?

Solution:

a. For the sum of elements in a row to be even, one must have $(1,1)$, $(0,0)$ as the only options to fill in row$_1$ and row$_2$. Now suppose the sum of elements till $2n-2$ cells is S.

   If $S \equiv 0 \pmod 2$, then $(0,0)$ is the only possibility, and if $S \equiv 1 \pmod 2$, then $(1,1)$ is the only possibility. So the number of ways is simply the number of ways to form S or to arrange $(1,1)$, $(0,0)$ in $n-1$ spaces which can be done in 2^{n-1} ways, so the answer for this part is 2^{n-1}.

b. Suppose $B(n)$ are the total number of ways, so we have:

$$B(n) = \begin{cases} 2^{n-1}, & \text{for } n \equiv 0 \pmod 2 \\ 0, & \text{for } n \equiv 1 \pmod 2 \end{cases}$$

Proof: Suppose n is odd, then for the sum of rows to be odd, only $(1, 0)$ or $(0, 1)$ are permissible.

Now suppose there are t 1's in Column 1, so $n - j$ are 0 and we must have j to be odd. Then $n - j$ is even. Now in Column 2, there would be $n - j$ many 1's giving the sum of elements in Column 2 even which is not possible, hence in this case $B(n) = 0$.

Now if n is even, then we need to choose any odd number of cells to fill with 1 in Column 1, as a result that will fix the Column 2 numbers. This can be done in:

$$\binom{n}{1} + \binom{n}{3} + \cdots + \binom{n}{n-1} = 2^{n-1} \text{ ways}$$

Hence:

$$B(n) = \begin{cases} 2^{n-1}, & \text{for } n \equiv 0 \pmod 2 \\ 0, & \text{for } n \equiv 1 \pmod 2 \end{cases}$$

Example 9 (ISI-20) A finite sequence of numbers $(a_1, \ldots, a_n)$ is said to be alternating if

$$a_1 > a_2,\ a_2 < a_3,\ a_3 > a_4,\ a_4 < a_5,\ \ldots$$

or

$$a_1 < a_2,\ a_2 > a_3,\ a_3 < a_4,\ a_4 > a_5,\ \ldots$$

How many alternating sequences of length 5, with distinct numbers $a_1, \ldots, a_5$, can be formed such that $a_i \in \{1, 2, \ldots, 20\}$ for $i = 1, \ldots, 5$?

Solution: First of all, since all numbers in the chosen sample of 5 numbers are distinct, so we may choose them in $\binom{20}{5}$ ways. Say, in general, we have chosen $a < b < c < d < e$. Now let us consider 2 cases.

Case 1: $\_ > \_ < \_ > \_ < \_$

Observe that a is bigger than none of the numbers, b is bigger than only a, and e is the biggest. So, a must sit in one of the 2 "$> \_ <$" gaps. The other similar gap may be filled up with either b or c only. If a and b sit in those two gaps, the other 3 may sit in any way. But, in a and c occupy those two gaps, b can sit only in the gap which is a's neighbour.

So, the possible configurations and their number of possible occurrence are as follows:

- $\_ > a < \_ > b < \_ \rightarrow 3!$ ways
- $\_ > b < \_ > a < \_ \rightarrow 3!$ ways
- $b > a < \_ > c < \_ \rightarrow 2!$ ways
- $\_ > c < \_ > a < b \rightarrow 2!$ ways

Case 2: $\_ < \_ > \_ < \_ > \_$

An exactly similar argument as the previous case may be used in this case too. Unlike the previous argument, we may fix the positions of d and e at first. The possible configurations and their number of possible occurrence are as below:

- $\_ < e > \_ < d > \_ \rightarrow 3!$ ways
- $\_ < d > \_ < e > \_ \rightarrow 3!$ ways
- $d < e > \_ < c > \_ \rightarrow 2!$ ways
- $\_ < c > \_ < e > d \rightarrow 2!$ ways

Thus, the total number of possible configurations is

$$2 \times (3! + 3! + 2! + 2!) \times \binom{20}{5} = 32 \times \binom{20}{5}$$

1. Suppose n is odd and each square of an $n \times n$ grid is arbitrarily filled with either by 1 or by -1. Let r_j and c_k denote the product of all numbers in j-th row and k-th column respectively, $1 \leq j, k \leq n$. Prove that

$$\sum_{j=1}^{n} r_j + \sum_{k=1}^{n} c_k \neq 0.$$

2. For any natural number n, let $S(n)$ denote the sum of the digits of n. Find the number of all 3-digit numbers n such that $S(S(n)) = 2$.

3. A person moves in the $x - y$ plane moving along points with integer coordinates x and y only. When she is at point (x, y), she takes a step based on the following rules:

(a) if $x + y$ is even she moves to either $(x + 1, y)$ or $(x + 1, y + 1)$;

(b) if $x + y$ is odd she moves to either $(x, y + 1)$ or $(x + 1, y + 1)$.

How many distinct paths can she take to go from $(0, 0)$ to $(8, 8)$ given that she took exactly three steps to the right $((x, y) \to (x + 1, y))$?

4. Find the number of 10-tuples $(a_1, a_2, \ldots, a_{10})$ of integers such that $|a_1| \leq 1$ and

$$a_1^2 + a_2^2 + a_3^2 + \cdots + a_{10}^2 - a_1a_2 - a_2a_3 - a_3a_4 - \cdots - a_9a_{10} - a_{10}a_1 = 2.$$

5. For a natural number n, let $T(n)$ denote the number of ways we can place n objects of weights $1, 2, \ldots, n$ on a balance such that the sum of the weights in each pan is the same. Prove that $T(100) > T(99)$.

6. Let $X = \{1, 2, 3, \ldots, 10\}$. Find the number of pairs $\{A, B\}$ such that $A \subseteq X$, $B \subseteq X$, $A \neq B$ and $A \cap B = \{2, 3, 5, 7\}$.

7. Consider a 20-sided convex polygon K, with vertices $A_1, A_2, \ldots, A_{20}$ in that order. Find the number of ways in which three sides of K can be chosen so that every pair among them has at least two sides of K between them. (For example $(A_1A_2, A_4A_5, A_{11}A_{12})$ is an admissible triple while $(A_1A_2, A_4A_5, A_{19}A_{20})$ is not.)

8. Find the number of 4-digit numbers (in base 10) having non-zero digits and which are divisible by 4 but not by 8.

9. Find the number of all 6-digit natural numbers such that the sum of their digits is 10 and each of the digits 0, 1, 2, 3 occurs at least once in them.

10. Let n be a positive integer. Call a nonempty subset S of $\{1, 2, \ldots, n\}$ good if the arithmetic mean of the elements of S is also an integer. Further, let t_n denote the number of good subsets of $\{1, 2, \ldots, n\}$. Prove that t_n and n are both odd or both even.

---

20 Pigeon Hole Principle

The simplest version of Dirichlet's box principle reads as follows:

If $(n+1)$ pearls are put into n boxes, then at least one box has more than one pearl.

This simple combinatorial principle was first used explicitly by Dirichlet (1805–1859) in number theory. In spite of its simplicity it has a huge number of quite unexpected applications. It can be used to prove deep theorems. F.P. Ramsey made vast generalizations of this principle. The topic of *Ramsey Numbers* belongs to the deepest problems of combinatorics. In spite of huge efforts, progress in this area is very slow.

It is easy to recognize if the box principle is to be used. Every existence problem about finite and, sometimes, infinite sets is usually solved by the box principle. The principle is a pure existence assertion. It gives no help in finding a multiply occupied box. The main difficulty is the identification of the *pearls* and the *boxes*.

Example 1: There are n persons present in a room. Prove that among them there are two persons who have the same number of acquaintances in the room.

Solution: A person (pigeon) goes into hole #i if he has i acquaintances. We have n persons and n holes numbered $0, 1, \ldots, n-1$. But the holes with the numbers 0 and $n-1$ cannot both be occupied. Thus, there is at least one box with more than one pigeons.

Example 2: Let $a_1, a_2, \ldots, a_n$ be n not necessarily distinct integers. Then there always exists a subset of these numbers with sum divisible by n.

Solution: We consider the n integers

$$s_1 = a_1, \quad s_2 = a_1 + a_2, \quad s_3 = a_1 + a_2 + a_3, \ldots, \quad s_n = a_1 + a_2 + \cdots + a_n.$$

If any of these integers is divisible by n, then we are done. Otherwise, all their remainders are different modulo n. Since there are only $n-1$ such remainders, two of the sums, say s_p and s_q with $p < q$, are equal modulo n, that is, the following difference is divisible by n.

$$s_q - s_p = a_{p+1} + \cdots + a_q.$$

Example 4: One of $(n+1)$ numbers from $\{1, 2, \ldots, 2n\}$ is divisible by another.

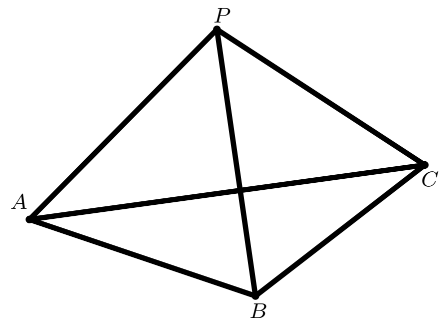
Solution: We select $(n+1)$ numbers $a_1, \ldots, a_{n+1}$ and write them in the form $a_i = 2^k b_i$ with b_i odd. Then we have $(n+1)$ odd numbers $b_1, \ldots, b_{n+1}$ from the interval $[1, 2n-1]$. But there are only n odd numbers in this interval. Thus two of them p, q are such that $b_p = b_q$. Then one of the numbers a_p, a_q is divisible by the other.

Example 5: Let $a, b \in \mathbb{N}$ be coprime. Then $ax - by = 1$ for some $x, y \in \mathbb{N}$.

Solution: Consider the remainders modulo b of the sequence $a, \ldots, (b-1)a$. The remainder 0 does not occur. If the remainder 1 would not occur either, then we would have positive integers $p, q, 0 < p < q < b$, so that $pa \equiv qa \pmod{b}$. But a and b are coprime. Hence we have $b \mid q - p$. This is a contradiction since $0 < q - p < b$. Thus there exists an x so that $ax \equiv 1 \pmod{b}$, that is, $ax - by = 1$.

Example 6: Among six persons, there are always three who know each other or three who are complete strangers.

Solution: The edges of a G_6 are colored red or blue. Take any of the six points and call it P. At least 3 of the 5 lines which start at P are of the same color, say *red*. These red lines end at 3 points A, B, C . If any side of the triangle ABC is red, we have a red triangle. If not, ABC is a blue triangle. In both cases, we have a *monochromatic triangle*. Figure below shows that with 5 points and 2 colors there need not exist a monochromatic triangle. Here sides and diagonals have different colors.



20.1 Exercise

1. n persons meet in a room. Everyone shakes hands with everyone else. Prove that during the greeting ceremony there are always two persons who have shaken the same number of hands.

2. In a tournament with n players, everybody plays with everybody else exactly once. Prove that during the game there are always two players who have played the same number of games.

3. Twenty pairwise distinct positive integers are all < 70. Prove that among their pairwise differences there are four equal numbers.

4. Let $P_1, \ldots, P_9$ be nine lattice points in space, no three collinear. Prove that there is a lattice point L lying on some segment P_iP_k, $i \neq k$.

5. Fifty-one small insects are placed inside a square of side 1. Prove that at any moment there are at least three insects which can be covered by a single disk of radius $1/7$.

6. Let n be a positive integer which is not divisible by 2 or 5. Prove that there is a multiple of n consisting entirely of ones.

7. S is a set of n positive integers. None of the elements of S is divisible by n. Prove that there exists a subset of S such that the sum of its elements is divisible by n.

8. Among $n+1$ integers from $\{1, 2, \ldots, 2n\}$ there are two which are coprime.

9. From ten distinct two-digit numbers, one can always choose two disjoint nonempty subsets, so that their elements have the same sum (IMO 1972).

10. Let k be a positive integer and $n = 2^{k-1}$. Prove that, from $(2n-1)$ positive integers, one can select n integers, such that their sum is divisible by n.

11. Let $a_1, \ldots, a_n$ $(n \geq 5)$ be any sequence of positive integers. Prove that it is always possible to select a subsequence and add or subtract its elements such that the sum is a multiple of n^2.

12. One of the positive reals $a, 2a, \ldots, (n-1)a$ has at most distance $\frac{1}{n}$ from a positive integer.

13. Two of six points placed into a 3×4 rectangle will have distance $\leq \sqrt{5}$.

14. Prove that, among any seven real numbers $y_1, \ldots, y_7$, there exist two, such that

$$0 \leq \frac{y_i - y_j}{1 + y_i y_j} \leq \frac{1}{\sqrt{3}}.$$

21 Invariance Principle

There are different strategies for solving problems and one of them is the Invariance Priciple whose basic idea is

If there is repetition, look for what doesn't change

This quantity that doesn't not change in every repetition or every iteration is known as the invariant.

Suppose we look the following scenario. You are defining a sequence recursively using the following definition

$$x_0 = a \quad y_0 = b \quad x_{n+1} = \frac{x_n + y_n}{2} \quad y_{n+1} = \frac{2x_n y_n}{x_n + y_n}$$

Now the typical question is what can be the invariant. It differs from question to question but in this case we can see that the numerator in the definition of x_{n+1} and the denominator in the definiton of y_{n+1} is the same so a good strategy would be to multiply them together and doing so we get that

$$x_{n+1}y_{n+1} = x_n y_n \ \forall \ n$$

Thus since the product of the initial terms is ab hence the product us going to be ab throughout. Now why is this helpful? The question could be as simple as find $\lim x_n y_n$ So instead of solving the recurrence we can directly say what the limit is going to be.

One more common property that could turn out to be the invariant is the parity or maybe the remainder modulo n for some $n \in \mathbb{N}$. Let us look at a very elegant application of this.

Example 1: Eight rooks are placed on a chessboard so that none of them attacks another. Prove that the number of rooks standing on black squares is even.

Solution: There doesn't seem to be any direct way of solving this. Let us start of by looking at the chessboard. If we look carefully every square can be uniquely determined by its coordinates as (i, j) with $1 \leq i, j \leq 8$ stating from the bottom left corner and then proceeding row wise. If we associate this with the colour of the squares we can say that the colour of the square is goiing to be

$$C(i,j) = \begin{cases} B & i + j \equiv 0 \pmod 2 \\ W & i + j \equiv 1 \pmod 2 \end{cases}$$

Now based on the little bit of chess knowledge we have we can say that two rooks attack each other if they are in the same row or column. So if we look at the position of the rooks as $R_i(a_i, b_i)$ then no two a_i's or b_i's can be the same.

Now the question asks to prove that the no of rooks on black squares should be even. For the sake of contradiction assume that the number of rooks on the black squares is odd. Then if we look at the sum

$$\sum_{i=1}^{8}(a_i + b_i) = \sum_{\text{black squares}} (a_i + b_i) + \sum_{\text{white squares}} (a_i + b_i)$$

Now from the colouring rule of the chessboard, we know that for rooks on the white squares, the sum of its coordinates is odd and if there are an odd number of rooks on black squares, trhe number of rooks on the white squares should also be odd which in turn implies that the second sum is odd. Now, the first sum is even no matter what which implies that the total sum is odd. Now we also know that the values of a_i's and b_i's are both some permutations of $1, \cdots, 8$ which means that the total sum should be 72 which is even hence this gives us a contradiction.

So in this particular example, the invariant is the parity of the sum of the coordinates of the rooks which is always even no matter which way you arrange them.

Example 2: Suppose the positive integer n is odd. First Al writes the numbers $1, 2, \ldots, 2n$ on the blackboard. Then he picks any two numbers a, b, erases them, and writes, instead, $|a - b|$. Prove that an odd number will remain at the end.

Solution: Suppose S is the sum of all the numbers still on the blackboard. Initially this sum is $S = 1+2+\cdots+2n = n(2n+1)$, an odd number. Each step reduces S by $2\min(a, b)$, which is an even number. So the parity of S is an invariant. During the whole reduction process we have $S \equiv 1 \mod 2$. Initially the parity is odd. So, it will also be odd at the end.

Example 3: A circle is divided into six sectors. Then the numbers $1, 0, 1, 0, 0, 0$ are written into the sectors (counterclockwise, say). You may increase two neighboring numbers by 1. Is it possible to equalize all numbers by a sequence of such steps?

Solution: Suppose $a_1, \ldots, a_6$ are the numbers currently on the sectors. Then $I = a_1 - a_2 + a_3 - a_4 + a_5 - a_6$ is an invariant. Initially $I = 2$. The goal $I = 0$ cannot be reached.

So it clear from these examples that different problems need different approaches but the key idea is the same. **Look for what does not change**. So this is one of those topics which are questions based that is the more the number of question you do, the better you understand the topic. So let us look at a few more solved examples.

Example 4: The numbers 1, 2, 3, ..., 19, 20 are written on a blackboard. It is allowed to erase any two numbers a and b and write the new number $a+b-1$. What number will be on the blackboard after 19 such operations?

Solution: For any collection of n numbers on the blackboard we consider the following quantity X: the sum of all the numbers decreased by n. Assume that we have transformed the collection as described in the statement. How would the quantity X change? If the sum of all the numbers except a and b equals S, then before the transformation $X = S + a + b - n$, and after the transformation $X = S + (a + b - 1) - (n - 1) = S + a + b - n$. So the value of X is the same: it is invariant. Initially (for the collection in the statement) we have

$$X = (1 + 2 + \cdots + 19 + 20) - 20 = 190.$$

Therefore, after 19 operations, when there will be only one number on the blackboard, X will be equal to 190. This means that the last number, which is $X + 1$, is 191.

Example 5: There are 13 grey, 15 brown, and 17 red chameleons on Chromatic Island. When two chameleons of different colours meet they both change their colour to the third one (for instance, grey and brown both become red). Is it possible that after some time all the chameleons on the island are the same colour?

Solution: The first question that comes to our mind is that do we express this idea of changing colours mathematically? One way is to say that two chameleons of the different colours vanish and two chameleons of the third colour appear. Thus if we have a triplet (a, b, c) where we have a grey chameleon, b brown chameleon and 17 red chameleon then we have three possibilities for the next step

$$(a, b, c) \to (a - 1, b - 1, c + 2) \text{ or } (a - 1, b + 2, c - 1) \text{ or } (a + 2, b - 1, c - 1)$$

Now, if we look at the difference between the no of chameleons of any two color remains invariant modulo 3. Thus in finally we have all chameleons of the same colour say grey then we would have 45 grey chameleons and 0 brown chameleons so their difference is $\equiv 0 \pmod 3$ whereas initially we had their diffrernce as $13 - 15 \equiv -2 \pmod 3$. Hence it is not possible for the chameleons to be grey. Similarly we can prove it for the other colours.

21.1 Exercise

1. Start with the positive integers $1, \ldots, 4n-1$. In one move you may replace any two integers by their difference. Prove that an even integer will be left after $4n-2$ steps.

2. Around a circle, 5 ones and 4 zeros are arranged in any order. Then between any two equal digits, you write 0 and between different digits 1. Finally, the original digits are wiped out. If this process is repeated indefinitely, you can never get 9 zeros.

3. Each of the numbers 1 to 10^6 is repeatedly replaced by its digital sum until we reach 10^6 one-digit numbers. Will these have more 1's or 2's?

4. Each term in a sequence $1, 0, 1, 0, 1, 0, \ldots$ starting with the seventh is the sum of the last 6 terms mod 10. Prove that the sequence $\ldots, 0, 1, 0, 1, 0, 1, \ldots$ never occurs.

5. The integers $1, \ldots, 2n$ are arranged in any order on $2n$ places numbered $1, \ldots, 2n$. Now we add its place number to each integer. Prove that there are two among the sums which have the same remainder mod $2n$.

6. Many handshakes are exchanged at a big international congress. We call a person an *odd person* if he has exchanged an odd number of handshakes. Otherwise he will be called an *even person*. Show that, at any moment, there is an even number of odd persons.

7. A dragon has 100 heads. A knight can cut off 15, 17, 20, or 5 heads, respectively, with one blow of his sword. In each of these cases, 24, 2, 14, or 17 new heads grow on its shoulders. If all heads are blown off, the dragon dies. Can the dragon ever die?

8. The numbers $1, 2, 3, \ldots, 1989$ are written on a blackboard. It is permitted to erase any two of them and replace them with their difference. Can this operation be used to obtain a situation where all the numbers on the blackboard are zeros?

9. The numbers $1, 2, \ldots, 20$ are written on a blackboard. It is permitted to erase any two numbers a and b and write the new number $ab + a + b$. Which number can be on the blackboard after 19 such operations?

10. There are Martian amoebae of three types (A, B, and C) in a test tube. Two amoebae of any two different types can merge into one amoeba of the third type. After several such merges only one amoeba remains in the test tube. What is its type, if initially there were 20 amoebae of type A, 21 amoebae of type B, and 22 amoebae of type C?
