MATH OLYMPIAD MASTERY

MOM

MATH OLYMPIAD MASTERY LEVEL II

1st EDITION

August 2023

Authors

Nkundayezu Emmanuel

Musangwa Innocent

Warakoze Bel-ami

Abayo Joseph Desire

Munezero Jean Nepo

Akimana Nadine

Korusenge Obed

Hategekimana Hirwa Arnold

Irakarama Alain

Subukino Arnaud

Kagaba Etienne

Kigali City, Rwanda

Contact: math.olympiad.mastery@gmail.com

PREFACE

Dear Readers,

Welcome to "MATH OLYMPIAD MASTERY LEVEL II," the ultimate challenge for those seeking to conquer the highest peaks of mathematical problem-solving. This book builds upon the foundation laid in its predecessor, pushing the boundaries of your mathematical prowess to even greater heights. As you delve into the intricate world of mathematics, you will encounter a diverse array of topics that will not only expand your knowledge but also sharpen your problem-solving skills.

Journey Through Advanced Mathematics:

Level 2 of the "MATH OLYMPIAD MASTERY" series is a monumental step forward, exploring deeper realms of algebra, number theory, geometry, and combinatorics. Within these pages, you will unearth the beauty of advanced factorization techniques, inequalities, and functional equations. You will unravel the mysteries of prime numbers, modular arithmetic, and complex equations in number theory. Geometry will captivate your mind with theorems like Ceva's, Menelaus', and Ptolemy's, while combinatorics will challenge you with integral solutions, proof by induction, and graph theory.

Mastering Complexity:

The challenges presented in this book are not for the faint of heart. They are meticulously curated to foster your intellectual growth and deepen your understanding of intricate mathematical concepts. Throughout your journey, you will encounter in-depth explanations, step-by-step solutions, and exercises that will test your limits. These problems are not merely mathematical puzzles; they are gateways to unlocking your full potential.

Unlocking Olympian Wisdom:

As you navigate through the contents of this book, you will uncover the wisdom of renowned mathematicians who have paved the way before us. You will unravel the threads that connect seemingly disparate concepts and discover the elegant simplicity underlying the most complex problems. This is not just a compilation of knowledge; it is a guided exploration of the mathematical universe.

Embrace the Challenge:

While the path ahead may be demanding, remember that every challenge you overcome is a step closer to mathematical mastery. Embrace each problem as an opportunity to refine your problem-solving skills, broaden your horizons, and cultivate the art of logical thinking. As you progress through these pages, know that you are not alone on this journey – the authors, mentors, and fellow enthusiasts are with you every step of the way.

Acknowledgments:

Let the voyage through "MATH OLYMPIAD MASTERY LEVEL II" be a transformative experience. May you emerge from these pages not only as a mathematically adept individual but also as a resilient problem solver capable of conquering any challenge that comes your way.

Enjoy the journey and embrace the art of mathematical mastery!

Sincerely,

Authors.

Contents

Part I

MATH OLYMPIAD CONTENT

Chapter 1

ALGEBRA

1.1 GENERAL FACTORIZATION

1. $x(a+b) = xa + xb$
2. $(a+b)(c+d) = ac + ad + bc + bd$
3. $(a^b)^c = a^{bc}$
4. $a^{b^{c^d}} = a^{(b^{(c^d)})}$
5. $a^2 - b^2 = (a-b)(a+b)$
6. $(a+b)^2 = a^2 + 2ab + b^2$
7. $(a+b+c)^2 = a^2 + b^2 + c^2 + 2ab + 2ac + 2bc$
8. $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$
9. $a^3 + b^3 = (a+b)(a^2 - ab + b^2)$
10. $a^3 - b^3 = (a-b)(a^2 + ab + b^2)$
11. $a^3 + b^3 + c^3 - 3abc = (a+b+c)(a^2 + b^2 + c^2 - ab - bc - ac)$
12. $(a+b+c)^3 = a^3 + b^3 + c^3 + 3(a+b)(b+c)(a+c)$
13. $a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$
14. $(1 - r^n) = (1-r)(1 + r + r^2 + \ldots + r^{n-1})$
15. $(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \ldots + \binom{n}{n-1}ab^{n-1} + b^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i +$ (It's called binomial expansion.)
16. $a^n + b^n = (a-b)(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + ab^{n-1})$

1.2 INEQUALITIES

[2]

1.2.1 General AM-GM Inequality

The most well-known and frequently used inequality is the Arithmetic mean-Geometric mean inequality or widely known as the AM-GM inequality. The term AM-GM is the combination of the two terms Arithmetic Mean and Geometric Mean. The arithmetic mean of two numbers a and b is defined by $\frac{a+b}{2}$. Similarly $\sqrt{ab}$ is the geometric mean of a and b. The simplest form of the AM-GM inequality is the following:

Basic AM-GM Inequality. For positive real numbers a, b

$$\frac{a+b}{2} \geq \sqrt{ab}$$

The proof is simple. Squaring, this becomes

$$(a+b)^2 \geq 4ab$$

which is equivalent to

$$(a-b)^2 \geq 0.$$

This is obviously true. Equality holds if and only if $a = b$.

Example 1.1.1. For real numbers a, b, c prove that

$$a^2 + b^2 + c^2 \geq ab + bc + ca.$$

First Solution. By AM-GM inequality, we have

$$\begin{aligned} a^2 + b^2 &\geq 2ab, \\ b^2 + c^2 &\geq 2bc, \\ c^2 + a^2 &\geq 2ca. \end{aligned}$$

Adding the three inequalities and then dividing by 2 we get the desired result. Equality holds if and only if $a = b = c$.

Second Solution. The inequality is equivalent to

$$(a-b)^2 + (b-c)^2 + (c-a)^2 \geq 0,$$

which is obviously true.

However, the general AM-GM inequality is also true for any n positive numbers.

General AM-GM Inequality. For positive real numbers $a_1, a_2, \ldots, a_n$ the following inequality holds.

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \cdots a_n},$$

with equality if and only if $a_1 = a_2 = \cdots = a_n$.

Proof. Here we present the well known Cauchy's proof by induction. This special kind of induction is done by performing the following steps:

i. Base case.

ii. $P_n \Longrightarrow P_{2n}$.

iii. $P_n \Longrightarrow P_{n-1}$.

Here P_n is the statement that the AM-GM is true for n variables.

Step 1: We already proved the inequality for $n = 2$. For $n = 3$ we get the following inequality:

$$\frac{a+b+c}{3} \geq \sqrt[3]{abc}$$

Letting $a = x^3, b = y^3, c = z^3$ we equivalently get

$$x^3 + y^3 + z^3 - 3xyz \geq 0.$$

This is true by Example 1.1.1 and the identity

$$x^3 + y^3 + z^3 - 3xyz = (x + y + z)\left(x^2 + y^2 + z^2 - xy - yz - zx\right).$$

Equality holds for $x = y = z$, that is, $a = b = c$.
Step 2: Assuming that P_n is true, we have

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \cdots a_n}.$$

Now it's not difficult to notice that

$$a_1 + a_2 + \cdots + a_{2n} \geq n\sqrt[n]{a_1 a_2 \cdots a_n} + n\sqrt[n]{a_{n+1} a_{n+2} \cdots a_{2n}} \geq 2n\sqrt[2n]{a_1 a_2 \cdots a_{2n}}$$

implying P_{2n} is true.
Step 3: First we assume that P_n is true i.e.

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \cdots a_n}.$$

As this is true for all positive a_i s, we let $a_n = \sqrt[n-1]{a_1 a_2 \cdots a_{n-1}}$. So now we have

$$\begin{aligned}
\frac{a_1 + a_2 + \cdots + a_n}{n} &\geq \sqrt[n]{a_1 a_2 \cdots a_{n-1} \sqrt[n-1]{a_1 a_2 \cdots a_{n-1}}} \\
&= \sqrt[n]{(a_1 a_2 \cdots a_{n-1})^{\frac{n}{n-1}}} \\
&= \sqrt[n-1]{a_1 a_2 \cdots a_{n-1}} \\
&= a_n
\end{aligned}$$

which in turn is equivalent to

$$\frac{a_1 + a_2 + \cdots + a_{n-1}}{n-1} \geq a_n = \sqrt[n-1]{a_1 a_2 \cdots a_{n-1}}.$$

The proof is thus complete. It also follows by the induction that equality holds for $a_1 = a_2 = \cdots = a_n$. Try to understand yourself why this induction works. It can be useful sometimes.

Example 1.1.2. Let $a_1, a_2, \ldots, a_n$ be positive real numbers such that $a_1 a_2 \cdots a_n = 1$. Prove that

$$(1 + a_1)(1 + a_2) \cdots (1 + a_n) \geq 2^n.$$

Solution. By AM-GM,

$$\begin{aligned}
1 + a_1 &\geq 2\sqrt{a_1}, \\
1 + a_2 &\geq 2\sqrt{a_2}, \\
&\vdots \\
1 + a_n &\geq 2\sqrt{a_n}.
\end{aligned}$$

Multiplying the above inequalities and using the fact $a_1 a_2 \cdots a_n = 1$ we get our desired result. Equality holds for $a_i = 1, i = 1, 2, \ldots, n$.

Example 1.1.3. Let a, b, c be nonnegative real numbers. Prove that

$$(a + b)(b + c)(c + a) \geq 8abc$$

Solution. The inequality is equivalent to

$$\left(\frac{a + b}{\sqrt{ab}}\right)\left(\frac{b + c}{\sqrt{bc}}\right)\left(\frac{c + a}{\sqrt{ca}}\right) \geq 2 \cdot 2 \cdot 2,$$

true by AM-GM. Equality holds if and only if $a=b=c$.
Example 1.1.4. Let $a,b,c>0$. Prove that

$$\frac{a^3}{bc}+\frac{b^3}{ca}+\frac{c^3}{ab}\geq a+b+c.$$

Solution. By AM-GM we deduce that

$$\begin{aligned}\frac{a^3}{bc}+b+c&\geq 3\sqrt[3]{\frac{a^3}{bc}\cdot b\cdot c}=3a\\ \frac{b^3}{ca}+c+a&\geq 3\sqrt[3]{\frac{b^3}{ca}\cdot c\cdot a}=3b\\ \frac{c^3}{ab}+a+b&\geq 3\sqrt[3]{\frac{c^3}{ab}\cdot a\cdot b}=3c.\end{aligned}$$

Adding the three inequalities we get

$$\frac{a^3}{bc}+\frac{b^3}{ca}+\frac{c^3}{ab}+2(a+b+c)\geq 3(a+b+c)$$

which was what we wanted.
Example 1.1.5. (Samin Riasat) Let a,b,c be positive real numbers. Prove that

$$ab(a+b)+bc(b+c)+ca(c+a)\geq\sum_{cyc}ab\sqrt{\frac{a}{b}(b+c)(c+a)}.$$

Solution. By AM-GM,

$$\begin{aligned}&2ab(a+b)+2ac(a+c)+2bc(b+c)\\ =&ab(a+b)+ac(a+c)+bc(b+c)+ab(a+b)+ac(a+c)+bc(b+c)\\ =&a^2(b+c)+b^2(a+c)+c^2(a+b)+\left(a^2b+b^2c+a^2c\right)+\left(ab^2+bc^2+a^2c\right)\\ \geq&a^2(b+c)+b^2(a+c)+c^2(a+b)+\left(a^2b+b^2c+a^2c\right)+3abc\\ =&a^2(b+c)+b^2(a+c)+c^2(a+b)+ab(a+c)+bc(a+b)+ac(b+c)\\ =&\left(a^2(b+c)+ab(a+c)\right)+\left(b^2(a+c)+bc(a+b)\right)+\left(c^2(a+b)+ac(b+c)\right)\\ \geq&2\sqrt{a^3b(b+c)(a+c)}+2\sqrt{b^3c(a+c)(a+b)}+2\sqrt{c^3a(a+b)(b+c)}\\ =&2ab\sqrt{\frac{a}{b}(b+c)(a+c)}+2cb\sqrt{\frac{b}{c}(a+c)(a+b)}+2ac\sqrt{\frac{c}{a}(a+b)(b+c)}.\end{aligned}$$

Equality holds if and only if $a=b=c$.
Exercise 1.1.1. Let $a,b>0$. Prove that

$$\frac{a}{b}+\frac{b}{a}\geq 2$$

Exercise 1.1.2. For all real numbers a,b,c prove the following chain inequality

$$3\left(a^2+b^2+c^2\right)\geq(a+b+c)^2\geq 3(ab+bc+ca).$$

Exercise 1.1.3. Let a,b,c be positive real numbers. Prove that

$$a^3+b^3+c^3\geq a^2b+b^2c+c^2a$$

Exercise 1.1.4. Let a,b,c be positive real numbers. Prove that

$$a^3+b^3+c^3+ab^2+bc^2+ca^2\geq 2\left(a^2b+b^2c+c^2a\right).$$

Exercise 1.1.5. Let a,b,c be positive real numbers such that $abc=1$. Prove that

$$a^2+b^2+c^2\geq a+b+c.$$

1.2.2 More Challenging Problems

Exercise 1.3.1. Let a, b, c be positive real numbers such that $abc = 1$. Prove that

$$\frac{a}{b} + \frac{b}{c} + \frac{c}{a} \geq a + b + c$$

Exercise 1.3.2. (Michael Rozenberg) Let a, b, c and d be non-negative numbers such that $a+b+c+d = 4$. Prove that

$$\frac{4}{abcd} \geq \frac{a}{b} + \frac{b}{c} + \frac{c}{d} + \frac{d}{a}$$

Exercise 1.3.3. (Samin Riasat) Let a, b, c be positive real numbers. Prove that

$$\frac{a^3+b^3+c^3}{3} \geq \frac{a+b+c}{3} \cdot \frac{a^2+b^2+c^2}{3} \geq \frac{a^2b+b^2c+c^2a}{3}$$

Exercise 1.3.4.(a) (Pham Kim Hung) Let a, b, c be positive real numbers. Prove that

$$\frac{a}{b} + \frac{b}{c} + \frac{c}{a} + \frac{3\sqrt[3]{abc}}{a+b+c} \geq 4$$

(b) (Samin Riasat) For real numbers $a, b, c > 0$ and $n \leq 3$ prove that

$$\frac{a}{b} + \frac{b}{c} + \frac{c}{a} + n\left(\frac{3\sqrt[3]{abc}}{a+b+c}\right) \geq 3 + n$$

Exercise 1.3.5. (Samin Riasat) Let a, b, c be positive real numbers such that $a+b+c = ab+bc+ca$ and $n \leq 3$. Prove that

$$\frac{a^2}{b} + \frac{b^2}{c} + \frac{c^2}{a} + \frac{3n}{a^2+b^2+c^2} \geq 3 + n.$$

1.2.3 Cauchy-Schwarz Inequality

The Cauchy-Schwarz inequality is a very powerful inequality. It is very useful in proving both cyclic and symmetric inequalities. The special equality case also makes it exceptional. The inequality states:

Cauchy-Schwarz Inequality. For any real numbers $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ the following inequality holds.

$$\left(a_1^2 + a_2^2 + \cdots + a_n^2\right)\left(b_1^2 + b_2^2 + \cdots + b_n^2\right) \geq \left(a_1b_1 + a_2b_2 + \cdots + a_nb_n\right)^2,$$

with equality if the sequences are proportional. That is if $\frac{a_1}{b_1} = \frac{a_2}{b_2} = \cdots = \frac{a_n}{b_n}$.

First proof. This is the classical proof of Cauchy-Schwarz inequality. Consider the quadratic

$$f(x) = \sum_{i=1}^{n} (a_i x - b_i)^2 = x^2 \sum_{i=1}^{n} a_i^2 - x \sum_{i=1}^{n} 2a_i b_i + \sum_{i=1}^{n} b_i^2 = Ax^2 + Bx + C.$$

Clearly $f(x) \geq 0$ for all real x. Hence if D is the discriminant of f, we must have $D \leq 0$. This implies

$$B^2 \leq 4AC \Rightarrow \left(\sum_{i=1}^{n} 2a_i b_i\right)^2 \leq 4\left(\sum_{i=1}^{n} a_i^2\right)\left(\sum_{i=1}^{n} b_i^2\right)$$

which is equivalent to

$$\left(\sum_{i=1}^{n} a_i^2\right)\left(\sum_{i=1}^{n} b_i^2\right) \geq \left(\sum_{i=1}^{n} a_i b_i\right)^2$$

Equality holds when $f(x)=0$ for some x, which happens if $x=\frac{b_1}{a_1}=\frac{b_2}{a_2}=\cdots=\frac{b_n}{a_n}$. Second Proof. By AM-GM, we have

$$\begin{aligned}\frac{a_1^2}{\sum a_i^2}+\frac{b_1^2}{\sum b_i^2}&\geq\frac{2a_1b_1}{\sqrt{\left(\sum a_i^2\right)\left(\sum b_i^2\right)}},\\ \frac{a_2^2}{\sum a_i^2}+\frac{b_2^2}{\sum b_i^2}&\geq\frac{2a_2b_2}{\sqrt{\left(\sum a_i^2\right)\left(\sum b_i^2\right)}},\\ &\vdots\\ \frac{a_n^2}{\sum a_i^2}+\frac{b_n^2}{\sum b_i^2}&\geq\frac{2a_nb_n}{\sqrt{\left(\sum a_i^2\right)\left(\sum b_i^2\right)}}.\end{aligned}$$

Summing up the above inequalities, we have

$$2\geq\sum\frac{2a_ib_i}{\sqrt{\left(\sum a_i^2\right)\left(\sum b_i^2\right)}},$$

which is equivalent to

$$\left(\sum_{i=1}^n a_i^2\right)\left(\sum_{i=1}^n b_i^2\right)\geq\left(\sum_{i=1}^n a_ib_i\right)^2$$

Equality holds if for each $i\in\{1,2,\ldots,n\}$, $\frac{a_i^2}{a_1^2+a_2^2+\cdots+a_n^2}=\frac{b_i^2}{b_1^2+b_2^2+\cdots+b_n^2}$, which in turn is equivalent to $\frac{a_1}{b_1}=\frac{a_2}{b_2}=\cdots=\frac{a_n}{b_n}$.

We could rewrite the above solution as follows

$$\begin{aligned}2&=\sum\frac{a_i^2}{a_1^2+a_2^2+\cdots+a_n^2}+\sum\frac{b_i^2}{b_1^2+b_2^2+\cdots+b_n^2}\\ &\geq\sum\frac{2a_ib_i}{\sqrt{\left(a_1^2+a_2^2+\cdots+a_n^2\right)\left(b_1^2+b_2^2+\cdots+b_n^2\right)}}.\end{aligned}$$

Here the sigma $\sum$ notation denotes cyclic sum and it will be used everywhere throughout this note. It is recommended that you get used to the summation symbol. Once you get used to it, it makes your life easier and saves your time.

Cauchy-Schwarz in Engel Form. For real numbers $a_i,a_2,\ldots,a_n$ and $b_1,b_2,\ldots,b_n>0$ the following inequality holds:

$$\frac{a_1^2}{b_1}+\frac{a_2^2}{b_2}+\cdots+\frac{a_n^2}{b_n}\geq\frac{\left(a_1+a_2+\cdots+a_n\right)^2}{b_1+b_2+\cdots+b_n},$$

with equality if and only if $\frac{a_1}{b_1}=\frac{a_2}{b_2}=\cdots=\frac{a_n}{b_n}$.

Although this is a direct consequence of the Cauchy-Schwarz inequality, let us prove it in a different way. For $n=2$ this becomes

$$\frac{a^2}{x}+\frac{b^2}{y}\geq\frac{(a+b)^2}{x+y}.$$

Clearing out the denominators, this is equivalent to

$$(ay-bx)^2\geq 0$$

which is clearly true. For $n=3$ we have from (2.2)

$$\frac{a^2}{x}+\frac{b^2}{y}+\frac{c^2}{z}\geq\frac{(a+b)^2}{x+y}+\frac{c^2}{z}\geq\frac{(a+b+c)^2}{x+y+z}.$$

A similar inductive process shows that

$$\frac{a_1^2}{b_1}+\frac{a_2^2}{b_2}+\cdots+\frac{a_n^2}{b_n} \geq \frac{(a_1+a_2+\cdots+a_n)^2}{b_1+b_2+\cdots+b_n}.$$

And the case of equality easily follows too.
From (2.1) we deduce another proof of the Cauchy-Schwarz inequality.
Third Proof. We want to show that

$$\left(\sum b_i^2\right)\left(\sum c_i^2\right) \geq \left(\sum b_i c_i\right)^2.$$

Let a_i be real numbers such that $a_i = b_i c_i$. Then the above inequality is equivalent to

$$\frac{a_1^2}{b_1^2}+\frac{a_2^2}{b_2^2}+\cdots+\frac{a_n^2}{b_n^2} \geq \frac{(a_1+a_2+\cdots+a_n)^2}{b_1^2+b_2^2+\cdots+b_n^2}.$$

This is just (2.1).
Example 2.1.1. Let a, b, c be real numbers. Show that

$$3\left(a^2+b^2+c^2\right) \geq (a+b+c)^2.$$

Solution. By Cauchy-Schwarz inequality,

$$\left(1^2+1^2+1^2\right)\left(a^2+b^2+c^2\right) \geq (1\cdot a+1\cdot b+1\cdot c)^2.$$

Example 2.1.2. (Nesbitt's Inequality) For positive real numbers a, b, c prove that

$$\frac{a}{b+c}+\frac{b}{c+a}+\frac{c}{a+b} \geq \frac{3}{2}.$$

First Solution. Our inequality is equivalent to

$$\frac{a}{b+c}+1+\frac{b}{c+a}+1+\frac{c}{a+b}+1 \geq \frac{9}{2}$$

or

$$(a+b+c)\left(\frac{1}{b+c}+\frac{1}{c+a}+\frac{1}{a+b}\right) \geq \frac{9}{2}.$$

This can be written as

$$\left(x^2+y^2+z^2\right)\left(\frac{1}{x^2}+\frac{1}{y^2}+\frac{1}{z^2}\right) \geq (1+1+1)^2,$$

where $x=\sqrt{b+c}, y=\sqrt{c+a}, z=\sqrt{a+b}$. Then this is true by Cauchy-Schwarz.
Second Solution. As in the previous solution we need to show that

$$(a+b+c)\left(\frac{1}{b+c}+\frac{1}{c+a}+\frac{1}{a+b}\right) \geq \frac{9}{2},$$

which can be written as

$$\frac{b+c+c+a+a+b}{3}\cdot\frac{\frac{1}{b+c}+\frac{1}{c+a}+\frac{1}{a+b}}{3} \geq \sqrt[3]{(b+c)(c+a)(a+b)}\cdot\sqrt[3]{\frac{1}{(b+c)(c+a)(a+b)}}$$

which is true by AM-GM.
Third Solution. We have

$$\sum\frac{a}{b+c}=\sum\frac{a^2}{ab+ca} \geq \frac{(a+b+c)^2}{2(ab+bc+ca)}$$

So it remains to show that

$$(a+b+c)^2 \geq 3(ab+bc+ca) \Leftrightarrow (a-b)^2+(b-c)^2+(c-a)^2 \geq 0.$$

Example 2.1.3. For nonnegative real numbers x, y, z prove that

$$\sqrt{3x^2+xy}+\sqrt{3y^2+yz}+\sqrt{3z^2+zx} \leq 2(x+y+z).$$

Solution. By Cauchy-Schwarz inequality,

$$\sum \sqrt{x(3x+y)} \leq \sqrt{\left(\sum x\right)\left(\sum (3x+y)\right)} = \sqrt{4(x+y+z)^2} = 2(x+y+z).$$

Example 2.1.4. (IMO 1995) Let a, b, c be positive real numbers such that $abc = 1$. Prove that

$$\frac{1}{a^3(b+c)}+\frac{1}{b^3(c+a)}+\frac{1}{c^3(a+b)} \geq \frac{3}{2}$$

Solution. Let $x = \frac{1}{a}, y = \frac{1}{b}, z = \frac{1}{c}$. Then by the given condition we obtain $xyz = 1$. Note that

$$\sum \frac{1}{a^3(b+c)} = \sum \frac{1}{\frac{1}{x^3}\left(\frac{1}{y}+\frac{1}{z}\right)} = \sum \frac{x^2}{y+z}$$

Now by Cauchy-Schwarz inequality

$$\sum \frac{x^2}{y+z} \geq \frac{(x+y+z)^2}{2(x+y+z)} = \frac{x+y+z}{2} \geq \frac{3\sqrt[3]{xyz}}{2} = \frac{3}{2}$$

where the last inequality follows from AM-GM.
Example 2.1.5. For positive real numbers a, b, c prove that

$$\frac{a}{2a+b}+\frac{b}{2b+c}+\frac{c}{2c+a} \leq 1$$

Solution. We have

$$\begin{aligned}
&\sum \frac{a}{2a+b} \leq 1 \\
\Leftrightarrow &\sum \left(\frac{a}{2a+b}-\frac{1}{2}\right) \leq 1-\frac{3}{2} \\
\Leftrightarrow &-\frac{1}{2}\sum \frac{b}{2a+b} \leq -\frac{1}{2} \\
\Leftrightarrow &\sum \frac{b}{2a+b} \geq 1.
\end{aligned}$$

This follows from Cauchy-Schwarz inequality

$$\sum \frac{b}{2a+b} = \frac{b^2}{2ab+b^2}+\frac{c^2}{2bc+c^2}+\frac{a^2}{2ca+a^2} \geq \frac{(a+b+c)^2}{2(ab+bc+ca)+b^2+c^2+a^2} = 1.$$

Example 2.1.6. (Vasile Cirtoaje, Samin Riasat) Let x, y, z be positive real numbers. Prove that

$$\sqrt{\frac{x}{x+y}}+\sqrt{\frac{y}{y+z}}+\sqrt{\frac{z}{z+x}} \leq \frac{3}{\sqrt{2}}.$$

Solution. Verify that

$$\begin{aligned}
\text{LHS} &= \frac{\sqrt{x(y+z)(z+x)}+\sqrt{y(z+x)(x+y)}+\sqrt{z(x+y)(y+z)}}{\sqrt{(x+y)(y+z)(z+x)}} \\
&\leq \sqrt{\frac{(x(y+z)+y(z+x)+z(x+y))(z+x+x+y+y+z))}{(x+y)(y+z)(z+x)}} \\
&= \sqrt{4\cdot\frac{(xy+yz+zx)(x+y+z)}{(x+y)(y+z)(z+x)}} \\
&= 2\cdot\sqrt{\frac{(x+y)(y+z)(z+x)+xyz}{(x+y)(y+z)(z+x)}} \\
&\leq 2\cdot\sqrt{1+\frac{xyz}{(x+y)(y+z)(z+x)}} \\
&\leq 2\cdot\sqrt{1+\frac{1}{8}}=\frac{3}{\sqrt{2}}
\end{aligned}$$

where the last inequality follows from Example 2.1.3.
Here Cauchy-Schwarz was used in the following form:

$$\sqrt{ax}+\sqrt{by}+\sqrt{cz}\leq\sqrt{(a+b+c)(x+y+z)}$$

Exercise 2.1.1. Prove Example 1.1.1 and Exercise 1.1.6 using Cauchy-Scwarz inequality.
Exercise 2.1.2. Let a,b,c,d be positive real numbers. Prove that

$$\frac{a}{b+c}+\frac{b}{c+d}+\frac{c}{d+a}+\frac{d}{a+b}\geq 2$$

Exercise 2.1.3 Let $a_1,a_2,\ldots,a_n$ be positive real numbers. Prove that

$$\frac{a_1^2}{a_2}+\frac{a_2^2}{a_3}+\cdots+\frac{a_n^2}{a_1}\geq a_1+a_2+\cdots+a_n$$

Exercise 2.1.4. (Michael Rozenberg) Let a,b,c,d be positive real numbers such that $a^2+b^2+c^2+d^2=4$. Show that

$$\frac{a^2}{b}+\frac{b^2}{c}+\frac{c^2}{d}+\frac{d^2}{a}\geq 4$$

Exercise 2.1.5. Let a,b,c be positive real numbers. Prove that

$$\left(\frac{a}{a+2b}\right)^2+\left(\frac{b}{b+2c}\right)^2+\left(\frac{c}{c+2a}\right)^2\geq\frac{1}{3}$$

Exercise 2.1.6. (Zhautykov Olympiad 2008) Let a,b,c be positive real numbers such that $abc=1$. Show that

$$\frac{1}{b(a+b)}+\frac{1}{c(b+c)}+\frac{1}{a(c+a)}\geq\frac{3}{2}$$

Exercise 2.1.7. If a,b,c and d are positive real numbers such that $a+b+c+d=4$ prove that

$$\frac{a}{1+b^2c}+\frac{b}{1+c^2d}+\frac{c}{1+d^2a}+\frac{d}{1+a^2b}\geq 2$$

Exercise 2.1.8. Let $a_1,a_2,\ldots,a_n$ and $b_1,b_2,\ldots,b_n$ be real numbers. Prove that

$$\sqrt{a_1^2+b_1^2}+\sqrt{a_2^2+b_2^2}+\cdots+\sqrt{a_n^2+b_n^2}\geq\sqrt{(a_1+a_2+\cdots+a_n)^2+(b_1+b_2+\cdots+b_n)^2}$$

Exercise 2.1.9. (Samin Riasat) Let a,b,c be the side lengths of a triangle. Prove that

$$\frac{a}{3a-b+c}+\frac{b}{3b-c+a}+\frac{c}{3c-a+b}\geq 1$$

Exercise 2.1.10. (Pham Kim Hung) Let a,b,c be positive real numbers such that $a+b+c=1$. Prove that

$$\frac{a}{\sqrt{a+2b}}+\frac{b}{\sqrt{b+2c}}+\frac{c}{\sqrt{c+2a}}<\sqrt{\frac{3}{2}}.$$

Exercise 2.1.11. Let $a,b,c>0$. Prove that

$$\sqrt{\frac{2a}{b+c}}+\sqrt{\frac{2b}{c+a}}+\sqrt{\frac{2c}{a+b}}\leq\sqrt{3\left(\frac{a}{b}+\frac{b}{c}+\frac{c}{a}\right)}.$$

Hölder's inequality is a generalization of the Cauchy-Schwarz inequality. This inequality states:

Hölder's Inequality. Let $a_{i_j}, 1\leq i\leq m, 1\leq j\leq n$ be positive real numbers. Then the following inequality holds

$$\prod_{i=1}^{m}\left(\sum_{j=1}^{n}a_{i_j}\right)\geq\left(\sum_{j=1}^{n}\sqrt[m]{\prod_{i=1}^{m}a_{i_j}}\right)^m.$$

It looks kind of difficult to understand. So for brevity a special case is the following: for positive real numbers a,b,c,p,q,r,x,y,z,

$$\left(a^3+b^3+c^3\right)\left(p^3+q^3+r^3\right)\left(x^3+y^3+z^3\right)\geq(aqx+bqy+crz)^3.$$

Not only Hölder's inequality is a generalization of Cauchy-Schwarz inequality, it is also a direct consequence of the AM-GM inequality, which is demonstrated in the following proof of the special case: by AM-GM,

$$\begin{aligned}3&=\sum\frac{a^3}{a^3+b^3+c^3}+\sum\frac{p^3}{p^3+q^3+r^3}+\sum\frac{x^3}{x^3+y^3+z^3}\\&\geq 3\sum\frac{apx}{\sqrt[3]{(a^3+b^3+c^3)(p^3+q^3+r^3)(x^3+y^3+z^3)}},\end{aligned}$$

which is equivalent to

$$\sqrt[3]{(a^3+b^3+c^3)(p^3+q^3+r^3)(x^3+y^3+z^3)}\geq apx+bqy+crz.$$

Verify that this proof also generalizes to the general inequality, and is similar to the one of the CauchySchwarz inequality. Here are some applications:

Example 2.2.1. (IMO 2001) Let a,b,c be positive real numbers. Prove that

$$\frac{a}{\sqrt{a^2+8bc}}+\frac{b}{\sqrt{b^2+8ca}}+\frac{c}{\sqrt{c^2+8ab}}\geq 1.$$

Solution. By Hölder's inequality,

$$\left(\sum\frac{a}{\sqrt{a^2+8bc}}\right)\left(\sum\frac{a}{\sqrt{a^2+8bc}}\right)\left(\sum a\left(a^2+8bc\right)\right)\geq(a+b+c)^3.$$

Thus we need only show that

$$(a+b+c)^3\geq a^3+b^3+c^3+24abc,$$

which is equivalent to

$$(a+b)(b+c)(c+a)\geq 8abc.$$

This is just Example 1.1.3.

Example 2.2.2. (Vasile Cirtoaje) For $a, b, c > 0$ prove that

$$\sum \frac{a}{\sqrt{a+2b}} \geq \sqrt{a+b+c} \geq \sum \frac{a}{\sqrt{2a+b}}.$$

Solution. For the left part, we have from Hölder's inequality,

$$\left(\sum \frac{a}{\sqrt{a+2b}}\right)\left(\sum \frac{a}{\sqrt{a+2b}}\right)\left(\sum a(a+2b)\right) \geq (a+b+c)^3.$$

Thus

$$\left(\sum \frac{a}{\sqrt{a+2b}}\right)^2 \geq a+b+c$$

Now for the right part, by Cauchy-Schwarz inequality we have

$$\sum \frac{a}{\sqrt{2a+b}} \leq \sqrt{(a+b+c)\left(\sum \frac{a}{2a+b}\right)}$$

So it remains to show that

$$\sum \frac{a}{2a+b} \leq 1$$

which is Example 2.1.5.

Example 2.2.3. (Samin Riasat) Let a, b, c be the side lengths of a triangle. Prove that

$$\frac{1}{8abc+(a+b-c)^3} + \frac{1}{8abc+(b+c-a)^3} + \frac{1}{8abc+(c+a-b)^3} \leq \frac{1}{3abc}.$$

Solution. We have

$$\begin{aligned} & \sum \frac{1}{8abc+(a+b-c)^3} \leq \frac{1}{3abc} \\ \Leftrightarrow & \sum \left(\frac{1}{8abc} - \frac{1}{8abc+(a+b-c)^3}\right) \geq \frac{3}{8abc} - \frac{1}{3abc} \\ \Leftrightarrow & \sum \frac{(a+b-c)^3}{8abc+(a+b-c)^3} \geq \frac{1}{3}. \end{aligned}$$

By Hölder's inequality we obtain

$$\sum \frac{(a+b-c)^3}{8abc+(a+b-c)^3} \geq \frac{(a+b+c)^3}{3\left(24abc+(a+b-c)^3+(a+c-b)^3+(b+c-a)^3\right)} = \frac{1}{3}.$$

In this solution, the following inequality was used: for all positive real numbers a, b, c, x, y, z,

$$\frac{a^3}{x} + \frac{b^3}{y} + \frac{c^3}{z} \geq \frac{(a+b+c)^3}{3(x+y+z)}$$

The proof of this is left to the reader as an exercise.

Example 2.2.4. (IMO Shortlist 2004) If a, b, c are three positive real numbers such that $ab+bc+ca = 1$, prove that

$$\sqrt[3]{\frac{1}{a}+6b} + \sqrt[3]{\frac{1}{b}+6c} + \sqrt[3]{\frac{1}{c}+6a} \leq \frac{1}{abc}$$

Solution. Note that $\frac{1}{a}+6b = \frac{7ab+bc+ca}{a}$. Hence our inequality becomes

$$\sum \sqrt[3]{bc(7ab+bc+ca)} \leq \frac{1}{(abc)^{\frac{2}{3}}}$$

From Hölder's inequality we have

$$\sum \sqrt[3]{bc(7ab+bc+ca)} \leq \sqrt[3]{\left(\sum a\right)^2 \left(9\sum bc\right)}$$

Hence it remains to show that

$$\begin{aligned} &9(a+b+c)^2(ab+bc+ca) \leq \frac{1}{(abc)^2} \\ \Leftrightarrow &[3abc(a+b+c)]^2 \leq (ab+bc+ca)^4, \end{aligned}$$

which is obviously true since

$$(ab+bc+ca)^2 \geq 3abc(a+b+c) \Leftrightarrow \sum a^2(b-c)^2 \geq 0.$$

Another formulation of Hölder's inequality is the following: for positive real numbers $a_i, b_i, p, q (1 \leq i \leq n)$ such that $\frac{1}{p} + \frac{1}{q} = 1$

$$a_1b_1 + a_2b_2 + \cdots + a_nb_n \leq (a_1^p + a_2^p + \cdots + a_n^p)^{\frac{1}{p}} (b_1^q + b_2^q + \cdots + b_n^q)^{\frac{1}{q}}.$$

Exercise 2.2.1. Prove Exercise 2.1.3 using Hölder's inequality.

Exercise 2.2.2. Let a, b, x and y be positive numbers such that $1 \geq a^{11} + b^{11}$ and $1 \geq x^{11} + y^{11}$. Prove that $1 \geq a^5x^6 + b^5y^6$.

Exercise 2.2.3. Prove that for all positive real numbers a, b, c, x, y, z,

$$\frac{a^3}{x} + \frac{b^3}{y} + \frac{c^3}{z} \geq \frac{(a+b+c)^3}{3(x+y+z)}.$$

Exercise 2.2.4. Let a, b, and c be positive real numbers. Prove the inequality

$$\frac{a^6}{b^2+c^2} + \frac{b^6}{a^2+c^2} + \frac{c^6}{a^2+b^2} \geq \frac{abc(a+b+c)}{2}.$$

Exercise 2.2.5. (Kyiv 2006) Let x, y and z be positive numbers such that $xy + xz + yz = 1$. Prove that

$$\frac{x^3}{1+9y^2xz} + \frac{y^3}{1+9z^2yx} + \frac{z^3}{1+9x^2yz} \geq \frac{(x+y+z)^3}{18}.$$

Exercise 2.2.6. Let $a, b, c > 0$. Prove that

$$\frac{ab}{\sqrt{ab+2c^2}} + \frac{bc}{\sqrt{bc+2a^2}} + \frac{ca}{\sqrt{ca+2b^2}} \geq \sqrt{ab+bc+ca}.$$

1.2.4 Rearrangement and Chebyshev's Inequalities

A wonderful inequality is that called the Rearrangement inequality. The statement of the inequality is as follows:

Rearrangement Inequality. Let $(a_i)_{i=1}^n$ and $(b_i)_{i=1}^n$ be sequences of positive numbers increasing or decreasing in the same direction. That is, either $a_1 \geq a_2 \geq \cdots \geq a_n$ and $b_1 \geq b_2 \geq \cdots \geq b_n$ or $a_1 \leq a_2 \leq \cdots \leq a_n$ and $b_1 \leq b_2 \leq \cdots \leq b_n$. Then for any permutation (c_n) of the numbers (b_n) we have the following inequalities

$$\sum_{i=1}^n a_ib_i \geq \sum_{i=1}^n a_ic_i \geq \sum_{i=1}^n a_ib_{n-i+1}.$$

That is, the maximum of the sum occurs when the two sequences are similarly sorted, and the minimum occurs when they are oppositely sorted.

Proof. Let S denote the sum $a_1b_1 + a_2b_2 + \cdots + a_nb_n$ and S' denote the sum $a_1b_1 + a_2b_2 + \cdots + a_xb_y + \cdots + a_yb_x + \cdots + a_nb_n$. Then

$$S - S' = a_xb_x + a_yb_y - a_xb_y - a_yb_x = (a_x - a_y)(b_x - b_y) \geq 0$$

since both of $a_x - a_y$ and $b_x - b_y$ are either positive, or negative, as the sequences are similarly sorted. Hence the sum gets smaller whenever any two of the terms alter. This implies that the maximum must occur when the sequences are sorted similarly. The other part of the inequality follows in a quite similar manner and is left to the reader.

A useful technique. Let $f(a_1, a_2, \ldots, a_n)$ be a symmetric expression in $a_1, a_2, \ldots, a_n$. That is, for any permutation $a_1', a_2', \ldots, a_n'$ we have $f(a_1, a_2, \ldots, a_n) = f(a_1', a_2', \ldots, a_n')$. Then in order to prove $f(a_1, a_2, \ldots, a_n) \geq 0$ we may assume, without loss of generality, that $a_1 \geq a_2 \geq \cdots \geq a_n$. The reason we can do so is because f remains invariant under any permutation of the a_i 's. This assumption is quite useful sometimes; check out the following examples:

Example 3.1.1. Let a, b, c be real numbers. Prove that

$$a^2 + b^2 + c^2 \geq ab + bc + ca$$

Solution. We may assume, WLOG [1], that $a \geq b \geq c \geq 0$, since the signs of a, b, c does not affect the left side of the inequality. Applying the Rearrangement inequality for the sequences (a, b, c) and (a, b, c) we conclude that

$$\begin{gathered} a \cdot a + b \cdot b + c \cdot c \geq a \cdot b + b \cdot c + c \cdot a \\ \Longrightarrow a^2 + b^2 + c^2 \geq ab + bc + ca. \end{gathered}$$

Example 3.1.2. For positive real numbers a, b, c prove that

$$a^3 + b^3 + c^3 \geq a^2 b + b^2 c + c^2 a.$$

Solution. WLOG let $a \geq b \geq c$. Applying Rearrangement inequality for $\left(a^2, b^2, c^2\right)$ and (a, b, c) we conclude that

$$a^2 \cdot a + b^2 \cdot b + c^2 \cdot c \geq a^2 \cdot b + b^2 \cdot c + c^2 \cdot a$$

Example 3.1.3. (Nesbitt's inequality) For positive real numbers a, b, c prove that

$$\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} \geq \frac{3}{2}$$

Solution. Since the inequality is symmetric in a, b, c we may WLOG assume that $a \geq b \geq c$. Then verify that $b + c \leq c + a \leq a + b$ i.e. $\frac{1}{b+c} \geq \frac{1}{c+a} \geq \frac{1}{a+b}$. Now applying the Rearrangement inequality for the sequences (a, b, c) and $\left(\frac{1}{b+c}, \frac{1}{c+a}, \frac{1}{a+b}\right)$ we conclude that

$$\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} \geq \frac{b}{b+c} + \frac{c}{c+a} + \frac{a}{a+b},$$

and

$$\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} \geq \frac{c}{b+c} + \frac{a}{c+a} + \frac{b}{a+b}.$$

Adding the above inequalities we get

$$2\left(\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b}\right) \geq \frac{b+c}{b+c} + \frac{c+a}{c+a} + \frac{a+b}{a+b} = 3.$$

which was what we wanted.

Example 3.1.4 (IMO 1975) We consider two sequences of real numbers $x_1 \geq x_2 \geq \ldots \geq x_n$ and $y_1 \geq y_2 \geq \ldots \geq y_n$. Let $z_1, z_2, \ldots, z_n$ be a permutation of the numbers $y_1, y_2, \ldots, y_n$. Prove that

$$\sum_{i=1}^{n} (x_i - y_i)^2 \leq \sum_{i=1}^{n} (x_i - z_i)^2.$$

Solution. Expanding and using the fact that $\sum y_i^2 = \sum z_i^2$, we are left to prove that

$$\sum_{i=1}^{n} x_i y_i \geq \sum_{i=1}^{n} x_i z_i$$

[1]WLOG = Without loss of generality. which is the Rearrangement inequality.
Example 3.1.5. (Rearrangement inequality in Exponential form) Let $a, b, c \geq 1$. Prove that

$$a^a b^b c^c \geq a^b b^c c^a$$

First Solution. First assume that $a \geq b \geq c \geq 1$. Then

$$a^a b^b c^c \geq a^b b^c c^a$$
$$\Leftrightarrow a^{a-b} b^{b-c} \geq c^{a-b} c^{b-c},$$

which is true, since $a^{a-b} \geq c^{a-b}$ and $b^{b-c} \geq c^{b-c}$.
Now let $1 \leq a \leq b \leq c$. Then

$$a^a b^b c^c \geq a^b b^c c^a$$
$$\Leftrightarrow c^{c-b} c^{b-a} \geq b^{c-b} a^{c-a},$$

which is also true. Hence the inequality holds in all cases.
Second Solution. Here is another useful argument: take ln on both sides

$$a \ln a + b \ln b + c \ln c \geq a \ln b + b \ln c + c \ln a.$$

It is now clear that this holds by Rearrangement since the sequences (a, b, c) and $(\ln a, \ln b, \ln c)$ are sorted similarly.

Note that the inequality holds even if $a, b, c > 0$, and in this case the first solution works but the second solution needs some treatment which is left to the reader to fix.
Example 3.1.6. Let $a, b, c \geq 0$. Prove that

$$a^3 + b^3 + c^3 \geq 3abc$$

Solution. Applying the Rearrangement inequality for $(a, b, c), (a, b, c), (a, b, c)$ we conclude that

$$a \cdot a \cdot a + b \cdot b \cdot b + c \cdot c \cdot c \geq a \cdot b \cdot c + b \cdot c \cdot a + c \cdot a \cdot b.$$

In the same way as above, we can prove the AM-GM inequality for n variables for any $n \geq 2$. This demonstrates how strong the Rearrangement inequality is. Also check out the following example, illustrating the strength of Rearrangement inequality:
Example 3.1.7 (Samin Riasat) Let a, b, c be positive real numbers. Prove that

$$\left(\sum_{cyc} \frac{a}{b+c}\right)^2 \leq \left(\sum_{cyc} \frac{a^2}{b^2+bc}\right)\left(\sum_{cyc} \frac{a}{c+a}\right).$$

Solution. Note that the sequences $\left(\sqrt{\frac{a^3}{b+c}}, \sqrt{\frac{b^3}{c+a}}, \sqrt{\frac{c^3}{a+b}}\right)$ and $\left(\sqrt{\frac{1}{ca+ab}}, \sqrt{\frac{1}{ab+bc}}, \sqrt{\frac{1}{bc+ca}}\right)$ are oppositely sorted. Therefore by Rearrangement inequality we get

$$\sum \frac{a}{b+c} = \sum \sqrt{\frac{a^3}{b+c}} \cdot \sqrt{\frac{1}{ca+ab}} \leq \sum \sqrt{\frac{a^3}{b+c}} \cdot \sqrt{\frac{1}{ab+bc}}.$$

Now from Cauchy-Schwarz inequality

$$\sum \sqrt{\frac{a^3}{b+c}} \cdot \sqrt{\frac{1}{ab+bc}} = \sum \sqrt{\frac{a^2}{b(b+c)}} \cdot \sqrt{\frac{a}{c+a}} \leq \sqrt{\left(\sum \frac{a^2}{b(b+c)}\right)\left(\sum \frac{a}{c+a}\right)}$$

which was what we wanted.

Can you generalize the above inequality?

Exercise 3.1.1. Prove Example 1.1.4 using Rearrangement inequality.

Exercise 3.1.2. For $a, b, c > 0$ prove that

$$\frac{ab}{c} + \frac{bc}{a} + \frac{ca}{b} \geq a + b + c$$

Exercise 3.1.3. Let $a, b, c > 0$. Prove that

$$\frac{a^8 + b^8 + c^8}{a^3 b^3 c^3} \geq \frac{1}{a} + \frac{1}{b} + \frac{1}{c}$$

Exercise 3.1.4. Prove Exercise 2.1.3 using Rearrangement inequality.

Exercise 3.1.5. Let a, b, c be positive real numbers. Prove that

$$\frac{a}{b(b+c)} + \frac{b}{c(c+a)} + \frac{c}{a(a+b)} \geq \frac{1}{b+c} + \frac{1}{c+a} + \frac{1}{a+b}.$$

Exercise 3.1.6. (Yaroslavle 2006) Let $a > 0, b > 0$ and $ab = 1$. Prove that

$$\frac{a}{a^2+3} + \frac{b}{b^2+3} \leq \frac{1}{2}$$

Exercise 3.1.7. Let a, b, c be positive real numbers satisfying $abc = 1$. Prove that

$$ab^2 + bc^2 + ca^2 \geq a + b + c.$$

Exercise 3.1.8. Let a, b, c be positive real numbers such that $a + b + c = 1$. Prove that

$$\frac{ab+c}{a+b} + \frac{ac+b}{a+c} + \frac{bc+a}{b+c} \geq 2$$

Exercise 3.1.9. (Novosibirsk 2007) Let a and b be positive numbers, and $n \in \mathbb{N}$. Prove that

$$(n+1)\left(a^{n+1} + b^{n+1}\right) \geq (a+b)\left(a^n + a^{n-1}b + \cdots + b^n\right).$$

Chebyshev's inequality

Chebyshev's inequality is a direct consequence of the Rearangement inquality. The statement is as follows:

Chebyshev's Inequality. Let $(a_i)_{i=1}^n$ and $(b_i)_{i=1}^n$ be two sequences of positive real numbers.

(i) If the sequences are similarly sorted, then

$$\frac{a_1b_1 + a_2b_2 + \cdots + a_nb_n}{n} \geq \frac{a_1 + a_2 + \cdots + a_n}{n} \cdot \frac{b_1 + b_2 + \cdots + b_n}{n}.$$

(ii) If the sequences are oppositely sorted, then

$$\frac{a_1b_1 + a_2b_2 + \cdots + a_nb_n}{n} \leq \frac{a_1 + a_2 + \cdots + a_n}{n} \cdot \frac{b_1 + b_2 + \cdots + b_n}{n}.$$

Proof. We will only prove (3.1). Since the sequences are similarly sorted, Rearrangement inequality implies

$$\begin{aligned}
a_1b_1 + a_2b_2 + \cdots + a_nb_n &= a_1b_1 + a_2b_2 + \cdots + a_nb_n,\\
a_1b_1 + a_2b_2 + \cdots + a_nb_n &\geq a_1b_2 + a_2b_3 + \cdots + a_nb_1,\\
a_1b_1 + a_2b_2 + \cdots + a_nb_n &\geq a_1b_3 + a_2b_4 + \cdots + a_nb_2,\\
&\vdots\\
a_1b_1 + a_2b_2 + \cdots + a_nb_n &\geq a_1b_n + a_2b_1 + \cdots + a_nb_{n-1}.
\end{aligned}$$

Adding the above inequalities we get

$$n\left(a_1b_1+a_2b_2+\cdots+a_nb_n\right)\geq\left(a_1+a_2+\cdots+a_n\right)\left(b_1+b_2+\cdots+b_n\right),$$

which was what we wanted.

Example 3.2.1. For $a,b,c>0$ prove that

$$3\left(a^2+b^2+c^2\right)\geq(a+b+c)^2.$$

Solution. Applying Chebyshev's inequality for (a,b,c) and (a,b,c) we conclude that

$$3(a\cdot a+b\cdot b+c\cdot c)\geq(a+b+c)(a+b+c).$$

Example 3.2.2. Let $a,b,c>0$. Prove that

$$\frac{a^8+b^8+c^8}{a^3b^3c^3}\geq\frac{1}{a}+\frac{1}{b}+\frac{1}{c}.$$

Solution. From Chebyshev's inequality we conclude that

$$\begin{aligned}3\left(a^8+b^8+c^8\right)&\geq\left(a^6+b^6+c^6\right)\left(a^2+b^2+c^2\right)\\&\geq 3a^2b^2c^2\left(a^2+b^2+c^2\right)\\&\geq 3a^2b^2c^2(ab+bc+ca),\end{aligned}$$

hence

$$\frac{a^8+b^8+c^8}{a^3b^3c^3}\geq\frac{ab+bc+ca}{abc}=\frac{1}{a}+\frac{1}{b}+\frac{1}{c}$$

Example 3.2.3. Let $a\geq b\geq c\geq 0$ and $0\leq x\leq y\leq z$. Prove that

$$\frac{a}{x}+\frac{b}{y}+\frac{c}{z}\geq\frac{a+b+c}{\sqrt[3]{xyz}}\geq 3\left(\frac{a+b+c}{x+y+z}\right).$$

Solution. Applying Chebyshev's inequality for $a\geq b\geq c$ and $\frac{1}{x}\geq\frac{1}{y}\geq\frac{1}{z}$ we deduce that

$$3\left(\frac{a}{x}+\frac{b}{y}+\frac{c}{z}\right)\geq(a+b+c)\left(\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\right)\geq\frac{3(a+b+c)}{\sqrt[3]{xyz}}\geq 9\left(\frac{a+b+c}{x+y+z}\right),$$

which was what we wanted. Here the last two inequalities follow from AM-GM.

Example 3.2.4. Let $a,b,c>0$. Prove that

$$\frac{a^3}{bc}+\frac{b^3}{ca}+\frac{c^3}{ab}\geq a+b+c$$

Solution. WLOG assume that $a\geq b\geq c$. Then $a^3\geq b^3\geq c^3$ and $bc\leq ca\leq ab$. Hence using (3.3) and (3.1) we conclude that

$$\sum\frac{a^3}{bc}\geq\frac{3\left(a^3+b^3+c^3\right)}{ab+bc+ca}\geq\frac{(a+b+c)\left(a^2+b^2+c^2\right)}{ab+bc+ca}\geq a+b+c.$$

Exercise 3.2.1. Prove the second Chebyshev's inequality (3.2).

Exercise 3.2.2. Let $a_1,a_2,\ldots,a_n\geq 0$ and $k\geq 1$. Prove that

$$\sqrt[k]{\frac{a_1^k+a_2^k+\cdots+a_n^k}{n}}\geq\frac{a_1+a_2+\cdots+a_n}{n}$$

Exercise 3.2.3. Deduce a proof of Nesbitt's inequality from Chebyshev's inequality. (Hint: you may use Example 3.2.3)

Exercise 3.2.4. Let $a_1\geq a_2\geq\cdots\geq a_n$ and $b_1\leq b_2\leq\cdots\leq b_n$ be positive. Prove that

$$\sum_{i=1}^{n}\frac{a_i}{b_i}\geq\frac{a_1+a_2+\cdots+a_n}{\sqrt[n]{b_1b_2\ldots b_n}}\geq\frac{n\left(a_1+a_2+\cdots+a_n\right)}{b_1+b_2+\cdots+b_n}.$$

Exercise 3.2.5. Let $a \geq c \geq 0$ and $b \geq d \geq 0$. Prove that

$$(a+b+c+d)^2 \geq 8(ad+bc).$$

Exercise 3.2.6. (Radu Titiu) Let $a, b, c > 0$ such that $a^2+b^2+c^2 \geq 3$. Show that

$$\frac{a^2}{b+c}+\frac{b^2}{c+a}+\frac{c^2}{a+b} \geq \frac{3}{2}$$

1.3 FUNCTIONAL EQUATION

A functional equation is an equation whose variables are ranging over functions and our aim is to find all possible functions satisfying the equation. [3]

There is no fixed method to solve a functional equation few standard approaches as follows:

1.3.1 Substitution of Variable/Function

This is most common method for solving functional equations. By substitution we get simplified form or some time some additional information regarding equation. We replace old variable with new variable by keeping domain of old variable unchanged. See the following examples: Example I Let $f : \mathbb{R} \backslash \{0\} \rightarrow \mathbb{R}$ be such that $f\left(1+\frac{1}{x}\right)=x^2+\frac{1}{x^2} \quad \forall x \in \mathbb{R} \backslash \{0\}$, find $f(x)$.

Solution: Let $y=1+\frac{1}{x} \Rightarrow x=\frac{1}{y-1}$

$\Rightarrow \quad f(y)=\left(\frac{1}{y-1}\right)^2+(y-1)^2 \quad \forall y \in \mathbb{R}-\{1\}$.

Example 2 Let p, q be fixed non-zero real numbers. Find all function $f : \mathbb{R} \rightarrow \mathbb{R}$ such that $f\left(x-\frac{q}{p}\right)+2x \leq \frac{p}{q}x^2+\frac{2q}{p} \leq f\left(x+\frac{q}{p}\right)-2x \forall x \in \mathbb{R}$.

Solution: Substitute $x-\frac{q}{p}=y$ in left inequality, we get $f(y) \leq \frac{p}{q}y^2+\frac{q}{p}$

Similarly substituting $x+\frac{q}{p}=y$ in right inequality, we get $f(y) \geq \frac{p}{q}y^2+\frac{q}{p}$

From Inequations (1) and (2), we get

$f(y)=\frac{p}{q}y^2+\frac{q}{p} \quad \forall y \in \mathbb{R}$.

Example $3 f : \mathbb{R} \backslash \{0\} \rightarrow \mathbb{R}$ such that $2f(x)+3f\left(\frac{1}{x}\right)=x \forall x \in \mathbb{R} \backslash \{0\}$, find $f(x)$.

Solution: Replace x by $\frac{1}{x}$, we get $2f\left(\frac{1}{x}\right)+3f(x)=\frac{1}{x}$

Now by eliminating $f\left(\frac{1}{x}\right)$ from the two equations, we get

$(9-4)f(x)=\frac{3}{x}-2x$

$\Rightarrow f(x)=\frac{3-2x^2}{5x}$.

Example 4 Find all functions $f : \mathbb{R} \rightarrow \mathbb{R}$ such that $x^2 f(x)+f(1-x)=2x-x^4 \forall x \in \mathbb{R}$.

Solution: Replace x by $(1-x)$, we get

$(1-x)^2 f(1-x)+f(x)=2(1-x)-(1-x)^4$

Now eliminating $f(1-x)$ from the two equations, we get $f(x)=1-x^2$. Charles Babbage

26 Dec 179 | −18 Oct 187 | Nationality: British Example 5 $\quad f : \mathbb{R}-\{0,1\} \rightarrow \mathbb{R}, f(x)+f\left(\frac{x-1}{x}\right)=1+x$ find $f(x)$

Solution: Replacing x by $\frac{x-1}{x}$, we get

$$f\left(\frac{x-1}{x}\right)+f\left(\frac{\frac{x-1}{x}-1}{\frac{x-1}{x}}\right)=1+\frac{x-1}{x}$$

$$\text{or } f\left(\frac{x-1}{x}\right)+f\left(\frac{1}{1-x}\right)=\frac{2x-1}{x}$$

again replacing x by $\frac{1}{1-x}$ in parent equation, we get

$$\begin{aligned}
&f\left(\frac{1}{1-x}\right)+f\left(\frac{\frac{1}{1-x}-1}{\frac{1}{1-x}}\right)=1+\frac{1}{1-x}=\frac{2-x}{1-x}\\
&f\left(\frac{1}{1-x}\right)+f(x)=\frac{2-x}{1-x}
\end{aligned}$$

By adding parent equation + Eq. (2) and subtracting Eq. (1), we get

$$2f(x)=1+x+\frac{2-x}{1-x}-\frac{2x-1}{x}\Rightarrow f(x)=\frac{x^3-x^2-1}{2x(x-1)}$$

1.3.2 Isolation of Variables

We try to bring all functions of x to one side and all functions of y on other side. For some particular type of problems this works wonderfully. See the following examples:

Example 6: Find $f(x)$ such that $xf(y)=yf(x)\forall x,y\in\mathbb{R}-\{0\}$.

Solution: $xf(y)=yf(x)$

$$\Rightarrow\frac{f(x)}{x}=\frac{f(y)}{y}$$

as x,y are independent of each other

$$\begin{aligned}
&\Rightarrow\frac{f(x)}{x}=\text{ Constant }=c\\
&\Rightarrow f(x)=cx.
\end{aligned}$$

Example 7 If $(x-y)f(x+y)-(x+y)f(x-y)=4xy\left(x^2-y^2\right)\forall x,y\in\mathbb{R}$, find $f(x)$.

Solution: Given equation is equivalent to

$$\begin{aligned}
&\frac{f(x+y)}{x+y}-\frac{f(x-y)}{x-y}=4xy\\
&=(x+y)^2+(x-y)^2\\
&\Rightarrow\frac{f(x+y)}{x+y}-(x+y)^2=\frac{f(x-y)}{x-y}-(x-y)^2\\
&\Rightarrow\frac{f(t)}{t}-t^2\text{ is constant}
\end{aligned}$$

Let $\frac{f(x)}{x}-x^2=c\Rightarrow f(x)=x^2+cx$.

which satisfies the parent equation.

Exercises

1. Find $f:\mathbb{R}\backslash\{0,1\}\to\mathbb{R}$, such that

$$f\left(\frac{x}{x-1}\right)=2f\left(\frac{x-1}{x}\right)\forall x\in\mathbb{R}\backslash\{0,1\}.$$

2. Find $f:\mathbb{R}\backslash\{0,1\}\to\mathbb{R}$, such that

$$f(x)+f\left(\frac{1}{1-x}\right)=x\forall x\in\mathbb{R}\backslash\{0,1\}.$$

3. $f\left(x^2+x\right)+2f\left(x^2-3x+2\right)=9x^2-15x\forall x\in\mathbb{R}$, find $f(2016)$.

4. Find $f:\mathbb{R}\to\mathbb{R}$, such that $f(x)+xf(1-x)=1+x\forall x\in\mathbb{R}$.

5. $f:\mathbb{R}\to\mathbb{R}, f(x+y)+f(x-y)=2f(x)\cos y \forall x,y\in\mathbb{R}$, find all such functions.

6. Find all functions $f:\mathbb{R}\backslash\{0,1\}\to\mathbb{R}$, such that

$$f(x)+f\left(\frac{1}{1-x}\right)=\frac{2(1-2x)}{x(1-x)}\forall x\in\mathbb{R}\backslash\{0,1\}.$$

7. Find all functions $f:\mathbb{R}\backslash\{0,1\}\to\mathbb{R}$, such that

$$f(x)+2f\left(\frac{1}{x}\right)+3f\left(\frac{x}{x-1}\right)=x.$$

1.3.3 Evaluation of Function at Some Point of Domain

We try to determine the unknown function at points $0,1,-1$, etc, which is mostly crucial to simplify the complex functional equation. Observe the following examples:

Example 8 Find all functions $f:\mathbb{R}\to\mathbb{R}$ such that
$f(xf(x)+f(y))=(f(x))^2+y\forall x,y\in\mathbb{R}$.
Solution: Let $P(x,y): f(xf(x)+f(y))=(f(x))^2+y$
$P(0,x): f(f(x))=(f(0))^2+x$
Let $f(0)=a\Rightarrow f(f(x))=x+a^2$
at $x=-a^2, f\left(f\left(-a^2\right)\right)=0$
Let $f\left(-a^2\right)=b$
$\Rightarrow f(b)=0$
$P(b,b): f(bf(b)+f(b))=(f(b))^2+b$
$\Rightarrow f(b(0)+0)=0^2+b$
$\Rightarrow f(0)=b$
Also $P(0,b): f(0\cdot f(0)+f(b))=(f(0))^2+b$
$f(0)=(f(0))^2+b$
$\Rightarrow (f(0))^2=0\quad(\text{as } f(0)=b)$
$\Rightarrow f(0)=0\Rightarrow a=0$
From Eq. (1), we get $f(f(x))=x\forall x\in\mathbb{R}$
Also from $P(x,0): f(xf(x))=(f(x))^2$
Replace x by $f(x)$ in Eq. (3) We get, $f(f(x)\cdot f(x))=(f(f(x)))^2$
$\Rightarrow f(f(x)x)=x^2$ (from Eq. (2))
From Eqs. (3) and (4), we get
$(f(x))^2=x^2$
$\Rightarrow f(x)=x$ or $-x$
Now we will prove either $f(x)=x\forall x\in\mathbb{R}$ or $f(x)=-x\forall x\in\mathbb{R}$.
If possible let $f\left(x_1\right)=x_1$ and $f\left(x_2\right)=-x_2, x_1\neq x_2$
$P\left(x_1,x_2\right): f\left(x_1f\left(x_1\right)+f\left(x_2\right)\right)=\left(f\left(x_1\right)\right)^2+x_2$
$f\left(x_1^2-x_2\right)=x_1^2+x_2$
$\Rightarrow\pm\left(x_1^2-x_2\right)=x_1^2+x_2$
$+$ve, ${x_1}^2+x_2={x_1}^2+x_2\Rightarrow x_2=0$
-ve, $-x_1^2+x_2=x_1^2+x_2\Rightarrow x_1^2=0$
$\Rightarrow x_1=0$
Hence either $f(x)=x\forall x\in\mathbb{R}$
or, $f(x)=-x\forall x\in\mathbb{R}$.
Example 9$f:\mathbb{N}_0\to\mathbb{N}_0$ such that
$f\left(x^2+f(y)\right)=xf(x)+y\forall x,y\in\mathbb{N}_0$.
Solution: $P(x,y): f\left(x^2+f(y)\right)=xf(x)+y$
$P(0,x): f(f(x))=x\forall x\in\mathbb{N}_0$
$P(1,0): f(1+f(0))=f(1)$

$\Rightarrow f(f(1+f(0)))=f(f(1))$
(taking f on both side of Eq. (2))
$\Rightarrow 1+f(0)=1$
(using Eq. (1))
$\Rightarrow f(0)=0$
$P(1, f(x)): f\left(1^2+f(f(x))\right)=1 \cdot f(1)+f(x)$
$\Rightarrow f(1+x)=a+f(x)(\text{Let } f(1)=a)$
$f(x+1)-f(x)=a$
Plugging $x=0,1,2, \ldots, n-1$ in Eq. (3) and adding all, we get
$f(n)=n a \forall n \in \mathbb{N}_0$
Checking it in parent equation, we get
$a\left(x^2+a y\right)=a x^2+y$
$\Rightarrow a^2 y=y \Rightarrow a^2=1 \Rightarrow a= \pm 1$
But $a=-1$, not possible as co-domain $=\mathbb{N}_0$.
$\Rightarrow f(n)=n$.
Example 10 Find all functions $f: \mathbb{R} \rightarrow \mathbb{R}$, such that
$f(f(x+y))=f(x+y)+f(x) \cdot f(y)-x y \forall x, y \in \mathbb{R}$.
Solution: $P(x, y): f(f(x+y))=f(x+y)+f(x) \cdot f(y)-x y$
$P(x, 0): f(f(x))=f(x)(1+f(0))$
Let $f(x)=t$
$\Rightarrow f(t)=(1+f(0)) t$
When $t \in$ image set of f
$\Rightarrow f(f(x+y))=(1+f(0)) f(x+y)$
$\Rightarrow f(x+y)+f(x) \cdot f(y)-x y=(1+f(0)) f(x+y)$
$\Rightarrow f(x) \cdot f(y)-x y=f(0) \cdot f(x+y)$ Let $f(0)=a, x=-a$ and $y=a$ in Eq. (2)
$f(a) \cdot f(-a)+a^2=a^2$
$\Rightarrow f(a) \cdot f(-a)=0$
$\Rightarrow 0 \in I_m(f)$
From Eq. (1), we get
$f(0)=(1+f(0)) \cdot 0=0$
Using this in Eq. (2), we get
$f(x) \cdot f(y)=x y$
$\Rightarrow(f(1))^2=1 \Rightarrow f(1)= \pm 1$
$\Rightarrow f(x)=x$ or $-x$
But $f(x)=x$ only satisfy the parent equation.

1.3.4 Application of Properties of the Function

Sometime investigating for injectivity or surjectivity of function involved in the equation is very useful in order to determine it. Sometime identifying function as monotonous reduces the complexity of the problem at great length. See the following examples:

Example II Let $f: \mathbb{Z} \rightarrow \mathbb{Z}$ satisfies
$f(f(n)+2)=n \forall n \in \mathbb{Z}, f(1)=0$ find $f(n)$.
Solution: Let $f(n)+2=g(n)$
$\Rightarrow f(g(n))=n$
as $f \circ g$ is one to one and onto function, g is one to one and f must be onto. As $g(n)=f(n)+2 \Rightarrow f$ is one to one function and $g(n)$ is onto also $\Rightarrow f$ and g are inverse of each other.
As $f(1)=0 \Rightarrow g(0)=1 \Rightarrow f(0)+2=g(0)=1$
$\Rightarrow f(0)=-1$
from $f(n)+2=g(n)$, we get
$f(f(n))+2=g(f(n))=n$
$\Rightarrow n=f(f(n))+2$
Replacing n by $f(n+2)$, we get
$f(n+2)=f(f(f(n+2)))+2$

$= f(n+2-2)+2 \quad (\text{as } f(f(n)) = n-2)$
$\Rightarrow f(n+2) = f(n)+2$
$\Rightarrow f(n+2) - f(n) = 2$
using telescoping sum we get
$\Rightarrow f(n) = n-1 \quad (\text{ as } f(0) = -1, f(1) = 0)$
Example 12 Find all functions $f : \mathbb{R} \to \mathbb{R}$ that have the following two properties:
$f(f(x)) = x \forall x \in \mathbb{R}$ and $x \geq y$ then $f(x) \geq f(y)$.
Solution: Fix any number $x \in \mathbb{R}$ and Let $y = f(x)$.
From first property $f(y) = x$
Let $x \neq y, \Rightarrow x < y$ or $x > y$
Case 1: $x < y \Rightarrow f(x) \leq f(y)$
$\Rightarrow y \leq x$ contradiction
Case 2: $y < x \Rightarrow f(y) \leq f(x)$
$\Rightarrow x \leq y$ contradiction
Hence $x = y \Rightarrow f(x) = x \forall x \in \mathbb{R}$. Example 13 Prove that there is no function
$f : \mathbb{N}_0 \to \mathbb{N}_0$ such that $f(f(n)) = n + 1987$
Solution: f must be injective (if it exists)
Let $x \neq y, f(x) = f(y)$
$\Rightarrow f(f(x)) = f(f(y))$
$\Rightarrow x + 1987 = y + 1997$
$\Rightarrow x = y$ Contradiction.
$\Rightarrow f$ must be injective.

Let $f(n)$ misses exactly k distinct values $C_1, C_2, \ldots, C_k$ in $\mathbb{N}_0$, i.e., $f(n) \neq C_1, C_2, \ldots, C_k \ \forall n \in \mathbb{N}_0$, then $f(f(n))$ misses the $2k$ distinct values $C_1, C_2, \ldots, C_k$ and $f(C_1), f(C_2), \ldots, f(C_k)$ in $\mathbb{N}_0$ (No two $f(C_i)$ is equal as f is one to one function). Let $y \in \mathbb{N}_0$ and $y \neq C_1, C_2, \ldots, C_k, f(C_1), f(C_2), \ldots, f(C_k)$, then there exist $x \in \mathbb{N}_0$ such that $f(x) = y$. Since $y \neq f(C_j), x \neq C_j$, so there is $n \in \mathbb{N}_0$ such that $f(n) = x$, then $f(f(n)) = y$.

This implies $f(f(n))$ misses only the $2k$ values $C_1, C_2, \ldots, C_k, f(C_1), f(C_2), \ldots, f(C_k)$ and no others since $n + 1987$ misses the 1987 values $0, 1, \ldots, 1986$ and $2k \neq 1987$ this is a contradiction.

1.3.5 Application of Mathematical Induction

Many functional equation on natural number or on integer can be solved using induction, sometimes it is also applicable in case of rational numbers. See the following examples:

Example 14 Let $f : \mathbb{N} \to \mathbb{N}$ be a function such that $f(n+1) > f(f(n)) \forall n \in \mathbb{N}$.

Prove that $f(n) = n \forall n \in \mathbb{N}$.

Solution: Our claim is $f(1) < f(2) < f(3) < \ldots$. This follows if we can show that, for every $n > 1, f(n)$ is the unique smallest element of $\{f(n), f(n+1), f(n+1), \ldots\}$.

Let us apply introduction on n.

Firstly for $m \geq 2, f(m) \geq f(f(m-1))$. Since $f(m-1) \in \{1, 2, 3, \ldots\}$, this mean that $f(m)$ cannot be the smallest of $\{f(1), f(2), f(3), \ldots\}$.

Since $\{f(1), f(2), \ldots\}$ is bounded below by 1 , it follows that $f(1)$ must be the unique smallest element of $\{f(1), f(2), f(3), \ldots\}$.

Now suppose that $f(n)$ is the smallest of $\{f(n), f(n+1), \ldots\}$. Let $m > n+1$. By the induction hypothesis, $f(m-1) > f(n)$. Since $f(n) > f(n-1) > \ldots > f(1) \geq 1$, we have $f(n) \geq n$ and so $f(m-1) \geq n+1$, so $f(m-1) \in \{n+1, n+2, \ldots\}$.

But $f(m) > f(f(m-1))$, so $f(m)$ is not smallest in $\{f(n+1), f(n+2), \ldots\}$. Since $\{f(n+1), f(n+2), \ldots\}$ is bounded below, it follows that $f(n+1)$ is the unique smallest element of $\{f(n+1), f(n+2), \ldots\}$.

Now since, $1 \leq f(1) < f(2) < f(3) < \ldots$, clearly we have $f(n) \geq n \forall n \in \mathbb{N}$. But if $f(n) > n$ for some n, then $f(f(n)) > f(n+1)$ a contradiction. Hence $f(n) = n \forall \mathbb{N}$.

Example 15 Let $f : \mathbb{Q} \to \mathbb{Q}$, such that $f(1) = 2$ and $f(xy) = f(x) \cdot f(y) - f(x+y) + 1$, find $f(x)$.

Solution: Putting $y = 1$, then

$$\begin{aligned}f(x) &= f(x)\cdot f(1) - f(x+1) + 1\\ &= 2f(x) - f(x+1) + 1\\ &\Rightarrow f(x+1) = f(x) + 1\end{aligned}$$

Therefore by applying condition $f(1) = 2$ and by mathematical induction, for all integer n, we have $f(x) = x + 1$. For any rational number, let $x = \frac{m}{n}$ where $m, n \in \mathbb{Z}$ and $n \neq 0$, putting $x = \frac{m}{n}, y = n$ then

$$\begin{aligned}&f\left(\frac{m}{n}\cdot n\right) = f\left(\frac{m}{n}\right)\cdot f(n) - f\left(\frac{m}{n}+n\right) + 1\\ &f(m) = f\left(\frac{m}{n}\right)(n+1) - f\left(\frac{m}{n}+n\right) + 1\\ &m+1 = f\left(\frac{m}{n}\right)(n+1) - f\left(\frac{m}{n}\right) - n + 1 \quad (\text{ as } f(x+1) = f(x) + 1 \forall x \in \mathbb{Q})\\ &\Rightarrow nf\left(\frac{m}{n}\right) = n + m\\ &\text{or } f\left(\frac{m}{n}\right) = 1 + \frac{m}{n}\\ &\Rightarrow f(x) = x + 1 \forall x \in \mathbb{Q}.\end{aligned}$$

Exercises

1. The function f is defined for all real numbers and satisfies $f(x) \leq x$ and $f(x+y) \leq f(x) + f(y)$ for all real x, y. Prove that $f(x) = x$ for every real number x.

2. Let R denote the real numbers and $f : \mathbb{R} \to [-1, 1]$ satisfy

$$f\left(x + \frac{13}{42}\right) + f(x) = f\left(x + \frac{1}{6}\right) + f\left(x + \frac{1}{7}\right)$$

for every $x \in \mathbb{R}$. Show that f is a periodic function, i.e., there is a non-zero real number T such that $f(x+T) = f(x)$ for every $x \in \mathbb{R}$. [IMO Shortlisted Problem, 1996]

3. Find all functions $f : \mathbb{R} \to \mathbb{R}$ such that $f(f(x+y)) = f(x+y) + f(x)f(y) - xy$ for all $x, y \in \mathbb{R}$.

4. Find all functions $f : \mathbb{R} \to \mathbb{R}$ such that $f((x + yf(x)) = f(x) + xf(y)$ for all x, y in $\mathbb{R}$.

5. Let $f : \mathbb{R} \to \mathbb{R}$ be a continuous function such that $f(f(x)) + f(x) + x = 0 \forall x \in \mathbb{R}$. Find all such $f(x)$.

1.4 POLYNOMIAL FUNCTIONS

Any function, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, is a polynomial function in ' x ' where $a_i (i = 0, 1, 2, 3, \ldots, n)$ is a constant which belongs to the set of real numbers and sometimes to the set of complex numbers, and the indices, $n, n-1, \ldots, 1$ are natural numbers. If $a_n \neq 0$, then we can say that $f(x)$ is a polynomial of degree n. a_n is called leading coefficient of the polynomial. If $a_n = 1$, then polynomial is called monic polynomial. Here, if $n = 0$, then $f(x) = a_0$ is a constant polynomial. Its degree is 0 , if $a_0 \neq 0$. If $a_0 = 0$, the polynomial is called zero polynomial. Its degree is defined as $-\infty$ to preserve the first two properties listed below. Some people prefer not to defined degree of zero polynomial. The domain and range of the function are the set of real numbers and complex numbers, respectively. Sometimes, we take the domain also to be complex numbers. If z is a complex number and $f(z) = 0$, then z is called 'a zero of the polynomial'.

If $f(x)$ is a polynomial of degree n and $g(x)$ is a polynomial of degree m then

1. $f(x) \pm g(x)$ is polynomial of degree $\leq \max\{n, m\}$

2. $f(x) \cdot g(x)$ is polynomial of degree $m + n$

3. $f(g(x))$ is polynomial of degree $m \cdot n$, where $g(x)$ is a non-constant polynomial.

Examples

Examples

1. $x^4 - x^3 + x^2 - 2x + 1$ is a polynomial of degree 4 and 1 is a zero of the polynomial as

$$1^4 - 1^3 + 1^2 - 2 \times 1 + 1 = 0.$$

2. $x^2 - (\sqrt{3} - \sqrt{2})x - \sqrt{6}$ is a polynomial of degree 2 and $\sqrt{3}$ is a zero of this polynomial as $(\sqrt{3})^2 - (\sqrt{3} - \sqrt{2})\sqrt{3} - \sqrt{6} = 3 - 3 + \sqrt{6} - \sqrt{6} = 0$.

Note: The above-mentioned definition and examples refer to polynomial functions in one variable. Similarly, polynomials in $2, 3, \ldots, n$ variables can be defined. The domain for polynomial in n variables being the set of (ordered) n tuples of complex numbers and the range is the set of complex numbers.

IIlustration $f(x, y, z) = x^2 - xy + z + 5$ is a polynomial in x, y, z of degree 2 as both x^2 and xy have degree 2 each.

Note: In a polynomial in n variables, say, $x_1, x_2, \ldots, x_n$, a general term is $x_1^{k_1} \cdot x_2^{k_2} \cdots x_n^{k_n}$. Degree of the term is $k_1 + k_2 + \cdots + k_n$ where $k_i \in \mathbb{N}_0, i = 1, 2, \ldots, n$. The degree of a polynomial in n variables is the maximum of the degrees of its terms.

1.4.1 Division in Polynomials

If $P(x)$ and $\phi(x)(\phi(x) \# 0)$ are any two polynomials, then we can find unique polynomials $Q(x)$ and $R(x)$, such that $P(x) = \phi(x) \times Q(x) + R(x)$ where the degree of $R(x) <$ degree of $\phi(x)$ or $R(x) \equiv 0.Q(x)$ is called the quotient and $R(x)$, the remainder.

In particular, if $P(x)$ is a polynomial with complex coefficients, and a is a complex number, then there exists a polynomial $Q(x)$ of degree 1 less than $P(x)$ and a complex number R, such that $P(x) = (x - a)Q(x) + R$.

IIlustration $x^5 = (x - a)\left(x^4 + ax^3 + a^2x^2 + a^3x + a^4\right) + a^5$. Here, $P(x) = x^5, Q(x) = x^4 + ax^3 + a^2x^2 + a^3x + a^4$, and $R = a^5$.

Example I What is the remainder when $x + x^9 + x^{25} + x^{49} + x^{81}$ is divided by $x^3 - x$.

Solution: We have,

$$\begin{aligned} x + x^9 + x^{25} + x^{49} + x^{81} &= x\left(1 + x^8 + x^{24} + x^{48} + x^{80}\right) \\ &= x\left[\left(x^{80} - 1\right) + \left(x^{48} - 1\right) + \left(x^{24} - 1\right) + \left(x^8 - 1\right) + 5\right] \\ &= x\left(x^{80} - 1\right) + x\left(x^{48} - 1\right) + x\left(x^{24} - 1\right) + x\left(x^8 - 1\right) + 5x \end{aligned}$$

Now, $x^3 - x = x\left(x^2 - 1\right)$ and all, but the last term $5x$ is divisible by $x\left(x^2 - 1\right)$. Thus, the remainder is $5x$.

Example 2 Prove that the polynomial $x^{9999} + x^{8888} + x^{7777} + \cdots + x^{1111} + 1$ is divisible by $x^9 + x^8 + x^7 + \cdots + x + 1$.

Solution: Let,

$$P = x^{9999} + x^{8888} + x^{7777} + \cdots + x^{1111} + 1$$
$$Q = x^9 + x^8 + x^7 + \cdots + x + 1$$
$$\begin{aligned} P - Q &= x^9\left(x^{9990} - 1\right) + x^8\left(x^{8880} - 1\right) + x^7\left(x^{7770} - 1\right) + \cdots + x\left(x^{1110} - 1\right) \\ &= x^9\left[\left(x^{10}\right)^{999} - 1\right] + x^8\left[\left(x^{10}\right)^{888} - 1\right] + x^7\left[\left(x^{10}\right)^{777} - 1\right] + \cdots + x\left[\left(x^{10}\right)^{111} - 1\right] \end{aligned}$$

But, $\left(x^{10}\right)^n - 1$ is divisible by $x^{10} - 1$ for all $n \geq 1$.
$\therefore$ RHS of Eq. (1) divisible by $x^{10} - 1$.
$\therefore$ $P - Q$ is divisible by $x^{10} - 1$
As $x^9 + x^8 + \cdots + x + 1 \mid \left(x^{10} - 1\right)$
$\Rightarrow x^9 + x^8 + x^7 + \cdots + x + 1 \mid (P - Q)$
$\Rightarrow x^9 + x^8 + x^7 + \cdots + x + 1 \mid P$

1.4.2 Remainder Theorem and Factor Theorem

Remainder Theorem

If a polynomial $f(x)$ is divided by $(x-a)$, then the remainder is equal to $f(a)$.
Proof:

If $R=0$, then $f(x)=(x-a)Q(x)$ and hence, $(x-a)$ is a factor of $f(x)$.
Further, $f(a)=0$, and thus, a is a zero of the polynomial $f(x)$. This leads to the factor theorem.

Factor Theorem

$(x-a)$ is a factor of polynomial $f(x)$, if and only if, $f(a)=0$.

Example 3 If $f(x)$ is a polynomial with integral coefficients and, suppose that $f(1)$ and $f(2)$ both are odd, then prove that there exists no integer n for which $f(n)=0$.

Solution: Let us assume the contrary. So, $f(n)=0$ for some integer n.

Then, $(x-n)$ divides $f(x)$.

Therefore, $f(x)=(x-n)g(x)$

where $g(x)$ is again a polynomial with integral coefficients.

Now, $f(1)=(1-n)g(1)$ and $f(2)=(2-n)g(2)$ are odd numbers but one of $(1-n)$ and $(2-n)$ should be even as they are consecutive integers.

Thus one of $f(1)$ and $f(2)$ should be even, which is a contradiction. Hence, the result. Aliter: See the Example (41) on page 6.24 in Number Theory chapter.

Example 4 Iff is a polynomial with integer coefficients such that there exists four distinct integer a_1, a_2, a_3 and a_4 with $f(a_1)=f(a_2)=f(a_3)=f(a_4)=1991$, show that there exists no integer b, such that $f(b)=1993$.

Solution: Suppose, there exists an integer b, such that $f(b)=1993$, let $g(x)=f(x)-1991$.

Now, g is a polynomial with integer coefficients and $g(a_1)=0$ for $i=1,2,3,4$.

Thus $(x-a_1)(x-a_2)(x-a_3)$ and $(x-a_4)$ are all factors of $g(x)$.

So, $g(x)=(x-a_1)(x-a_2)(x-a_3)(x-a_4)\times h(x)$

where $h(x)$ is polynomial with integer coefficients.

$$\begin{aligned} g(b) &= f(b)-1991 \\ &= 1993-1991=2(\text{ by our choice of } b) \end{aligned}$$

But, $g(b)=(b-a_1)(b-a_2)(b-a_3)(b-a_4)h(b)=2$

Thus, $(b-a_1)(b-a_2)(b-a_3)(b-a_4)$ are all divisors of 2 and are distinct.

$\therefore \quad (b-a_1)(b-a_2)(b-a_3)(b-a_4)$ are $1,-1,2,-2$ in some order, and $h(b)$ is an integer.

$\therefore \quad g(b)=4\cdot h(b)\neq 2$.

Hence, such b does not exist.

1.4.3 Fundamental Theorem of Algebra

Every polynomial function of degree ≥ 1 has at least one zero in the complex numbers. In other words, if we have

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

with $n\geq 1$, then there exists atleast one $h\in\mathbb{C}$, such that

$$a_n h^n+a_{n-1}h^{n-1}+\cdots+a_1 h+a_0=0.$$

From this, it is easy to deduce that a polynomial function of degree ' n ' has exactly n zeroes.

i.e., $f(x)=a(x-r_1)(x-r_2)\ldots(x-r_n)$

Notes:

1. Some of the zeroes of a polynomial may repeat.
2. If a root α is repeated m times, then m is called multiplicity of the root ' α ' or α is called m fold root.
3. The real numbers of the form $\sqrt{3}, \sqrt{5}, \sqrt{12}, \sqrt{27}, \ldots, \sqrt{5}+\sqrt{3}$, etc. are called, 'quadratic surds'. In general, $\sqrt{a}, \sqrt{b}$, and $\sqrt{a}+\sqrt{b}$, etc. are quadratic surds, if a, b are not perfect squares. In a polynomial with integral coefficients (or rational coefficients), if one of the zeroes is a quadratic surd, then it has the conjugate of the quadratic surd also as a zero.

Illustration $f(x)=x^2+2x+1=(x+1)^2$ and the zeroes of $f(x)$ are -1 and -1 . Here, it can be said that $f(x)$ has a zero -1 with multiplicity two.

Similarly, $f(x)=(x+2)^3(x-1)$ has zeroes $-2,-2,-2,1$, i.e., the zeroes of $f(x)$ are -2 with multiplicity 3 and 1 .

Example 5 Find the polynomial function of lowest degree with integral coefficients with $\sqrt{5}$ as one of its zeroes.

Solution: Since the order of the surd $\sqrt{5}$ is 2 , you may expect that the polynomial of the lowest degree to be a polynomial of degree 2 .

Let, $\quad P(x)=ax^2+bx+c; a, b, c \in \mathbb{Q}$

$$P(\sqrt{5})=5a+\sqrt{5}b+c=0 \Rightarrow (5a+c)+\sqrt{5}b=0$$

But, $\sqrt{5}$ is irrational.

So,

$$\begin{gathered}5a+c=0 \text{ and } b=0 \\ \Rightarrow c=-5a \text{ and } b=0.\end{gathered}$$

So, the required polynomial function is $P(x)=ax^2-5a, a \in \mathbb{Z}\backslash\{0\}$

You can find the other zero of this polynomial to be $-\sqrt{5}$.

Aliter: You know that any polynomial function having, say, n zeroes $\alpha_1, \alpha_2, \ldots, \alpha_n$ can be written as $P(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ and clearly, this function is of nth degree. Here, the coefficients may be rational, real or complex depending upon the zeroes $\alpha_1, \alpha_2, \ldots, \alpha_n$.

If the zero of a polynomial is $\sqrt{5}$, then $P_0(x)=(x-\sqrt{5})$ or $a(x-\sqrt{5})$.

But, we want a polynomial with rational coefficients.

So, here we multiply $(x-\sqrt{5})$ by the conjugate of $x-\sqrt{5}$, i.e., $x+\sqrt{5}$. Thus, we get the polynomial $P(x)=(x-\sqrt{5})(x+\sqrt{5})$, where the other zero of $P(x)$ is $-\sqrt{5}$. Now, $P_1(x)=x^2-5$, with coefficient of $x^2=1, x=0$ and constant term -5 , and all these coefficients are rational numbers.

Now, we can write the required polynomial as $P(x)=ax^2-5a$ where a is a non-zero integer.

Example 6 Obtain a polynomial of lowest degree with integral coefficient, whose one of the zeroes is $\sqrt{5}+\sqrt{2}$.

Solution: Let, $P(x)=x-(\sqrt{5}+\sqrt{2})=[(x-\sqrt{5})-\sqrt{2}]$.

Now, following the method used in the previous example, using the conjugate, we get:

$$\begin{aligned}
P_1(x) &= [(x-\sqrt{5})-\sqrt{2}][(x-\sqrt{5})+\sqrt{2}] \\
&= \left(x^2-2\sqrt{5}x+5\right)-2 \\
&= \left(x^2+3-2\sqrt{5}x\right) \\
P_2(x) &= \left[\left(x^2+3\right)-2\sqrt{5}x\right]\left[\left(x^2+3\right)+2\sqrt{5}x\right] \\
&= \left(x^2+3\right)^2-20x^2 \\
&= x^4+6x^2+9-20x^2 \\
&= x^4-14x^2+9 \\
P(x) &= ax^4-14ax^2+9a, \quad \text{ where } a \in \mathbb{Z}, a \neq 0.
\end{aligned}$$

The other zeroes of this polynomial are $\sqrt{5}-\sqrt{2}, -\sqrt{5}+\sqrt{2}, -\sqrt{5}-\sqrt{2}$.

1.4.4 Identity Theorem

A polynomials $f(x)$ of degree n is identically zero if it vanishes for atleast $n+1$ distinct values of ' x '.

Proof: Let $\alpha_1, \alpha_2, \ldots \alpha_n$ be n distinct values of x at which $f(x)$ becomes zero.

Then we have

$$f(x)=a\left(x-x_1\right)\left(x-x_2\right)\ldots\left(x-x_n\right)$$

Let α_{n+1} be the $n+1^{\text{th}}$ value of x at which $f(x)$ vanishes. Then

$$f\left(\alpha_{n+1}\right)=a\left(\alpha_{n+1}-\alpha_1\right)\left(\alpha_{n+1}-\alpha_2\right)\ldots\left(\alpha_{n+1}-\alpha_n\right)=0$$

As α_{n+1} is different from $\alpha_1, \alpha_2 \ldots \alpha_n$ none of the number $\alpha_{n+1}-\alpha_i$ vanishes for $i=1,2,3, \ldots n$. Hence $a=0 \Rightarrow f(x) \equiv 0$.

Using above result we can say that,

If two polynomials $f(x)$ and $g(x)$ of degree m, n respectively with $m \leq n$ have equal values at $n+1$ distinct values of x, then they must be equal.

Proof: Let $P(x)=f(x)-g(x)$, now degree of $P(x)$ is at most ' n ' and it vanishes for at least $n+1$ distinct values of $x \Rightarrow P(x) \equiv 0 \Rightarrow f(x) \equiv g(x)$.

Corollary: The only periodic polynomial function is constant function.

i.e., if $f(x)$ is polynomials with $f(x+T)=f(x) \forall x \in \mathbb{R}$ for some constant T then $f(x)=$ constant $=c$ (say)

Proof: Let $f(0)=c$

$\Rightarrow f(0)=f(T)=f(2T)=\ldots=c$

$\Rightarrow$ Polynomial $f(x)$ and constant polynomial $g(x)=c$ take same values at an infinite number of points. Hence they must be identical. Example 7 Let $P(x)$ be a polynomial such that $x \cdot P(x-1)=(x-4) P(x) \forall x \in \mathbb{R}$. Find all such $P(x)$.

Solution: Put $x=0,0=-4P(0)$

$$\Rightarrow P(0)=0$$

Put $x=1,1 \cdot P(0)=-3P(1)$

$$\Rightarrow P(1)=0$$

Put $x=2,2 \cdot P(1)=-2P(2)$

$$\Rightarrow P(2)=0$$

Put $x=3,3 \cdot P(2)=-P(3)$

$$\Rightarrow P(3)=0$$

Let us assume $P(x)=x(x-1)(x-2)(x-3) Q(x)$, where $Q(x)$ is some polynomial. Now using given relation we have

$$\begin{aligned}
& x(x-1)(x-2)(x-3)(x-4) Q(x-1)=x(x-1)(x-2)(x-3)(x-4) Q(x) \\
& \Rightarrow Q(x-1)=Q(x) \quad \forall x \in \mathbb{R}-\{0,1,2,3,4\} \\
& \Rightarrow Q(x-1)=Q(x) \quad \forall x \in \mathbb{R} \quad \text{(From identity theorem)} \\
& \Rightarrow Q(x) \text{ is periodic} \\
& \Rightarrow Q(x)=c \\
& \Rightarrow P(x)=c x(x-1)(x-2)(x-3)
\end{aligned}$$

Example 8 Let $P(x)$ be a monic cubic equation such that $P(1)=1, P(2)=2, P(3)=3$, then find $P(4)$.

Solution: as $P(x)$ is a monic, coefficient of highest degree will be ' 1 '. Let $Q(x)=P(x)-x$, where $Q(x)$ is also monic cubic polynomial.

$$Q(1)=P(1)-1=0; Q(2)=P(2)-2=0; Q(3)=P(3)-3=0$$
$$\Rightarrow \quad Q(x)=(x-1)(x-2)(x-3)$$
$$\Rightarrow \quad P(x)=Q(x)+x=(x-1)(x-2)(x-3)+x$$
$$\Rightarrow \quad P(x)=(4-1)(4-2)(4-3)+4=10$$

Excercises

1. Find a fourth degree equation with rational coefficients, one of whose roots is, $\sqrt{3}+\sqrt{7}$.
2. Find a polynomial equation of the lowest degree with rational coefficients whose one root is $\sqrt[3]{2}+3\sqrt[3]{4}$
3. Form the equation of the lowest degree with rational coefficients which has $2+\sqrt{3}$ and $3+\sqrt{2}$ as two of its roots.
4. Show that $(x-1)^2$ is a factor of $x^n-nx+n-1$.
5. If a, b, c, d, e are all zeroes of the polynomial $\left(6x^5+5x^4+4x^3+3x^2+2x+1\right)$, find the value of $(1+a)(1+b)(1+c)(1+d)(1+e)$.
6. If $1, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ be the roots of the equation $x^n-1=0, n \in \mathbb{N}, n \geq 2$ show that $n=\left(1-\alpha_1\right)\left(1-\alpha_2\right)\left(1-\alpha_3\right)\ldots(1-$
7. If $\alpha, \beta, \gamma, \delta$ be the roots of the equation $x^4+px^3+qx^2+rx+s=0$, show that $\left(1+\alpha^2\right)\left(1+\beta^2\right)\left(1+\gamma^2\right)\left(1+\delta^2\right)=(1-q+s)^2+(p-r)^2$. 8. If $f(x)=x^4+ax^3+bx^2+cx+d$ is a polynomial such that $f(1)=10, f(2)=20, f(3)=30$, find the value of $\frac{f(12)+f(-8)}{10}$.
8. The polynomial $x^{2k}+1+(x+1)^{2k}$ is not divisible by x^2+x+1. Find the value of $k \in \mathbb{N}$.
9. Find all polynomials $P(x)$ with real coefficients such that

$$(x-8)P(2x)=8(x-1)P(x).$$

11. Let $(x-1)^3$ divides $(p(x)+1)$ and $(x+1)^3$ divides $(p(x)-1)$. Find the polynomial $p(x)$ of degree 5 .

1.4.5 Polynomial Equations

Let, $P(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0; a_n \neq 0, n \geq 1$ be a polynomial function.

Then, $P(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$ is called a polynomial equation in x of degree n. Thus,

1. Every polynomial equation of degree n has n roots counting repetition.
2. If $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$

$a_n \neq 0$ and $a_i,(i=0,1,2,3,\ldots,n)$ are all real numbers and if, $\alpha+i\beta$ is a zero of (1), then $\alpha-i\beta$ is also a root. For real polynomial, complex roots occur in conjugate pairs.

However, if the coefficients of Eq. (1) are complex numbers, it is not necessary that the roots occur in conjugate pairs.

Example 9 Form a polynomial equation of the lowest degree with $3+2i$ and $2+3i$ as two of its roots, with rational coefficients.

Solution: Since, $3+2i$ and $2+3i$ are roots of polynomial equation with rational coefficients, $3-2i$ and $2-3i$ are also the roots of the polynomial equation. Thus, we have identified four roots so that there are 2 pairs of roots and their conjugates. So, the lowest degree of the polynomial equation should be 4 . The polynomial equation should be

$$P(x)=a[x-(3-2i)][x-(3+2i)][x-(2+3i)][x-(2-3i)]=0$$
$$\Rightarrow \quad a\left[(x-3)^2+4\right]\left[(x-2)^2+9\right]=0$$
$$\Rightarrow a\left((x-3)^2(x-2)^2+9(x-3)^2+4(x-2)^2+36\right)=0$$
$$\Rightarrow a\left(\left(x^2-5x+6\right)^2+9\left(x^2-6x+9\right)+4\left(x^2-4x+4\right)+36\right)=0$$
$$\Rightarrow a\left(x^4-10x^3+50x^2-130x+169\right)=0, \quad a \in \mathbb{Q} \mid \{0\}$$

1.4.6 Rational Root Theorem

An important theorem regarding the rational roots of polynomial equations:

If the rational number $\frac{p}{q}$, where $p, q \in \mathbb{Z}, q \neq 0, \gcd(p, q)=1$, i.e., p and q are relatively prime, is a root of the equation

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

where $a_0, a_1, a_2, \ldots, a_n$ are integers and $a_n \neq 0$, then p is a divisor of a_0 and q that of a_n.

Proof: Since $\frac{p}{q}$ is a root, we have

$$\begin{aligned}
& a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1 \frac{p}{q} + a_0 = 0 \\
& \Rightarrow a_n p^n + a_{n-1} q p^{n-1} + \cdots + a_1 q^{n-1} p + a_0 q^n = 0 \\
& \Rightarrow a_{n-1} p^{n-1} + a_{n-2} p^{n-2} q + \cdots + a_1 q^{n-2} p + a_0 q^{n-1} = -\frac{a_n p^n}{q}
\end{aligned}$$

Since the coefficients $a_{n-1}, a_{n-2}, \ldots, a_0$ and p, q are all integers, hence the left-hand side is an integer, so the right- hand side is also an integer. But, p and q are relatively prime to each other, therefore q should divide a_n.

Again,

$$\begin{aligned}
& a_n p^n + a_{n-1} q p^{n-1} + \cdots + a_1 q^{n-1} p = a_0 q^n \\
\Rightarrow & a_n p^{n-1} + a_{n-1} q p^{n-2} + \cdots + a_1 q^{n-1} = \frac{a_0 q^n}{p} \\
\Rightarrow & p \mid a_0
\end{aligned}$$

As a consequence of the above theorem, we have the following corollary.

1.4.7 Integer Root Theorem

Every rational root of $x^n + a_{n-1} x^{n-1} + \cdots + a_0; 0 \leq i \leq n-1$ is an integer, where $a_i (i=0,1,2,\ldots,n-1)$ is an integer, and each of these roots is a divisor of a_0.

Example 10 Find the roots of the equation $x^4 + x^3 - 19x^2 - 49x - 30$, given that the roots are all rational numbers.

Solution: Since all the roots are rational by the above corollary, they are the divisors of -30 .

The divisors of -30 are $\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30$.

By applying the remainder theorem, we find that $-1, -2, -3$, and 5 are the roots. Hence, the roots are $-1, -2, -3$ and $+5$.

Example II Find the rational roots of $2x^3 - 3x^2 - 11x + 6 = 0$.

Solution: Let the roots be of the form $\frac{p}{q}$, where $(p, q) = 1$ and $q > 0$.

Then, since $q/2, q$ must be 1 or 2 and $p \mid 6 \Rightarrow p = \pm 1, \pm 2, \pm 3, \pm 6$ By applying the remainder theorem,

$$f\left(\frac{1}{2}\right) = f\left(\frac{-2}{1}\right) = f\left(\frac{3}{1}\right) = 0.$$

(Corresponding to $q=2$ and $p=1; q=1, p=-2; q=1, p=3$, respectively.) So, the three roots of the equation are $\frac{1}{2}, -2$, and 3 .

Example 12 Solve: $x^3 - 3x^2 + 5x - 15 = 0$.

Solution: $x^3 - 3x^2 + 5x - 15 = 0 \Rightarrow \left(x^2+5\right)(x-3) = 0$

$$\Rightarrow x = \pm\sqrt{5} i, 3$$

So the solution are $3, \sqrt{5} i, -\sqrt{5} i$.

Example 13 Show that $f(x) = x^{1000} - x^{500} + x^{100} + x + 1 = 0$ has no rational roots.

Solution: If there exists a rational root, let it be $\frac{p}{q}$ where $(p, q) = 1, q \neq 0$. Then, q should divide the coefficient of the leading term and p should divide the constant term.

Thus, $q \mid 1 \Rightarrow q = \pm 1$,
And $p \mid 1 \Rightarrow p = \pm 1$
Thus, $\frac{p}{q} = \pm 1$
If the root $\frac{p}{q} = 1$,
Then, $f(1) = 1 - 1 + 1 + 1 + 1 = 3 \neq 0$, so, 1 is not a root.
If $\frac{p}{q} = -1$,
Then, $f(-1) = 1 - 1 + 1 - 1 + 1 = 1 \neq 0$
And hence, (-1) is not a root.
Thus, there exists no rational roots for the given polynomial.

1.4.8 Vieta's relations

If $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$ are the roots of the polynomial equation

$$a_n x_n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0 = 0 \quad (a_n \neq 0),$$

then,

$$\sum_{1 \leq i \leq n} \alpha_i = -\frac{a_{n-1}}{a_n}; \sum_{1 \leq i < j \leq n} \alpha_i \cdot \alpha_j = \frac{a_{n-2}}{a_n}$$
$$\sum_{1 \leq i < j < k \leq n} \alpha_i \alpha_j \alpha_k = -\frac{a_{n-3}}{a_n}, \cdots; \alpha_1 \alpha_2 \alpha_3 \cdots \alpha_n = (-1)^n \frac{a_0}{a_n}$$

If we represent the sum $\sum \alpha_i, \sum \alpha_i \alpha_j, \ldots, \sum \alpha_i \alpha_j \ldots \alpha_n$, respectively, as $\sigma_1, \sigma_2, \sigma_3, \ldots, \sigma_n$, (Read it 'sigma 1', 'sigma 2', etc.)
then,

$$\sigma_1 = -\frac{a_{n-1}}{a_n}, \sigma_2 = \frac{a_{n-2}}{a_n}, \ldots$$
$$\sigma_r = (-1)^r \frac{a_{n-r}}{a_n}, \ldots, \sigma_n = (-1)^n \frac{a_0}{a_n}$$

These relations are known as Vieta's relations.

Let us consider the following quadratic, cubic and biquadratic equations and see how we can relate $\sigma_1, \sigma_2, \sigma_3, \ldots$, with the coefficients. 1. $ax^2 + bx + c = 0$, where α and β are its roots. Thus,

$$\sigma_1 = \alpha + \beta = \frac{-b}{a} \quad \text{and} \quad \sigma_2 = \alpha\beta = \frac{c}{a}$$

2. $ax^3 + bx^2 + cx + d = 0$, where α, β and γ are its roots. Thus,

$$\sigma_1 = \alpha + \beta + \gamma = -\frac{b}{a}$$
$$\sigma_2 = \alpha\beta + \beta\gamma + \gamma\alpha = \frac{c}{a}$$
$$\sigma_3 = \alpha\beta\gamma = \frac{-d}{a}$$

Here, expressing $\sigma_2 = \alpha(\beta + \gamma) + \beta\gamma = \frac{c}{a}$ will be helpful when we apply this property in computations.

3. $ax^4 + bx^3 + cx^2 + dx + e = 0$, where $\alpha, \beta, \gamma, \delta$ are its roots. Thus,

$$
\begin{aligned}
& \sigma_1=\alpha+\beta+\gamma+\delta=\frac{-b}{a} \\
& \sigma_2=\alpha \beta+\alpha \gamma+\alpha \delta+\beta \gamma+\beta \delta+\gamma \delta=\frac{c}{a} \\
& \sigma_3=\alpha \beta \gamma+\alpha \beta \delta+\alpha \gamma \delta+\beta \gamma \delta=\frac{-d}{a}, \\
& \sigma_4=\alpha \beta \gamma \delta=\frac{e}{a}
\end{aligned}
$$

Here, again, σ_2 can be written as $(\alpha+\beta)(\gamma+\delta)+\alpha \beta+\gamma \delta$ and σ_3 can be written as $\alpha \beta(\gamma+\delta)+\gamma \delta(\alpha+\beta)$.

Example 14 If $x^2+a x+b+1=0$, where $a, b \in \mathbb{Z}$ and $b \neq-1$, has a root in integers then prove that a^2+b^2 is a composite.

Solution: Let, α and β be the two roots of the equation where, $\alpha \in \mathbb{Z}$. Then,

$$
\begin{aligned}
\alpha+\beta & =-a \\
\alpha \cdot \beta & =b+1
\end{aligned}
$$

$\therefore \quad \beta=-a-\alpha$ is an integer. Also, since $b+1 \neq 0, \beta \neq 0$.

From Eqs. (1) and (2), we get

$$
\begin{aligned}
a^2+b^2 & =(\alpha+\beta)^2+(\alpha \beta-1)^2 \\
& =\alpha^2+\beta^2+\alpha^2 \beta^2+1 \\
& =\left(1+\alpha^2\right)\left(1+\beta^2\right)
\end{aligned}
$$

Now, as $\alpha \in \mathbb{Z}$ and β is a non-zero integer, $1+\alpha^2>1$ and $1+\beta^2>1$.

Hence, a^2+b^2 is composite number.

Example I5 For what value of p will the sum of the squares of the roots of $x^2-p x=1-p$ be minimum?

Solution: If r_1 and r_2 are the roots of $x^2-p x+(p-1)=0$, then $r_l+r_2=p, r_1 r_2=p-1$

$$
r_1^2+r_2^2=\left(r_1+r_2\right)^2-2 r_1 r_2=p^2-2 p+2=(p-1)^2+1
$$

and $r^2+r_2{}^2$ is minimum when $(p-1)^2$ is minimum, then $p=1$.

Thus, for $p=1$, the sum of the squares of the roots is minimum.

Example 16 Let u, v be two real numbers none equql to -1 , such that u, v and uv are the roots of a cubic polynomial with rational coefficients. Prove or disprove that uv is rational.

Solution: Let, $x^3+a x^2+b x+c=0$ be the cubic polynomial of which u, v, and uv are the roots and a, b, and c are all rationals.

and

$$
\begin{aligned}
& u+v+u v=-a \\
& \Rightarrow u+v=-a-u v, \\
& u v+u v^2+u^2 v=b \\
& u^2 v^2=-\mathrm{c}
\end{aligned}
$$

From (2)

$$
\begin{aligned}
b & =u v+u v^2+u^2 v=u v(1+v+u) \\
& =u v(1-a-u v) \quad(\text { From }(1)) \\
& =(1-a) u v-u^2 v^2 \\
& =(1-a) u v+c \\
\Rightarrow & (1-a) u v=b-c
\end{aligned}
$$

As $a \neq 1, u v=\frac{(b-c)}{1-a}$ and since, a, b, c are rational, uv is rational.

Note that $a=1 \Rightarrow 1+u+v+u v=0 \Rightarrow(1+u)(1+v)=0 \Rightarrow u=-1$ or $v=-1$, which is not the case.

Example 17 Solve the cubic equation $9x^3-27x^2+26x-8=0$, given that one of the root of this equation is double the other.

Solution: Let the roots be $\alpha, 2\alpha$ and β.

Now,

$$\begin{aligned}
&3\alpha+\beta=-\frac{-27}{9}=3\\
&\Rightarrow \quad \beta=3(1-\alpha)\\
&2\alpha^2+3\alpha\beta=\frac{26}{9}\\
&2\alpha^2\beta=\frac{8}{9}
\end{aligned}$$

From Eqs. (1) and (2), we get

$$\begin{aligned}
&2\alpha^2+3\alpha\times 3(1-\alpha)=\frac{26}{9}\\
\Rightarrow &63\alpha^2-81\alpha+26=0\\
\Rightarrow &\quad (21\alpha-13)(3\alpha-2)=0
\end{aligned}$$

So, $\alpha=\frac{13}{21}$ or $\frac{2}{3}$

If $\alpha=\frac{13}{21}$ $\therefore \beta=3\left(1-\frac{13}{21}\right)=\frac{24}{21}=\frac{8}{7}$

This leads to $2\alpha^2\beta=2\times\frac{169}{441}\times\frac{8}{7}\neq\frac{8}{9}$ (a contradiction)

So, taking $\alpha=\frac{2}{3}, \quad \beta=3\left(1-\frac{2}{3}\right)=3\times\frac{1}{3}=1$

Hence, $\alpha+2\alpha+\beta=\frac{2}{3}+\frac{4}{3}+1=3$,

$$2\alpha^2+3\alpha\beta=2\times\frac{4}{9}+\frac{3\times 2}{3}\times 1=\frac{26}{9},$$

and

$$2\alpha^2\beta=2\times\frac{4}{9}\times 1=\frac{8}{9}$$

Thus, the roots are $\frac{2}{3},\frac{4}{3}$, and 1 .

Example 18 Solve the equation $6x^3-11x^2+6x-1-0$, given that the roots are in harmonic progression.

Solution: Let the roots be α,β and γ.

Since they are in HP,

$$\therefore \quad \beta=\frac{2\alpha\gamma}{\alpha+\gamma}$$

Now,

$$\begin{aligned}
&\sigma_1=\alpha+\beta+\gamma=\frac{11}{6}\\
&\sigma_2=\beta(\alpha+\gamma)+\alpha\gamma=1\\
&\sigma_3=\alpha\beta\gamma=\frac{1}{6}
\end{aligned}$$

Using Eqs. (1) and (3), we get

$$\begin{aligned}
&\frac{2\alpha\gamma}{(\alpha+\gamma)}\times(\alpha+\gamma)+\alpha\gamma=1\\
\Rightarrow &3\alpha\gamma=1\\
\Rightarrow &\alpha\gamma=\frac{1}{3}
\end{aligned}$$

From Eqs. (4) and (5), we get

$$\beta = \frac{1}{6} \div \frac{1}{3} = \frac{1}{2}$$

From Eqs. (2) and (6), we get

$$\begin{aligned} \alpha + \gamma &= \frac{11}{6} - \frac{1}{2} = \frac{8}{6} = \frac{4}{3} \\ \therefore \quad \alpha &= \frac{4}{3} - \gamma \end{aligned}$$

$\therefore$

$$\begin{aligned} \alpha \times \gamma = &\frac{1}{3} \Rightarrow \left(\frac{4}{3} - \gamma\right)\gamma = \frac{1}{3} \\ &\gamma^2 - \frac{4}{3}\gamma + \frac{1}{3} = 0 \\ &3\gamma^2 - 4\gamma + 1 = 0 \\ &(3\gamma - 1)(\gamma - 1) = 0 \\ &\gamma = \frac{1}{3} \text{ or } \gamma = 1 \end{aligned}$$

Hence, $\alpha = 1$ or $\alpha = \frac{1}{3}$.

Thus, the roots are $1, \frac{1}{2}, \frac{1}{3}$ or $\frac{1}{3}, \frac{1}{2}, 1$.

Example 19 If the product of two roots of the equation $4x^4 - 24x^3 + 31x^2 + 6x - 8 = 0$ is 1 , find all the roots.

Solution: Suppose, the roots are $\alpha, \beta, \gamma, \delta$ and $\alpha\beta = 1$.

Now,

$$\begin{aligned} &\sigma_1 = (\alpha + \beta) + (\gamma + \delta) = -\frac{-24}{4} = 6 \\ &\sigma_2 = (\alpha + \beta)(\gamma + \delta) + \alpha\beta + \gamma\delta = \frac{31}{4} \\ &\Rightarrow \quad (\alpha + \beta)(\gamma + \delta) + \gamma\delta = \frac{31}{4} - 1 = \frac{27}{4} \\ &\sigma_3 = \gamma\delta(\alpha + \beta) + \alpha\beta(\gamma + \beta) = \frac{-3}{2} \\ &\Rightarrow \quad \gamma\delta(\alpha + \beta) + (\gamma + \delta) = \frac{-3}{2} \\ &\sigma_4 = \alpha\beta\gamma\delta = -2 \\ &\Rightarrow \quad \gamma\delta = -2 \end{aligned}$$

From Eqs. (2) and (4), we get

$$(\alpha + \beta)(\gamma + \delta) = \frac{35}{4}$$

From Eqs. (3) and (4), we get

$$-2(\alpha + \beta) + (\gamma + \delta) = \frac{-3}{2}$$

From Eqs. (1) and (6), we get

or

$$\begin{aligned} 3(\alpha + \beta) &= \tfrac{15}{2} \\ \alpha + \beta &= \tfrac{5}{2} \\ \alpha\beta &= 1 \\ \Rightarrow \quad \beta &= \tfrac{1}{\alpha} \end{aligned}$$

and Putting the value of β in Eq. (7), we get

$$\begin{aligned}
&\alpha+\frac{1}{\alpha}=\frac{5}{2}\\
\Rightarrow &2\alpha^2-5\alpha+2=0\\
\Rightarrow &(2\alpha-1)(\alpha-2)=0\\
\Rightarrow &\alpha=\frac{1}{2} \text{ or } \alpha=2
\end{aligned}$$

Hence, $\beta=2$ or $\beta=\frac{1}{2}$.
Taking $\alpha=\frac{1}{2}$ and $\beta=2$, and substituting in Eq. (5), we get $\gamma+\delta=\frac{7}{2}$. We know that $\gamma\delta=-2$.
Again, solving for γ and δ, we get

$$\gamma=\frac{-1}{2} \text{ and } \delta=4 \text{ or } \delta=\frac{-1}{2} \text{ and } \gamma=4$$

Thus, the four roots are $\frac{1}{2}, \frac{-1}{2}, 2$, and 4 .
Example 20 One root of the equation $x^4-5x^3+ax^2+bx+c=0$ is $3+\sqrt{2}$. If all the roots of the equation are real, find extremum values of a, b, c; given that a, b and c are rational.
Solution: Since the coefficients are rational, where $3+\sqrt{2}$ is a root, so $3-\sqrt{2}$ is also a root.
Thus, if the other two roots are α and β, we have

$$\begin{aligned}
&\sigma_1=\alpha+\beta+3+\sqrt{2}+3-\sqrt{2}=-(-5)=5\\
&\Rightarrow \alpha+\beta=-1\\
&\sigma_2=(\alpha+\beta)(3+\sqrt{2}+3-\sqrt{2})+\alpha\beta+(3+\sqrt{2})(3-\sqrt{2})=a\\
&\text{ or }\quad 6(\alpha+\beta)+\alpha\beta+7=a\\
&\text{ or }\quad \alpha\beta=a-1\\
&\sigma_3=\alpha\beta(3+\sqrt{2}+3-\sqrt{2})+(3+\sqrt{2})(3-\sqrt{2})(\alpha+\beta)\\
&=-b\\
&=6\alpha\beta+7(-1)=-b\\
&\alpha\beta=\frac{7-b}{6}\\
&\sigma_4=7\alpha\beta=c\\
&\Rightarrow \quad \alpha\beta=\frac{c}{7}
\end{aligned}$$

Since, we are interested in finding a, b and c, we take $\alpha+\beta=-1, \alpha\beta=k.\alpha$ and β are the roots of $x^2+x+k=0$.
Since the roots of the given equation are real and hence, the roots of above equation are real, if

$$\begin{aligned}
&D\geq 0\Rightarrow 1-4k\geq 0\\
&\text{or, } k\leq\frac{1}{4}
\end{aligned}$$

Now for $a, k=a-1$

$$\begin{aligned}
&\Rightarrow a-1\leq\frac{1}{4}\\
&\Rightarrow a\leq\frac{5}{4}
\end{aligned}$$

So, the greatest value of a is $\frac{5}{4}$.
For $b, k=\frac{7-b}{6}$
$\Rightarrow \frac{7-b}{6}\leq\frac{1}{4}$
$\Rightarrow b\geq 7-\frac{3}{2}$

$\Rightarrow b \geq \frac{11}{2}$
So, least value of b will be $\frac{11}{2}$ and for c, take $k = \frac{c}{7}$
$\Rightarrow \frac{c}{7} \leq \frac{1}{4}$
$\Rightarrow c \leq \frac{7}{4}$
So, maximum value of c will be $\frac{7}{4}$
For these extremum values of a, b and c, the equation becomes

$$x^4 - 5x^3 + \frac{5}{4}x^2 + \frac{11}{2}x + \frac{7}{4} = 0$$

The four roots of this equation are

$$3 + \sqrt{2}, 3 - \sqrt{2}, \frac{-1}{2}, \frac{-1}{2} \qquad \text{(verify this)}$$

1.5 PROBLEMS

1. Find the rational roots of $x^4 - 4x^3 + 6x^2 - 4x + 1 = 0$.
2. Solve the equation $x^4 + 10x^3 + 35x^2 + 50x + 24 = 0$, if sum of two of its roots is equal to sum of the other two roots.
3. Find the rational roots of $6x^4 + x^3 - 3x^2 - 9x - 4 = 0$.
4. Find the rational roots of $6x^4 + 35x^3 + 62x^2 + 35x + 2 = 0$.
5. Given that the sum of two of the roots of $4x^3 + ax^2 - x + b = 0$ is zero, where $a, b \in \mathbb{Q}$. Solve the equation for all values of a and b.
6. Find all a, b, such that the roots of $x^3 + ax^2 + bx - 8 = 0$ are real and in G.P.
7. Show that $2x^6 + 12x^5 + 30x^4 + 60x^3 + 80x^2 + 30x + 45 = 0$ has no real roots.
8. Construct a polynomial equation, of the least degree with rational coefficients, one of whose roots is $\sin 10°$.
9. Construct a polynomial equation of the least degree with rational coefficients, one of whose roots is $\sin 20°$.
10. Construct a polynomial equation of the least degree, with rational coefficients, one of whose roots is $(a) \cos 10° (b) \cos 20°$.
11. Construct a polynomial equation of the least degree with rational coefficient, one of whose roots is $(a) \tan 10° (b) \tan 20°$.
12. Construct a polynomial equation with rational coefficients, two of whose roots are $\sin 10°$ and $\cos 20°$.
13. If p, q, r are the real roots of $x^3 - 6x^2 + 3x + 1 = 0$, determine the possible values of $p^2q + q^2r + r^2p$.
14. The product of two of the four roots of the quartic equation $x^4 - 18x^3 + kx^2 + 200x - 1984 = 0$ is -32 . Determine the value of k.

[USA MO, 1984]

Chapter 2

NUMBER THEORY

2.1 NATURAL NUMBERS

2.1.1 Subsets of natural numbers

Until now, you know how the sets of numbers are greater and less than each other. Now, it's time to care much more about natural numbers. Do you remember them? Positive integers.

Within natural numbers, there are subsets that are mostly identifiable and commonly used. However, it is not necessary that they are complementary nor make a specific interval. Even numbers/integers: we define 'even numbers' as integers, not necessarily natural numbers which can be expressed as 2k, where k is any integers. Or simply, integers whose division by 2 leave a remainder of zero. Examples: $0, -2, 58, 1889283834$ Odd numbers: we define 'odd numbers' as integers, not necessarily natural numbers which can be expressed as 2k+1, where k is any integers. Or simply, integers whose division by 2 leave a remainder of one.

Prime numbers: prime numbers are strictly natural numbers or positive integers which have 1 and itself only as positive divisors. Example: $3, 17, 71, ...$ Composite numbers: these are positive integers or natural numbers that are not prime numbers. In simple words, these are positive integers which have positive divisors greater than 2. Is one a prime or a composite number? One is neither a prime number nor a composite number. It is very special. Two integers a and b are called relatively prime or coprime if and only if there does not exist another integer greater than 1, which can divide both a and b.

2.2 BASIC PROBLEM SOLVING TECHNIQUES

Which set am I working in? Most problems can be incredibly simplified by knowing and understanding their scope. The important thing is the boundaries. One of them is the set that you are working in. For instance, i) Find all real numbers...? This question extends to all real numbers. It is very obvious that taking and trying small numbers like 1, 2, 3 can't help much in this case. Rather we can start to think of theorems that work for real numbers than integers. ii) Find all positive integers x and y...? This question's solutions are limited to only integers. In the first place, we get an intuition of where to start from. Therefore, right before you approach any question, just pause a bit and understand its scope, especially its boundary set.

2.2.1 Basic properties of integers

Associativity a + (b + c) = (a + b) + c and a(bc) = (ab)c
Commutativity a + b = b + a and ab = ba
Distributivity a(b + c) = ab + ac and (a + b)c = ac + bc
Identity a + 0 1= 0 + a = a and a . 1 = 1 . a = a
Inverse a + (-a) = (-a) + a = 0
Transitivity a > b and b > c implies a > c

Trichotomy: Either a > b, a < b, or a = b
Cancellation law If a . c = b . c and c 0, then a = b

2.2.2 Divisibility

First and foremost, we are working in a natural numbers set.

Divisibility is the first chapter we start Number Theory with. The ideas involved in a number being divisible by another leads to all sorts of definitions and results. We explore some of them in this chapter.

Back in primary, do you remember the multiplication table? For instance, the numbers in this set $..., 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60, ...$ are in the multiplication table of 5.

We haven't even started yet and we already have our first definition: any number in this list is called a multiple of 5, and is said to be divisible by 5. This works for all natural numbers, say 3, 7 and 13.

Definition: A number n is said to be a multiple of m if it appears in the table of m. A number n is divisible by m if n is a multiple of m. Also, we say m divides n and write this symbolically as n | m, where the symbol notation simply reads "n divides m". Some properties:

Properties of Divisibility

For any x, y, z being a natural number different from zero, the below properties hold.

- $x|x$.
- $1|x$ and $x|0$.
- $x|y$ and $y|z \Rightarrow x|z$.
- If $z|x, y$, then $z|ax + by$ for any integers a, b(possibly negative).
- If $x|y$, then either $y = 0$, or $|x| \leq |y|$.
- If $x|y$ and $y|x$, then $x = y, i.e.|x| = |y|$
- $x|y$ if and only if $xz|yz$ for some non-zero integer z.
- $x|y \Rightarrow x|yz$for any z.

GCD and LCM

Every natural number greater than 1 is divisible by at least one prime.

The greatest common divisor of two natural numbers is donated gcd (a, b), it is the greatest natural number that can divide both a and b.

The lowest common multiple of two numbers is the smallest integer divisible by both a and b.

Therefore, $a\dot{b} = gcd(a, b)\dot{l}cm(a, b)$

Some number theoretic functions: Floor function: is called the greatest integer function ie: an integer less than or equal to x. Ex: where n is an integer. Ceiling function: is called the least integer function. ie: an integer greater than or equal to x.

Four basic operations

For integers, the four operations namely addition, subtraction, multiplication, and positive-power are closed under integers set. In simple words, that's to mean when you add, subtract, multiply or positive-power an integer or integers, the results should be an integer or integers too.

Addition and subtraction Addition is the most basic of the four operations. There is a famous story in the mathematical folklore about the great German mathematician Guass. He was a precocious child. When he was in elementary school, his teacher was constantly worried about being asked smart questions by the little boy. One day, the teacher asked him to sum the positive integers from 1 to 100, thinking it would keep him quiet for quite a while. However, Gauss produced the answer 5050 immediately. How could he do it so fast?

Mostly likely, Gauss did it this way. He wrote down the numbers from 1 to 100 in a row. Right below, he wrote down another row of numbers, the same ones but in the opposite order. Guass then added up the two numbers in each column. In each case, he got the answer 101. Since he had 100 columns of numbers, the sum of all the numbers in the two rows must be $100 \times 101 = 10100$. Since both rows consisted of the same numbers, the sum of all the numbers in either row must be $10100 \div 2 = 5050$. Gauss probably did all this in his head.

Addition operation has some interesting facts especially when it comes to integers.

In general, the sum of all the positive integers from 1 to a certain number is equal to half the product of that number and the next number.

1. Arrange the numbers 1, 2, 3, 4, 5, 6, 7, 8 and 9 in a row so that all of the following conditions are satisfied: (1) the sum of 1 and 2 and all the numbers between them is 9; (2) the sum of 2 and 3 and all the numbers between them is 19; (3) the sum of 3 and 4 and all the numbers between them is 45; (4) the sum of 4 and 5 and all the numbers between them is 18.
   Solution
   By (3), 3 and 4 must be at the ends. By (1), 6 must be the only number between 1 and 2. By (4), the sum of the numbers between 4 and 5 is 9. If they consist of the block $1-6-2$, 7, 8 and 9 will all lie between 2 and 3, contradicting (2). Hence none of 1, 6 and 2 appear between 4 and 5, so that 9 must be the only number there. By (2), the sum of the numbers between 2 and 3 is 14. They cannot include the block $4-9-5$. It follows that the arrangement must be $3-7-1-6-2-8-5-9-4$ or its reversal.

2. Find the number of different ways of expressing 27 as a sum of four integers greater than 3, such that the first is less than the second, the second is less than the third and the third is less than the fourth.
   Solution
   We may have 4 as the first number. If the second number is 5, then the sum of the third number and the fourth number is $27-4-5=18$. Since each is at least 6, they may be $6+12$, $7+11$ or $8+10$. If the second number is increased to 6, then the sum of the third number and the fourth number is $27-4-6=17$. Since each is at least 7, they may be $7+10$ or $8+9$. We cannot increase the second number to 7 as $4+7+8+9=28$ is too big. However, we may increase the first number to 5. Then we can have $27=5+6+7+9$. Since no further modification is possible, the total number of ways is $3+2+1=6$.

3. Five consecutive two-digit numbers are such that 37 is a divisor of the sum of three of them, and 71 is also a divisor of the sum of three of them. Find the largest of these five numbers.
   Solution
   Among five consecutive numbers, the sum of the largest three is only 6 more than the sum of the smallest three. Thus we are looking for a multiple of 37 and a multiple of 71 which differ by at most 6. Now 37 x 2 - 71 = 3 and 37 x 4 - 71 x 2 = 6. In the latter case, 148 must be the sum of the largest three numbers, which are consecutive. Hence the sum is divisible by 3, but 148 is not a multiple of 3. In the former case, note that $71 < 23+24+25 = 72 < 74$. Hence the smallest of the five numbers cannot be 23 or more, and the largest cannot be 25 or less. This means that the five numbers must be $22, 23, 24, 25$ and 26, the largest of which is 26. There is no need to consider higher multiples of 37 and 71 as the sums will be too large to allow the five numbers to have only t wo digits.

4. Five different positive integers are multiplied two at a time, yielding ten products. The smallest product is 28, the largest product is 240 and 128 is also one of the products. Find the sum of these five numbers.
   Solution
   Note that 28 is the product of the smallest two numbers while 240 is the product of the largest two. Hence the smallest two are 1 and 28, 2 and 14 or 4 and 7. Note that the second smallest number is no less than 7, so that the second largest number is no less than 9. Hence the largest two numbers are 10 and 24, 12 and 20 or 15 and 16. Note that the second largest number is no greater than 15, so that the second smallest number is no greater than 13. Hence the smallest two numbers are 4 and 7. Now 128 is not divisible by 7, or by any of the possible values for the second largest number, namely 10, 12 and 15. The smallest number 4 cannot be one of its factors as the other factor 32 is greater than any possible value of the largest number. It follows that 128 is the product of the middle and the largest number. The largest number must be 16 as neither 20 or 24 divides 128. Hence the five numbers are 4, 7, 8, 15 and 16, and their sum is 50.

Division and Powers

Division is also a special bitwise operation on numbers. However, we have to be careful here. It is not closed under integers. This is to mean, when you divide two integers, it is not necessary that the result be an integer too. This is also another beautiful property though. It is important to learn which numbers whose division result in integers or otherwise. You are pretty used to property and it is called divisibility.

1. Omit one of the numbers 1, 2, 3, 4, 5, 6, 7, 8 and 9, and divide the sum of the remaining eight numbers into four pairs of equal sums. Find the number of possible values of the number omitted.
   Solution
   Note that 1+2+3+4+5+6+7+8+9=45. When divided by 4, it leaves a remainder 1. When the nine numbers are divided by 4 individually, they leave remainders 1, 2, 3, 0, 1, 2, 3, 0 and 1 respectively. The sum of the remainders is 13, and when 13 is divided by 4, it leaves a remainder 1. It follows

   that the number omitted should have remainder 1 when di- divided by 4. Hence it must be one of 1, 5 and 9. If 1 is omit- ted, we may have $2 + 9 = 3 + 8 = 4 + 7 = 5 + 6$. If 5 is omitted, we

   may have $1 + 9 = 2 + 8 = 3 + 7 = 4 + 6$. If 9 is omitted, we may have $1 + 8 = 2 + 7 = 3 + 6 = 4 + 5$. Hence all 3 values are possible.

If repeated addition is multiplication, what is repeated multiplication then? This leads to a fifth operation that may be called fifth power. For instance, we write 7 x 7 x 7 as 7^3, and we say that we are raising the number 7 to the power 3. A number raised to the power 2 is called a square, and a number raised to the power 3 is called a cube. Backwardly, if a number is a square of an integer is normally referred to a "perfect square", and if a number is a cube of an integer, it is normally referred to as "perfect cube".

1. Each of the letters T, E, N, I, L and A stand for a different positive integer. If T×E×E×N=52, T×I×L×T=77 and T×A×L×L=363, find T×A×T×T×L×E.
   Solution
   Note that each of the three given products contains a square. The first few squares are 1, 4, 9, 16, 25, 36, 49, 64, 81, 100 and 121. Since the largest square which divides 77 is 1, we must have T=1. Since the largest square which divides 52 is 4 and we already have T=1, we must have E=2. Similarly, we have L=11 and A=3. Hence T×A×T×T×L×E=66.

2. Find the number of different ways 90 can be expressed as the sum of at least two consecutive positive integers.
   Solution
   The odd factors of 90 greater than 1 are 3, 5, 9, 15 and 45. Thus there are 5 such expressions. They are a range of average of 30: 29+30+31, a range of average of 18: $16 + \cdots + 20$, a range of average of 10: $6 + 7 + \cdots + 14$, a range of average of 6: $(1) + 0 + \cdots + 12 + 13 = 2 + 3 + \cdots + 13$ and a range of average of 2: $(20) + (19) + \cdots + 23 + 24 = 21 + 22 + 23 + 24$. Hence there are only 5 ways. We don't count for 1 because they are such consecutive integers whose average is 1, except 1 only. We can prove this property by AM-GM inequality.

Digits We have limited digits, but they behave differently and follow beautiful properties. Most of them follow common behaviour of integers, not necessarily digits only. For instance, an integer ending in 5 multiplied by any other integer, the result can never end in 2 nor 6. What should it end in?

1. Find the number of positive integers under 1000 with units digit 9 which can be expressed as the sum of a power of 2 and a power of 3. Note that 1 is both a power of 2 and a power of 3.
   Solution
   The powers of 2 under 1000 are 1, 2, 4, 8, 16, 32, 64, 128, 256 and 512. They end in 1, 2, 4, 6 or 8. The powers of 3 under 1000 are 1, 3, 9, 27, 81, 243 and 729. They end in 1, 3, 7 or 9. If the desired number should end in 9, the only possibilities, from powers of 2 and powers of 3 respectively: 2 and 7, 6 and 3, and lastly 8 and 1 only. How many are they? The total number is 10.

2. Find the smallest positive integer whose product with 123 ends in 2004.
   Solution
   Since the last digit of the product is 4, the last digit of the multiplier must be 8. Now 8 x 123 = 984. If we delete the digit 8 from the multiplier, the new product is 984 less, and its last digit will be 2. Therefore, the last digit of the new multiplier must be 4. Now 4 x 123 = 492. If we delete the digit 4,

the new product is 492 less, and its last digit will be 1. Therefore, the last digit of the new multiplier must be 7. Now 748 x 123 = 92004, and 748 is the smallest positive integer whose product with 123 ends in 2004.

3. Find the number of two-digit positive integers such that when its digits are reversed, the new number is at least 3 times as large as the original number.
   Solution
   The tens digit cannot be 4 or more since 3×40 is a three-digit number. It cannot be 3 because the units digit must then be 9, but 3 x 39 is also a three-digit number. If it is 2, the units digits cannot be 8 or less since 3 x 28 $>$ 82. However, we do have 3 x 29 $<$ 92. If the tens digit is 1, the units digits cannot be 4 or less since 3 x 14 = 42. On the other hand, 15, 16, 17, 18 and 19 have the desired property, along with 29. Thus there are 6 such numbers.

4. The sum of 1006 different positive integers is 1019057. If none of them is greater than 2012, find the minimum number of these integers which must be odd.
   Solution
   Suppose we take the first 1006 even numbers. Then their sum is $\frac{1006(2+2012)}{2} = 1013042$. Now 1019057 - 1013042 = 6015. So we have to trade some even numbers for an equal amount of odd numbers. Clearly, trading only one number can raise the total by at most 2011 - 2 = 2009. Hence we have to trade more than one number. However, if we trade exactly two numbers, the total will increase by an even amount, which is not what we want. Hence we must trade at least three numbers. If we trade 2, 4 and 6 for 2007, 2009 and 2011, the total will increase by $2007 + 2009 + 2011 - 2 - 4 - 6 = 3$ x $(2009 - 4) = 6015$ exactly. Hence the minimum number of the 1006 integers which must be odd is 3.

2.2.3 Brief Introduction to Intermediate Number Theory

The N denotes a set of natural numbers. That is to say positive whole numbers: $1, 2, 3, \ldots$. We have two main categories of natural numbers, even and odd numbers which go alternatively. A number n is an even number, if $n = 2a$ where $a \in \mathbf{Z}$. Conversely, a number n is odd, if $n = 2a + 1$ where $a \in \mathbf{Z}$ (set of integers). A natural number p is called a prime number if it has exactly only two distinct positive divisors. Otherwise a number is called a composite number. However, 1 is neither a prime nor a composite.

2.2.4 Properties of a prime number

1. $p|ab \Rightarrow p|a$ or $p|b$

2. Every natural number greater than 1 is divisible by at least one prime.

3. The greatest common divisor of two natural numbers is donated $gcd(a, b)$, it is greatest natural number that can divide both a and b.

4. The lowest common multiple of two numbers is the smallest integer divisible by both a and b. Therefore $a * b = gcd(a, b) * lcm(a, b)$

5. Every natural number can be prime-factorised. This is to mean, it can be expressed as a product of prime numbers. Say, $m = p_1^{\alpha_1} * p_2^{\alpha_2} * p_3^{\alpha_3} * \ldots p_n^{\alpha_n}$. Number of divisors of m is $(\alpha_1 + 1) * (\alpha_2 + 1) * (\alpha_3 + 1) \ldots (\alpha_n + 1)$

2.2.5 Euclidean Algorithm

For two natural numbers a and b, $a > b$, then there exist unique integers q and r such that $a = bp + r$ where $0 \leq r < b$. In this case, a is called dividend, b a divisor, p is a quotient, and r a remainder.
The Euclidean algorithm is a way to find the greatest common divisor of two positive integers, a and b. The $gcd(a, b) = gcd(b, a - b)$ (called "initial statement" in our notes).
Then, to compute the $gcd(a, b)$, $a > b$,
Express $a = bq_1 + r_1$, and $0 \leq r_1 < b$
By initial statement, $gcd(a, b) = gcd(b, r_1)$

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

and $gcd(b, r_1) = gcd(r_1, r_2)$;

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

and $gcd(r_1, r_2) = gcd(r_2, r_3)$

and so on. Since $r_1 > r_2 > r_3 \geq 0$
...
...
...
eventually some $r_k = 0$ and $gcd(a, b) = (r_{k-1}, r_k) = (r_{k-1}, 0) = rk - 1$; in other words, $gcd(a, b)$ is the last non-zero remainder we compute. Note that $(a, 0) = a$

Example: Find the gcd(48,80)
Solution: gcd(48, 80) = gcd(48, 32) since $80 = 48(1) + 32$. Then, gcd(48, 32) = gcd(32,16) = gcd(16,16) = gcd(16,0) = 16. Hence, done.

Exercises. Find the gcd(2187,78642). Find the gcd(1758374,289738).

N.B: The gcd of two numbers is the least possible natural number which can be written as a linear combination of such two numbers. Say, if the gcd(a,b) = d, d is the least natural number which can be written as a linear combination of a and b. To express the gcd of two numbers as their linear combination, we reverse the Euclidean Algorithm. We go back replacing in the values of the previous step until we arrive at our initial numbers.

2.2.6 Modular Arithmetic

Time and Days

If the time is 10:00 (10pm), what time is it after 4 hours? What time is it after 100 hours? If today is Wednesday, what day of the week was it 1000 days ago?

In order to answer the above questions, we start with simple questions like the number of hours in a day and the number of days in a week. For the first question about time, we know that there are 24 hours in a day. We know that after exactly 24 hours, it will be tomorrow the same time as now. We do this a number of time and finally reach on the simple number of hours we to add. Say, after 100 hours, we only add 4 hours because after exactly 4 days (96 hours), it will be 10pm as of now. Then, after 100 hours, it will be 10pm + 4 hours = 02am.
Would you try the second question of days?

Equivalent Numbers

The two previous questions would be simplified in equivalent numbers. This is to say, after every 24 hours we come back to the same hour; and after every 7 days, we come back to the same day.
$24 \equiv 0(mod 24)$ and $7 \equiv 0(mod 7)$
Exercises: Answer by true or false. It is true that $25 \equiv 3(mod 24)$
It is true that $12 \equiv 7(mod 5)$
It is true that $5 \equiv 8(mod 6)$
It is true that $24 + 2 \equiv 0 + 2(mod 24)$
It is true that $5 \equiv 5(mod 8)$

Review and prove these Properties of Modular Arithmetic

1. If $a + b = c$, then $a + b \equiv c(modN)$
2. If $a \equiv b(modN)$, then $a + k \equiv b + k(modN)$ for any integer k
3. If $a \equiv b(modN)$ and $c \equiv d(modN)$, then $a + c \equiv b + d(modN)$
4. If $a \equiv b(modN)$, then $-a \equiv -b(modN)$
5. If $ab = c$, then $a(modN)b(modN) \equiv c(modN)$
6. If $a \equiv b(modN)$, then $ka \equiv kb(modN)$ for any integer k.
7. If $a \equiv b(modN)$ and $c \equiv d(modN)$, then $ac \equiv bd(modN)$.

Exercises

1. Find the sum of 31 and 148 in modulo 24.
2. Find the remainder when 123 + 234 + 32 + 56 + 22 + 12 + 78 is divided by 3
3. It is currently Wednesday 7:00 PM. What day of the way and time (in AM or PM) will it be in 12353 hours?
4. What is the remainder of 123456 × 345678 when divided by 17?
5. 124 × 134 × 23 × 49 × 235 × 13 is divided by 3
6. c) What is the last digit of 1234 × 5678?

To keep reading more, please have a look at: https://brilliant.org/wiki/modular-arithmetic

Modular Inverse

As in other sets of numbers and operations, it happens that they have identify element and inverse property. If every number is a set has corresponding number in that set for which they are operated together to result an identity element, for those two numbers, one is the inverse of the other. The same ideas applies here in modular arithmetic. The additive identity element is "zero" or "0". Its operations are simple. On the other hand, we have multiplicative identity element, which is "one" or "1". Then, symbolically, if

$$a * b = 1(modn),$$

Then, a is the inverse of b, and vice-verse modulo n. As this linear congruence only has a solution (we will see it later) if gcd(a,n) or gcd(b,n) is "1", then for b to exist, the gcd(a,n) should be "1". Good news! We can then calculate write our linear congruence as $ab + yn = 1$, for $y \in \mathbf{Z}$. Then, we are able to calculate the value of a or b if we know the other. Exercises

1. Does there exist of 4 modulo 6?
2. Does there exist of 5 module 7?
3. Find the inverse of 3 modulo 5?
4. Find the inverse of 19 modulo 29?

2.2.7 Linear Congruence

Definition

The linear congruence $ax \equiv b(modn)$, where a, b, n are given values and we aim to find x, has a solution if and only if $\gcd(a, n)|b$. For example, consider the linear congruence $102x \equiv 37(mod432)$. Since $gcd(102, 432) = 2 \not| 37$, there is no solution to $102x \equiv 37(mod432)$

Number of Solutions

The linear congruence $ax \equiv b(modn)$ with $gcd(a,n)|b$ has exactly $d = gcd(a,n)$ solutions modulo n. In particular, there is exactly one solution modulo n to the linear congruence $ax \equiv 1(modn)$ if gcd(a, n) = 1.

For example, consider the linear congruence 23x 7 mod 91. Since gcd(23, 91) = 1, it has only one solution modulo 91. For the linear congruence $35x \equiv 14(mod84)$, gcd(35, 84) = 7 and 7|14. So it has exactly 7 solutions modulo 84.

Useful steps while solving linear congruence

Suppose we want to solve: ax b mod n and assume that $b = kd$ where $d = gcd(a,n)$:

1. Find a single solution x0 for the linear congruence $ax \equiv b(modn)$,using the following observation: the linear congruence $ax \equiv b(modn)$ can be converted to the linear Diophantine equation $ax + nk = b$. Use the Euclidean algorithm from here.
2. . If x_0 is a solution to $ax \equiv b(modn)$, then all the solutions have the form $x = x_0 + m\frac{n}{d}$ or $x \equiv x_0(mod\frac{n}{d})$. For example, consider the linear congruence $35x \equiv 14(mod84)$. $gcd(35,84) = 7$ and 7|14, so it has solutions (and from above, we know that it has exactly 7 solution modulo 84). We now follow the above steps to find them.
3. Find a single solution x_0 the linear congruence $35x \equiv 14(mod84)$ by converting it to the linear Diophantine equation $35x + 84k = 14$, which is equivalent to $5x + 12k = 2$. By the Euclidean algorithm or by inspection, $x_0 = 2$ (and k = 1) is an integer solution.
4. All the solutions have the form $x = 2 + m * 12$, where m is any integer (here we take n = 84, d = 7) . Obviously, we can take m = 1 . . . 6, 7 to get solutions which are between 0 to 83 (note that from the above, the solution 2 of a linear congruence $ax \equiv b(modn)$, if it exists, will have the form $x \equiv x_0(modn)$ where $0 \leq x_0 \leq n-1$). They are $x \equiv 10(mod84), x \equiv 22(mod84), x \equiv 34(mod84), x \equiv 46(mod84), x \equiv 58(mod84), x \equiv 70(mod84), x \equiv 82(mod84)$. Note that, we know earlier that the linear congruence $35x \equiv 14(mod84)$ has exactly 7 solution modulo 84. We can also express all the solutions as $x \equiv -2(mod12)$.

Exercises

Find all solutions to the following linear congruences.

1. $2x \equiv 5(mod7)$
2. $6x \equiv 5(mod8)$
3. $234x \equiv 60(mod762)$
4. $128x \equiv 833(mod10001)$

2.2.8 Euler's Totient Function

Phi function and Totatives

Euler's totient function, also called the Phi function, counts the number of positive integers less than or equal to n that have no common factors with n (other than 1). $\phi(n) = |m \in 1, 2, ...n : gcd(m,n) = 1|$. We say that two numbers are relatively prime or coprime if their greatest common divisor is 1. We call these numbers less than or equal to n that have no common factors with n as the totatives of n- Euler's totient function counts the number of totatives.

For example, the totatives of $n = 9$ are the six numbers $1, 2, 4, 5, 7, 8$. Note that 3, 6 and 9 are not included, because their respective gcd's are different from 1. Note that $\phi(1) = 1$. Try to prove these outcomes.

1. $\phi(p) = p - 1$ for any prime p
2. $\phi(mn) = \phi(m)\phi(n)$ for any coprime integers m and n
3. $\phi(p^k) = p^{k-1}(p-1) = p^k(1 - \frac{1}{p})$ for any prime p
4. Combining the two above facts, by taking n in its prime-factorization $n = p_1^{\alpha_1}.p_2^{\alpha_2}.p_3^{\alpha_3}.\ldots.p_k^{\alpha_k}$, then $\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\ldots(1 - \frac{1}{p_k})$

Euler's Totient Theorem: For a relatively prime to m, we have $a^{\phi(n) \equiv 1(modn)}$, where ϕ is the Euler's totient functoin.
Fermat's Little Theorem: Let $gcd(a,p) = 1$, Then, we have $a^{p-1} \equiv 1(modp)$, where p is a prime. This is because $\phi(p) = p - 1$

Examples

1. Calculate $\phi(100)$
2. Calculate $\phi(29761)$
3. Find $128^{129} mod 17$
4. The number 2^{1000} is divided by 13. What is the remainder?

2.2.9 Chinese Remainder Theorem

The Chinese remainder theorem says that if one knows the remainders of the Euclidean division of an integer n by several integers, then one can determine uniquely the remainder of the division of n by the product of these integers, under the condition that the divisors are pairwise coprime. This can be written as:

Let b_1, b_2, b_n be pairwise coprime. In other words $gcd(b_i, b_j) = 1, \forall i \neq j$. Then, the system of linear congruence becomes,

$$x \equiv a_1(modb_1)$$
$$x \equiv a_2(modb_2)$$
$$...$$
$$x \equiv a_n(modb_n)$$

...has one distinct solution for x modulo $b_1 b_2 ... b_n$. We sometimes shorthand the "Chinese Remainder Theorem" to "CRT".

Example

Find the solution to the linear congruence

$$x \equiv 3(mod5)$$
$$x \equiv 4(mod11)$$

Solution Notice that we may write x in the form $5k + 3$ and $11m + 4$, so

$$x = 5k + 3 = 11m + 4$$

Taking this equation mod 5 we arrive at $11m + 4 \equiv 3(mod5) \Rightarrow m \equiv -1(mod5)$. Then $m = 5t - 1$ so $x = 55t - 11 + 4 = 55t - 7$. Thus the unique solution is $x \equiv -7(mod55)$.

Exercises

1. Find the smallest natural number that leaves a remainder of 4 when divided by 6, a remainder of 5 when divided by 7, and a remainder of 10 when divided by 11.

2.2.10 Challenging Problems

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

2. Prove that if p and p^2+2 are primes, then p^3+2 is also a prime.

3. Find the integer solutions, both x and y in:
   (a) $133x + 84y = 1$
   (b) $432x + 126y = 18$

4. Find the last 3 digits of 3^{100001}

5. Use linear congruence to show that if $n > 0$ has decimal expansion $a_k, a_{k-1} \dots a_1, a_0$. Then, $n \equiv a_0 - a_1 \dots + (-1)^k a_k (mod 11)$

6. For how many integer values of $i, 1 \leq i \leq 100$, does there exist an integer j where $1 \leq j \leq 1000$, such that i is a divisor of $2^j - 1$?

7. Prove that for every positive integer $n > 0$, 13 divides $11^{12n+6} + 1$

8. How many prime numbers p are there such that $29^p + 1$ is a multiple of p?

9. Find all positive integers n such that 21 divides $2^{2^n} + 2^n + 1$

2.3 PROBLEMS

(Easy) 1 What is the number of integers n for which $\frac{1}{7} \leq \frac{6}{n} \leq \frac{1}{n}$?

(Easy-Medium) 2 For how many pairs of digits (x, y) with $x \neq 0$ is the six-digit positive integer $x2315y$ divisible by 44?

(Medium) 3 For how many positive integers n with $n \leq 200$ is $486\dot{2}^{4n+1}$ a perfect fifth power?

(Hard) 4 The sum of the digits of the positive integer n is 123. The sum of the digits of $2n$ is 66. The digits of n include two $3s$, six $7s$, p $5s$, q $6s$ and no other digits. What is $p^2 + q^2$?

(Easy) 5 A two-digit positive integer x has the property that when 109 is divided by x, the remainder is 4. What is the sum of all such two-digit positive integers x?

(Easy-Medium) 6 If n is the smallest positive integer divisible by each of $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$ how many positive divisors does n have?

(Medium) 7 How many palindromes between 100 000 and 1 000 000 are multiples of 25?

(Hard) 8 Find the sum of all $x, 1 \leq x \leq 100$, such that 7 divides $x^2 + 15x + 1$

(Easy) 9 Sylvia chose positive integers a, b, and c.

- Peter determined the value of $\frac{a+b}{c}$ and got an answer of 101.
- Paul determined the value of $\frac{a+c}{c}$ and got an answer of 68.
- Mary determined the value of $\frac{(a+b)}{c}$ and got an answer of k.

What is the value of k?

(Easy-Medium) 10 Three distinct integers a, b and c satisfy the following three conditions:

- abc=17,955
- The a, b, c form an arithmetic sequence in that order, and
- (3a+b) (3b+c), and (3c+a) form a geometric sequence in that order.

What is the value of a + b + c?

(Medium) 11 How many pairs (x, y) of integers satisfy $18x + 30y = 2022$ and $xy > 1450$?

(Hard) 12 The integer $n = 3A4BC$ where A, B, and C are the thousands, tens, and units digits, respectively. Find all possible values of n for which n is a multiple of 220.

(Easy) 13 Dolly, Molly and Polly each can walk at 6 km/h. Their one motorcycle, which travels at 90 km/h, can accommodate at most two of them at once (and cannot drive by itself!). Let hours be the time taken for all three of them to reach a point 135 km away. Ignoring the time required to start, stop or change directions, what is true about the approximate smallest possible value of t?

(Easy-Medium) 14 If n is a positive integer, the symbol$n!$ (read "n factorial") represents the product of the integers from 1 to$n$. For example, $4! = (1)(2)(3)(4)$ or $4! = 24$. If x and y are integers and $\frac{30!}{36^x 25^y}$ is equal to an integer, what is the maximum possible value of $x + y$?

(Medium) 15 How many lattice points lie on the perimeter of the triangle with vertices $A(2, 1), B(54, 27), C(15, 53)$?

(Hard) 16 Find the sum of all $x, 1 \leq x \leq 100$, such that 7 divides $x^2 + 15x + 1$

(Easy) 17 Suppose that 2009/2014+2019/n=a/b, where a, b, and n are positive integers with a/b in lowest terms. What is the sum of the digits of the smallest positive integer n for which a is a multiple of 1004?

(Easy-Medium) 18 For any real number $\lfloor x \rfloor$ denotes the largest integer less than or equal to x. For example, $\lfloor 4.2 \rfloor$=4 and $\lfloor 0.9 \rfloor$=0. Let S be the sum of all integers with $1 \leq k \leq 999,999$ and for which k is divisible by $\lfloor \sqrt{k} \rfloor$. Find the value of S?

(Medium) 19 In the addition $XXX + YYY + ZZZ = ZYYX$, the letters X, Y, and Z each represent a different non-zero digit. The digit X is

(Hard) 20 A positive integer has k trailing zeros if its last k digits are all zero and it has a non-zero digit immediately to the left of these k zeros. For example, the number 1 030 000 has 4 trailing zeros. Define $Z(m)$ to be the number of trailing zeros of the positive integer m. Lloyd is bored one day, so makes a list of the value of $n - Z(n!)$ for each integer n from 100 to 10 000, inclusive. How many integers appear in his list at least three times? (Note: If n is a positive integer, the symbol $n!$ (read "n factorial") is used to represent the product of the integers from 1 to n. That is, $n! = n(n-1)(n-2)(3)(2)(1)$. For example, $5! = 5(4)(3)(2)(1) or 5! = 120$.)

Chapter 3

GEOMETRY

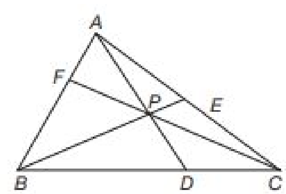
3.1 CEVA'S THEOREM

3.1.1 Introduction

This theorem is most of times used to prove that different lines meet at a given point by using side proportion or ratios. [3]

3.1.2 key idea of the theorem

if points D,E,F are taken onthe sides BC,CA,AB of triangle ABC so that the lines AD,BE,CF are concurrent at a point P,then



$$\frac{BD}{DC}.\frac{CE}{EA}.\frac{AF}{FB} = 1$$

AND trying to prove this theorem lets use areas

$$\frac{[ABD]}{ADC} = \frac{BD}{DC}$$

(1) and

$$\frac{[BPD]}{[CPD]} = \frac{BD}{DC}$$

(2) from eqs (1) and (2)

$$\frac{BD}{DC} = \frac{[ABD]}{[ADC]} = \frac{[BPD]}{[CPD]} = \frac{[ABD] - [BPD]}{[ADC] - [CPD]} = \frac{[ABP]}{[ACP]}$$

let

$$[BPC] = D_1$$

,

$$[ACP] = D_2$$

and

$$[ABP] = D_3$$

then

$$\frac{BD}{DC} = \frac{D_3}{D_2}$$

similarly

$$\frac{CE}{EA} = \frac{[BPC]}{APB} = \frac{D_1}{D_3}$$

AND

$$\frac{AF}{FB} = \frac{[APC]}{[BPC]} = \frac{D_2}{D_1}$$

THEN

$$\frac{BD}{DC}.\frac{CE}{EA}.\frac{AF}{FB} = \frac{D_3}{D_2}.\frac{D_1}{D_3}.\frac{D_2}{D_1} = 1$$

PROVED!

3.2 MENELAUS THEOREM

3.2.1 Introduction

In this theorem we will use sides proportionality to prove whether three points are collinear on transversal line through triangle. [3]

3.2.2 Key idea of the theorem

if a transversal cuts the sides BC,CA,AB of a triangle ABC at X,Y,Z respectively then

$$\frac{BX}{XC}.\frac{CY}{YA}.\frac{AZ}{ZB} = -1$$

proof; leth_1, h_2, h_3, be the length of perpendincural AP,BQ,CR respectively from A,B,C on transversal. lets

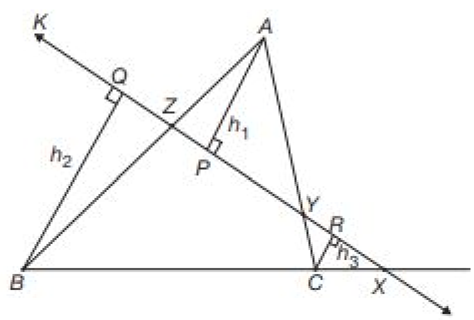


Figure 3.1: Caption

prove this by using similarity such that $\triangle$ CRY IS similar to $\triangle$APY where

$$\frac{CY}{YA} = \frac{CR}{AP} = \frac{h_3}{h_1}$$

and let consider $\triangle$ BQX which is similar to $\triangle$BCX then

$$\frac{BX}{XC} = \frac{BQ}{CR} = \frac{h_2}{h_3}$$

again consider triangle APZ which is similar to BQZ then

$$\frac{AZ}{ZB} = \frac{AP}{BQ} = \frac{h_1}{h_2}$$

now we cad deduce that

$$\frac{BX}{XC} \cdot \frac{CY}{YA} \cdot \frac{AZ}{ZB} = \frac{h_2}{h_3} \cdot \frac{h_3}{h_1} \cdot \frac{h_1}{h_2} = 1$$

as the per the directed segments we have BX is positive and XC is negative. therefore $\frac{BX}{XC}$is negative and the other two ratios are positive. then

$$\frac{BX}{XC} \cdot \frac{CY}{YA} \cdot \frac{AZ}{ZB} = -1$$

proved!

3.3 PTOLEMY'S THEOREM

3.3.1 Introduction

We use this theorem to prove equality where multiples of diagonals equal to addition of multiples of opposite sides of cyclic quadrilateral. [3]

3.3.2 Key idea of the theorem

in cyclic quadrilateral the product of the diagonals is equal to the sum of the products of the pairs of opposite sides. proof: Given ABCD is a cyclic quadrilateral to prove that

$$AB.CD + AD.BC = AC.BD$$

to prove this we use a hint saying that; you insert point E on line BD such that angle

$$< ADE =< CAB$$

to prove this identity lets use similar triangles obtained here $\triangle$ ABE is similar to $\triangle$ADC hence

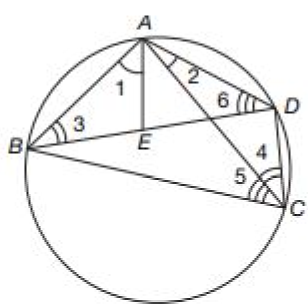


Figure 3.2: cyclic quadz

$$\frac{BE}{DC} = \frac{AB}{AC}$$

OR

$$AB.CD = AC.BE$$

(1) also consider $\triangle$ABC which is similar to $\triangle$ AED then

$$\frac{BC}{ED} = \frac{AC}{AD}$$

OR

$$BC.AD = AC.AE$$

(2) Adding corresponding sides of equations (1) and (2)

$$AB.CD + AD.BC = AC.BE + AC.ED$$

i.e,

$$AB.CD + AD.BC = AC(BE + ED)$$

THEN

$$AB.CD + AD.BC = AC.BD$$

PROVED!

3.4 BRAMHAGUPTA'S THEOREM

3.4.1 Introduction

In any triangle product of any two sides is equal to the product of the perpendicular drawn to the third side with circum-diameter. [3]

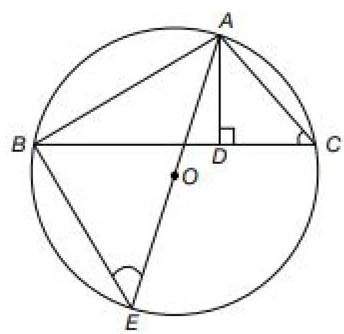


Figure 3.3:

In $\triangle$ ABC, AD$\perp$ BC. Let O be the circum-centre. Join AO and produced it to cut circu-mcircle at E, then AE is the diameter and

$$\angle ABE = 90°$$

. ° In $\triangle$ABE and $\triangle$ADC

$$\angle ABE = \angle ADC = 90°$$

$$\angle AEB = \angle ACD$$

(Angles in the same segment)

then By AA similarly,$\triangle ABE \sim \triangle ADC$.

$$\frac{AB}{AD} = \frac{AE}{AC}$$

$$\rightarrow AB.AC = AE.AD$$

$$\rightarrow AB.AC = 2R.AD$$

$$REQUIREDPROOF!$$

3.5 INTERSECTING CHORDS THEOREM

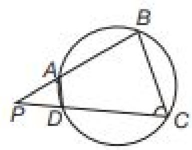
3.5.1 Introduction

If a line L through P intersects a circle ω at two points A and B, the product $PA.PB$ (of signed lengths) is equal to the power of P with respect to the circle.

More over if there are two lines through P one meets circle ω at points A and B, and let another line meets circle Ω at points C and D. Then

$$PA.PB = PC.PD$$

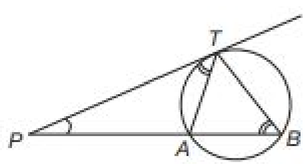
[3]



3.6 TANGENT SECANT THEOREM

3.6.1 Introduction

If through a point outside a circle a tangent and a chord be drawn. The square of the length of the tangent is equal to the rectangle contained by the segments of the chord. [3] proof: in$\triangle$PTA and $\triangle$PBT



$$\angle TPA = \angle BPT$$

$$\angle PTA = \angle PBT$$

(alternate segment theorem)

then by AA similarly

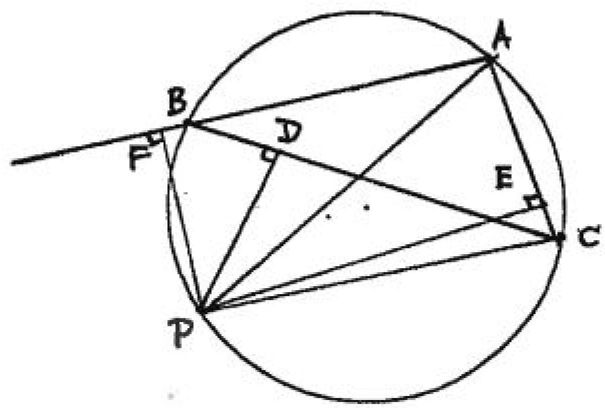
$$\triangle PTA \sim \triangle PBT$$

THEN

$$\frac{PT}{PB} = \frac{PA}{PT}$$

THEN

$$PT^2 = PB.PA$$



3.7 SIMPSON'S THEOREM

3.7.1 Introduction

let ABCP be a concyclic and let D,E,and F,respectively, be the feet of perpendiculars from P on BC,CA,and AB, respectively. then D,E,and F are collinear. [3]

proof:

$$| BD |=| BP | cos\angle CBP$$

$$| DC |=| CP | cos\angle BAP$$

$$| CE |=| CP | cos\angle ACP$$

$$| EA |=| AP | cos\angle CBP$$

$$| AF |=| AP | cos\angle BAP$$

$$| FB |=| BP | cos\angle ACP$$

THEN

$$\frac{| BD |}{| DC |}.\frac{| CE |}{| EA |}.\frac{| AF |}{| FB |} = 1$$

thus D,E,F are collinear, by the converse to menelous theorem

3.8 NINE POINT CIRCLE THEOREM

3.8.1 Introduction

The circle through the mid-points of the sides of a triangle also passes through the feet of the altitudes and the mid-points of the lines joining the orthocentre to the vertices. This circle is called the nine point circle of the triangle as there are nine fixed points on it, namely three mid-points of sides, three feet of altitudes, three mid-points of line segment joining the orthocentre and vertex. [3] To prove: There is one circle passes through D, E, F, X, Y, Z, P, Q, R In $\triangle$ ABH, P, F are the mid-points of AH and AB respectively By mid-point theorem PF$\|$ BH, i.e., PF$\|$ BY. In $\triangle$ ABC, F, D are the mid-points of AB, BC respectively By mid-point theorem FD$\|$ AC

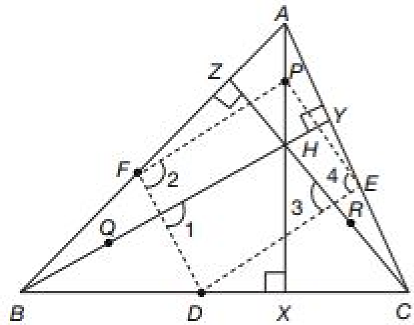
$$\angle 1 = \angle CYB = 90^\circ$$

(Interior angles) Also

$$\angle 2 = \angle 1 = 90^\circ$$

(Corresponding angles) i.e.,

$$\angle PFD = 90^\circ$$



(1) also

$$\angle PXD = 90^\circ$$

° (2) Now In △ AHC, P, E are the mid-points of AH, AC respectively By mid-point theorem PE‖ HC i.e., PE‖ ZC In △ ABC, E, D are the mid-points of AC, CB respectively By mid-point theorem DE‖ AB

$$\angle BZC = \angle 3 = 90^\circ$$

(Interior angles) Also

$$\angle 4 = \angle 3 = 90^\circ$$

° (Corresponding angles)

$$\angle PED = 90^\circ$$

° (3) From Eqs. (1), (2) and (3) Taking PD as a diameter if we draw a circle then it must passes through F, X and E

$$\angle PFD = \angle PXD = \angle PED = 90^\circ$$

. i.e., P, F, D, X, E are concyclic. Similarly Q, D, E, Y, F are concyclic and R, E, Z, F, D are concyclic. Since out of these, three point D, E, F are common and since from any three non collinear points, there passes one and only one circle. P, Q, R, D, E, F, X, Y, Z are concyclic it is a nine point circle

3.9 EXERCISES

1. In the triangle ABC,AB=AC.THe altitude AD of the triangle meets the circumcircle at P. Prove that AP.BC=2 AB.AP

2. prove that medians and altitudes of triangle meet at the same point

3. let ABC be a triangle and let D,E,F be the points on its sides such that starting at A.D divides the perimeter of the triangle into two equal parts starting at B,E divides the perimeter of the triangle into two equal parts at C. F divides the perimeter of triangle into two equal parts.prove that D,E,F lie on the sides BC,CA,AB respectively and the lines AD,BE,CF are concurrent.

4. prove Ceva's theorem by using similar triangles

5. on the sides BC,CA,AB of triangle ABC.Points D,E,F are taken in such a way that

   $$\frac{BD}{DC} = \frac{CE}{EA} = \frac{AF}{FB} = \frac{2}{1}$$

   show that the area of the triangle determined by the lines AD,BE,CFis $\frac{1}{7}$ of area of triangle ABC

6. ABCD is a cyclic quadrilateral. Prove the result:

   $$AC(AB.BC + CD.DA) = DA(AB.DA + CB.CD)$$

7. A circle has centre on the side AB of the cyclic quadrilateral ABCD. The other three sides are tangent to the circle. Prove that
$$AD + BC = AB$$
. [IMO, 1985]

8. A circle cuts the sides of △ ABC internally as follows; BC, at D,D'; CA at E, E' and AB at F', F. If AD, BE, CF are concurrent, prove that AD', BE', CF' are concurrent

9. Let BD be the internal angle bisector of angle B in triangle ABC with D on side AC. The circumcircle of triangle BDC meets AB at E, while the circumcircle of triangle ABD meets BC at F. Prove that AE = CF

10. let ABC be an acute triangle,le BE and CF be the altitudes of triangle ABC and denote M the midpoint of segment BC.prove that segments ME,MF and the line through A parallel to BC are all parallel to circumcircle of triangle AEF

3.10 POWER OF POINT

3.10.1 Introduction

Letω be a circle with centre O and radius r, and let P be a point. The power of P with respect toω is defined to be the difference of squared length $PO^2 - r^2$ This is positive, zero, or negative according as P is outside, on, or inside the circle ω.

EXPLANATION

Let line PO meet the circle ω at points A and B, so that AB is a diameter. Here we will be using directed lengths which is as follows: For three collinear points P, A, B, If PA and PB point in the same direction, then we will take PA and PB of same sign

$\rightarrow PA \cdot PB$ is positive. If PA and PB point in the opposite direction, then we will take PA and PB of opposite sign

$\rightarrow PA \cdot PB$ is negative.

Now, $PA \cdot PB = (PO + OA)(PO + OB) = (PO - r)(PO + r) = PO^2 - r^2$,

$\rightarrow PA \cdot PB = PO^2 - r^2$ (1)

Which is the power of the point P. Observe the right hand side of the Eq. (1), If P lies inside the circle, then $PO < r$, which forces $PO^2 - r^2$ to be negative and If P lies outside the circle, then $PO > r$, which forces $PO^2 - r^2$ to be positive [t]

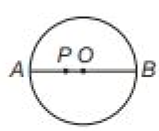


Figure 3.4: first Case

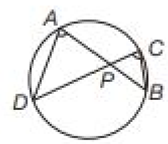
the other diagram p will be outside the circle

3.10.2 More details

the power of point can be used also on any point inside the circle to all different chords passing through it,it will remain with the same power. Example:

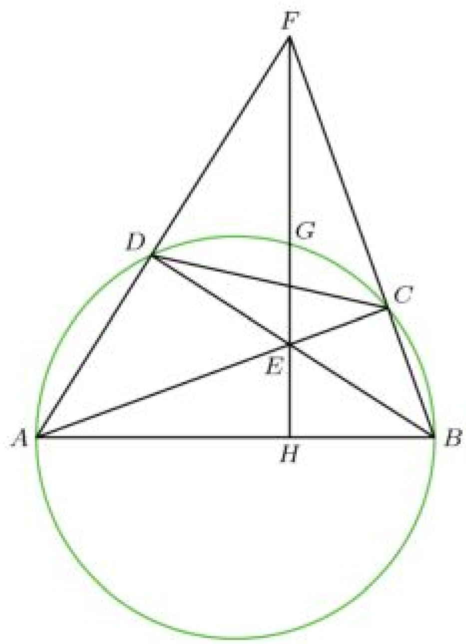
here the power of point p will be $PA \cdot PB$=$PD \cdot PC$

now its seen that power of point can be used also to find similar triangles inside circle here similar triangles meet at same point with constant power.



3.10.3 Solved example

Let ABCD be a convex quadrilateral inscribed in a semicircle with diameter AB. The lines AC and BD intersect at E and the lines AD and BC meet at F. The line EF meets the semicircle at G and AB at H. Prove that E is the midpoint of GH if and only if G is the midpoint of the line segment F H. Proof. Note



that $\angle ADB = \angle ACB = 90^0$. It follows that E is the orthocenter of F AB and $\angle FAH = 90^0$. We obtain many similar triangles, with one notable one begin $\triangle AEH = FBH$ which gives the relation

$$HE \cdot HF = HA \cdot HB.$$

However, note that

$$Pow(H) = HG^2 = HA \cdot HB$$

, so it follows that

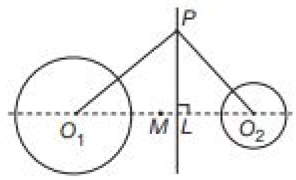
$$\frac{HG}{HF} = \frac{HE}{HG}$$

which proves the result.

3.11 RADICAL AXIS

3.11.1 Introduction

Let $\omega1$ and $\omega2$ be two nonconcentric circles, then the locus of point with equal power with respect to both $\omega1$ and $\omega2$, is a line, called their radical axis. It is perpendicular to line joining centres of the circles.



proof

Proof: Let $\omega 1$ and $\omega 2$ be two circles with different centres O_1 and O_2, and radii r_1 and r_2 respectively. Letr $r_1 \geq r_2$. Let P be a point on the locus, then

$$PO_1^2 - r_1^2 = PO_2^2 - r_2^2$$

(given) 1

Now join PO_1, PO_2 and O_1O_2 and draw perpendicular from P to O_1O_2. Let L be the foot of the perpendicular. Also assume M be the mid point of O_1O_2. Now,

$$PO_1^2 - r_1^2 = O_1L^2 + PL^2 - r_1^2$$

(Using Baudhayna theorem) (2) Also

$$PO_2^2 - r_2^2 = O_2L^2 + PL^2 - r_2^2$$

(Using Baudhayna theorem) (3) From Eqs. (1), (2) and (3), we get,

$$O_1L^2 + PL^2 - r_1^2 = O_2L^2 + PL^2 - r_2^2$$

$\rightarrow$

$$O_1L^2 - O_2L^2 = r_1^2 - r_2^2$$

$\rightarrow$

$$(O_1L - O_2)(O_1 + O_2) = r_1^2 - r_2^2$$

$\Rightarrow$

$$(O_1M + ML) - (O_2M - ML)(O_1O_2) = r_1^2 - r_2^2$$

(As M is the mid-point of O_1O_2) $\rightarrow$

$$2ML \cdot O_1O_2 = r_1^2 - r_2^2$$

$\rightarrow$ L is a fixed point

$\rightarrow$For any point P on the locus foot of perpendicular on O_1O_2 is always fix point L.

$\rightarrow$ Locus is a straight line perpendicular to O_1O_2.

3.11.2 Radical center

INTRODUCTION

Let $\omega 1$, $\omega 2$ and $\omega 3$ be three circles such that their centres are not collinear and no two concentric. Then their three pairwise radical axes are concurrent and point of concurrency is called radical centre.

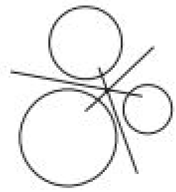
proof

Proof: Denote the three circles by $\omega 1$, $\omega 2$, and $\omega 3$, and denote the radical axes of ω_i and ω_j by l_{ij}. As centres are non collinear, no two radical axis is parallel.

Let l_{12} and l_{13} meet at P. Since P lies on l_{12}, it has equal powers with respect to ω_1 and ω_2.

Similarly since P lies on l_{13}, it has equal powers with respect to ω_1 and ω_3.

Therefore, P has equal powers with respect to all three circles, and hence it must lie on l23 as well Note: If centres are collinear then their three pairwise radical axes are parallel(here all students are assigned to make their clear proof considering that hint)



3.12 INVERSION IN GEOMETRY

Inversion is a transformation used in geometry that involves a specific type of reflection with respect to a circle (or a sphere in 3D). It is a powerful technique that has applications in various branches of geometry, especially in complex analysis and projective geometry. Inversion is commonly studied in the context of Euclidean geometry.

The basic idea of inversion is to transform points in the plane with respect to a fixed circle (or sphere in 3D). Given a circle (or sphere) with center O and radius r, the inversion of a point P not on the circle (or sphere) is a new point P' such that the following properties hold:

1. The line containing O and P' passes through P, and the line containing O and P passes through P'.
2. The product of the distances from O to P and P' is equal to the square of the radius r:

$$|OP| \cdot |OP'| = r^2$$

In other words, the inversion swaps points inside the circle (or sphere) with points outside, while leaving the points on the circle (or sphere) fixed.

Some important properties of inversion include:

1. Circles (or spheres) that do not pass through the center of inversion are transformed into circles (or spheres).
2. Circles (or spheres) that pass through the center of inversion are transformed into straight lines (planes in 3D) that do not intersect the center of inversion.
3. Lines (planes in 3D) that pass through the center of inversion are transformed into circles (spheres) that do not intersect the center of inversion.
4. The inversion of a circle through the center of another circle results in a straight line.

Inversion is a powerful tool in solving geometry problems, especially those involving angles, circles, and configurations of points and lines. It can help simplify complex configurations and reveal hidden symmetries in the problem.

3.13 PROBLEMS

1. Given circles ω_1 and ω_2 intersecting at points X and Y, let l_1 be a line through the centre of ω_1 intersecting ω_2 at points P and Q and let l_2 be a line through the centre of ω_2 intersecting ω_1 at points R and S. Prove that if P, Q, R and S lie on a circle then the centre of this circle lies on line XY.(USA MO,2009)
2. Let H be the orthocentre of acute angle triangle ABC. The tangents from A to the circle with diameter BC touch the circle at P and Q. Prove that P, Q, H are (China MO,1996) collinear
3. Let A, B, C and D be four distinct points on a line, in that order. The circles with diameters AC and BD intersect at the points X and Y. The line XY meets BC at the point Z. Let P be a point on the line XY different from Z. The line CP intersects the circle with diameter AC at the points C and M, and the line BP intersects the circle with diameter BD at the points B and N. Prove that the lines AM, DN and XY are concurrent. (IMO, 1995)

4. A circle with centre O passes through the vertices A and C of triangle ABC and intersects the segments AB and BC again at distinct points K and N, respectively. The circumscribed circles of the triangles ABC and KBN intersect at exactly two distinct points B and M. Prove that angle OMB is a right angle. [IMO, 1985]

5. Prove that three radical axes meet at the same point for non collinear centers

Chapter 4

COMBINATORICS

4.1 INTEGRAL SOLUTIONS

4.1.1 Number of non-negative integral solutions of a linear equation

Give the equation $x_1 + x_2 + \cdots + x_k = n$, let A be the set of non-negative integral solutions and B be the set of all $(n + k - 1)$ term binary sequences containing $n, 1^{'} s \text{and} (k - 1), 0^{'} s$. The number of $1^{'} s$ before the first zero is the value of x_1, the number of $1^{'} s$ between first and second zero is the value of x_2, and so on, number of $1^{'} s$ after the $(k - 1)th$ zero is the value of x_k.

Therefore, the number of non-negative integral solutions of the equation is the same as the number pf binary sequences.

$$\text{Number of non-negative integral solutions} = \binom{n+k-1}{k-1} = \frac{(n+k-1)!}{n!(k-1)!}$$

Examples

1. Find the number of non-negative integral solutions of $x_1 + x_2 + x_3 + x_4 = 9$.

   The total number of $1^{'} s$ is $n = 9$ and $0^{'} s$ are $k - 1 = 3$, giving us $9 + 3 = 12$ items to arrange, 9 of which are of one type and 4 of which are of another type.

   $$\text{Total number of arrangements} = \frac{12!}{9!3!} = \frac{12 \times 11 \times 10}{3 \times 2 \times 1} = 220$$

   Number of non-negative integral solutions = Total number of binary sequences of $9, 1^{'} s$ and $3, 0^{'} s$

2. Find the number of positive integral solutions of $x_1 + x_2 + x_3 + x_4 = 9$

   For this case, we're interested in positive solutions, which means that each x_i must have minimum value 1.

   So, we assign one $1^{'} s$ to each x_i, leaving $5, 1^{'} s$. Now the problem is similar to finding the number of non-negative integral solutions of:

   $$x_1 + x_2 + x_3 + x_4 = 5$$

   Total number of $1^{'} s$ is $n = 5$ and $0^{'} s$ are $k - 1 = 3$, giving us $5 + 3 = 8$ items to arrange, 5 of which are of one type and 3 of which are of another type.

   $$\text{Number of positive integral solutions} = \frac{8!}{5!3!} = \frac{8 \times 7 \times 6}{3 \times 2 \times 1} = 56$$

4.1.2 Number of non-negative integral solutions of a linear inequality

Given the inequality

$$x_1 + x_2 + \cdots + x_k \leq n \tag{4.1}$$

Add a non-negative integer x_{k+1} to get

$$x_1 + x_2 + \cdots + x_k + x_{k+1} = n \tag{4.2}$$

Number of solutions of Eq.4.1 $= \binom{n+k}{k} = \frac{(n+k)!}{n!k!}$

4.1.3 Number of integral solutions of a linear equation in $x_1,\ x_2,\ \cdots,\ x_k$ when $x_i^{'}$ are constrained

Given the equation

$$x_1 + x_2 + \cdots + x_k = n \tag{4.3}$$

where $x_1 \geq y_1,\ x_2 \geq y_2,\ \cdots,\ x_k \geq y_k$, for $y_i \in \mathbb{Z}$

By taking $x_1 = y_1 + x_1^{'},\ x_2 = y_2 + x_2^{'},\ \cdots,\ x_k = y_k + x_k^{'}$ where $x_i^{'} \geq 0$ for $1 \leq i \leq k$

Eq.4.3 becomes

$$(y_1 + y_2 + \cdots + y_k) + (x_1^{'} + x_2^{'} + \cdots + x_k^{'}) = n$$

$$\iff x_1^{'} + x_2^{'} + \cdots + x_k^{'} = n - (y_1 + y_2 + \cdots + y_k) \tag{4.4}$$

Therefore, for every solution of Eq.4.3, we can write a corresponding solution of Eq.4.4and vice versa. Hence, there is a bijection between the sets of solutions of Eqs.4.3 and ref4.

Number of solutions of Eq.4.3 $=$ Number of non-negative integral solutions of Eq.4.4 $= \dfrac{(n+k-1-(y_1+y_2+\cdots+y_k))!}{(k-1)!(n-(y_1+y_2+\cdots+y_k))!}$

Examples

1. Find the number of integral solutions of $x_1 + x_2 + x_3 + x_4 + x_5 = 17$ where $x_1 \geq -2,\ x_2 \geq 1,\ x_3 \geq 2,\ x_4 \geq 0,$ and $x_5 \geq -1$

   Let

   $$x_1 = -2 + x_1^{'},\ x_2 = 1 + x_2^{'},\ x_3 = 2 + x_3^{'}, x_4 = 0 + x_4^{'},\ x_5 = -1 + x_5^{'}$$

   where $x_1^{'},\ x_2^{'}, x_3^{'},\ x_4^{'}, x_5^{'} \geq 0$

   Our equation becomes

   $$(x_1^{'} + x_2^{'} + x_3^{'} + x_4^{'} + x_5^{'}) + (-2 + 1 + 2 + 0 - 1) = 17$$

   $$x_1^{'} + x_2^{'} + x_3^{'} + x_4^{'} + x_5^{'} = 17 \tag{4.5}$$

   Number of non-negative integral solutions of Eq.4.5 $=$ Number of integral solutions of the given equation $= \dfrac{21!}{17!4!} = \dfrac{21 \times 20 \times 19 \times 18}{4 \times 3 \times 2 \times 1} = 5985$

2. How many integral solutions are there such that $x+y+z+t=30$, when $x \geq 1$, $y \geq 2$, $z \geq 3$, and $t \geq 4$?
   Let
   $$x = 1 + x^{'},\ y = 2 + y^{'},\ z = 3 + z^{'},\ \text{and}\, t = 4 + t^{'}$$
   where $x^{'}, y^{'}, z^{'}, t^{'} \geq 0$

   Our equation becomes
   $$\begin{aligned}(x^{'} + y^{'} + z^{'} + t^{'}) + (1+2+3+4) &= 30\\ x^{'} + y^{'} + z^{'} + t^{'} &= 20\end{aligned}$$

   Number of integral solutions $= \dfrac{23!}{20!3!} = \dfrac{23 \times 22 \times 21}{3 \times 2 \times 1} = 1771$
3. How many integral solutions are there for $x_1 + x_2 + x_3 + x_3 + x_4 + x_5 = 25$ and $x_1 + x_2 + x_3 = 7$ when $x_1, x_2, x_3, x_4, x_5 \geq 0$
   From the given equations
   $$x_1 + x_2 + x_3 = 7 \tag{4.6}$$
   $$x_4 + x_5 = 18 \tag{4.7}$$

   Since Eqs.4.6 and 4.7 correspond to each other,
   Total number of integral solutions = Number of solutions of Eq.4.6 $\times$ Number of solutions of Eq.4.7 $= (\dfrac{9!}{7!2!}) \times (\dfrac{19!}{18!1!}) = \dfrac{9 \times 8}{2 \times 1} \times \dfrac{19}{1} = 684$

4.1.4 Exercises

1. Find the number of ways to select 10 balls from an unlimited number of red, white, blue and green balls.
2. Find the number of ordered triples of positive integers which are solutions of the equation $x+y+z=100$.
3. Let $x_i \in \mathbb{Z}$, such that $|x_1| + |x_2| + \cdots + |x_{10}| = 10$. Find number of solutions.
4. Let $x_i \in \mathbb{Z}$ such that $|x_1 x_2 \cdots x_{10}| = 1080000$. Find number of solutions.
5. Let y be an element of the set $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$ and x_1, x_2, x_3 be positive integers such that $x_1 x_2 x_3 = y$, then find the number of positive integral solutions pf $x_1 x_2 x_3 = y$.
6. The minimum marks required for clearing a certain screening paper is 210 out of 300. The screening paper consists of '3' sections each of Physics, Chemistry and Mathematics Each section has 100 as maximum marks. Assuming there is no negative marking and marks obtained in each section are integers, find the number of ways in which a student can qualify the examination (Assuming no subjectwise cut-off limit).
7. In how many different ways can 3 persons A, B and C having 6 one rupee coins, 7 one rupee coins and 8 one rupee coins respectively donate 10 one rupee coins collectively.
   (a) If each one giving at least one coin
   (b) If each one can give '0' or more coin.

   Also answer the above questions for 15 rupees donation.

4.2 PROOF BY INDUCTION

4.2.1 Introduction

Let a be an integer and $P(n)$ be a statement about n for each integer $n \geq a$. The principle of induction is a way of proving that $P(n)$ is true for all integers $n \geq a$. This principle is very useful in problem solving, especially when we observe a pattern and want to prove it.

It works in two steps:

- **Basic case**: Prove that $P(a)$ is true
- **Inductive step**: Assume that $P(k)$ is true for some integer $k \geq a$, and use this to prove that $P(k+1)$ is true. Then we may conclude that $P(n)$ is true for all integers $n \geq a$.

The trick to using the principle of induction is to figure out how to use $P(k)$ to prove $P(k+1)$. Sometimes, this might be done rather ingeniously.

4.2.2 Examples

1. Prove that $1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$

   Let $P(n)$ denote the statement to be proved.

   - **Basic case:**
     Let's examine $P(1)$: this gives us $1 = \dfrac{1(2)}{2} = 1$ which is correct
   - **Inductive step:**
     Now, we assume that $P(k)$ is true for some positive integer k

     $$\implies P(k) = 1 + 2 + \cdots + k = \frac{k(k+1)}{2} \tag{4.8}$$

     And we want to prove that $P(k+1) = \frac{(k+1)(k+2)}{2}$
     By using Eq.4.8,

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

     which completes our proof.
     This means that if $P(1)$ is true, then $P(2)$ is also true, and since $P(2)$ is true, then $P(3)$ is also true, and so on.

2. Find a formula for the sum of the first n odd numbers.

   We notice that for this problem, we're not told to prove a general formula, rather we have to find it ourselves.

Let us try some small cases:

$$\begin{aligned}
1 &= 1 = 1^2 \\
1+3 &= 4 = 2^2 \\
1+3+5 &= 9 = 3^2 \\
1+3+5+7 &= 16 = 4^2 \\
1+3+5+7+9 &= 25 = 5^2 \\
1+3+5+7+9+11 &= 36 = 6^2
\end{aligned}$$

We guess that the sum of n odd numbers is equal to n^2. Now, let's prove this proposition $P(n) = n^2$ by using the principle of induction.

- **Base case:**
  $P(1) = 1 = 1^2$ which is true
- **Inductive step:**
  Let's assume that $P(k)$ is true for some positive integer k

  $$\implies P(k) = 1 + 3 + 5 + \cdots + (2k-1)$$

  From the above equation, for $n = k+1$,

  $$\begin{aligned}
  P(k+1) &= 1 + 3 + 5 + \cdots + (2k-1) + (2K+1) \\
  &= P(k) + (2k+1) \\
  &= k^2 + 2k + 1 \\
  &= (k+1)^2
  \end{aligned}$$

  Hence proved that $P(k) \implies P(k+1)$ is true, which completes our proof.

3. Show that $7^{2n} + (2^{3n-3})(3^{n-1})$ is divisible by 25 for all $n \in \mathbb{N}$
   Let $P(n) = 7^{2n} + (2^{3n-3})(3^{n-1})$

   - **Base case:**
     $P(1) = 7^2 + (2^0)(3^0) = 50$, which is divisible by 25
   - **Inductive step:**
     Let $P(k)$ be true such that $7^{2k} + (2^{3k-3})(3^{k-1})$ is divisible by 25
     From the above,

     $$\begin{aligned}
     P(k+1) &= 7^{2(k+1)} + (2^{3(k+1)-3})(3^{k+1-1}) \\
     &= (24+25)7^{2k} + 24(2^{3k-3})(3^{k-1}) \\
     &= 24(7^{2k} + 2^{3k-3} \cdot 3^{k-1}) + 25 \cdot 7^{2k} \\
     &= 24P(k) + 25 \cdot 7^{2k}
     \end{aligned}$$

     And we know that $P(k)$ is divisible 25. Also, $25 \cdot 7^{2k}$ is clearly divisible by 25. Hence $P(k+1)$ is divisible by 25. So, by mathematical induction, our proposition is true for all n.

4. Prove by induction that if $n \geq 10$, then $2^n > n^3$.

- **Basic case:**
  For $n = 10$, we have $2^10 = 1024 > 10^3 = 1000$ which is true
- **Inductive step:**
  Let's assume that our statement is true for $n = k \geq 10$,

$$2^k > k^3 \implies 2^{k+1} > 2k^3$$

by doubling both sides
Now $2k^3 - (k^3 + 3k^2 + 3k + 1) = (k-1)^3 - 6k$
Let $k = 10 + a$, where $a \geq 0$
Then

$$\begin{aligned}(k-1)^3 - 6k &= (10 + a - 1)^3 - 6(10 + a) \\ &= (a+9)^3 - 60 - 6a \\ &= 729 + 243a + 27a^2 + a^3 - 60 - 6a \\ &= 669 + 183a + 27a^2 + a^3 \geq 0 \text{as} a \geq 0\end{aligned}$$

Hence

$$2k^3 - (k^3 + 3k^2 + 3k + 1) \geq 0$$
$$2k^3 - (k-1)^3 \geq 0 2^{k+1} \geq 2k^3 \qquad \geq (k-1)^3$$

Hence the inequality is true for all $n \geq 10$

5. Show using mathematical induction that

$$\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{3n+1} > 1$$

for all natural numbers n

- **Base case:**
  For $n = 1$, $\frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{6+3+4}{12} = \frac{13}{12} > 1$ is true
- **Inductive step:**
  We assume that our proposition is true for $n = k$

$$\implies \frac{1}{k+1} + \frac{1}{k+2} + \cdots + \frac{1}{3k+1} > 1$$

For $n = k + 1$,

$$\begin{aligned}&\frac{1}{k+2} + \frac{1}{k+3} + \cdots + \frac{1}{3k+1} + \frac{1}{3k+2} + \frac{1}{3k+3} + \frac{1}{3k+4} \\ &= \left(\frac{1}{k+1} + \frac{1}{k+2} + \cdots \frac{1}{3k+1}\right) + \left(\frac{1}{3k+2} + \frac{1}{3k+4} - \frac{2}{3k+3}\right) \\ &> 1 + \left(\frac{1}{3k+2} + \frac{1}{3k+4} - \frac{2}{3k+3}\right)\end{aligned}$$

Now, if $1 + \left(\frac{1}{3k+2} + \frac{1}{3k+4} - \frac{2}{3k+3}\right) > 1$, then we would be done.

Meanwhile,

$$1 + \left(\frac{1}{3k+2} + \frac{1}{3k+4} - \frac{2}{3k+3}\right)$$

$$= \frac{(3k+4)(3k+3) + (3k+2)(3k+3) - 2(3k+2)(3k+4)}{(3k+2)(3k+3)(3k+4)}$$

$$= \frac{2}{(3k+2)(3k+3)(3k+4)}$$

which is positive as $k \geq 1$

Hence, the result is true for $n = k+1 \implies$ our proposition is true for all n by using mathematical induction

4.2.3 Exercises

1. Prove that $1^2 + 2^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$

2. Prove that $1^2 + 4^2 + 7^2 + \cdots + (3n-2)^2 = \dfrac{n(6n^2 - 3n - 1)}{2}$

3. Use mathematical induction to prove that $\forall n \in \mathbb{N}$, $\dfrac{n^5}{5} + \dfrac{n^3}{3} + \dfrac{7n}{15}$ is a positive integer

4. Prove by induction that the last digit of $P(n) = 2^{2^n} + 1 \,\text{is}\, 7 \,\forall\, (n > 1)$

5. Prove by the principle of induction that $(1+x)^n > 1 + nx, n > 1, n \in \mathbb{N}$ and $x > -1$, $x \neq 0$

6. Show that $1 + 2x + 3x^2 + \cdots + nx^{n-1} = \dfrac{1 - (n+1)x^n + nx^(n+1)}{(1-x)^2}$ for all $n \in mathbbN$

7. Let a and b be positive integer with $(a, b) = 1$ and a, b having different parities. Let the set S have the following properties:

   - $a, b \in S$
   - If $x, y, z \in S$ then, $x, y, z \in S$

   Prove that all integers greater than $2ab$ are in S.

   [China MO, 2008]

8. There are n students standing in a circle, one behind the other. The students have heights $h_1 < h_2 < \cdots < h_n$. If a student with height h_k is standing directly behind a student with height h_{k-2} or less, the two students are permitted to switch places.

   Prove that it is not possible to make more than $\dbinom{n}{3}$ such switches before reaching a position in which no further switches are possible.

   [USA MO, 2010]

4.3 RECURRENCE RELATION

4.3.1 Introduction

A recurrence relation is an equation that recursively defines a sequence whose next term is a function of the previous terms. In general, $a_n = f(a_{n-1}, a_{n-2}, \cdots, a_{n-m})$; $n \geq m+1$ is called recurrence relation for sequence $\{a_n\} \geq 1$

For example, consider the sequence: $1, 1, 2, 3, 5, 8, \cdots$

This sequence is known as Fibonacci sequence. Each of its term is governed by the relation $a_{n+2} = a_{n+1} + a_n \, \forall n \in \mathbb{N}$.

4.3.2 Linear homogeneous recurrence

A linear homogeneous recurrence relation of degree k with constant coefficients is a recurrence of the form:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} \tag{4.9}$$

where $c_1, c_2, \cdots, c_k$ are real numbers, and $c_k \neq 0$.

It follows from the previous proposition that if we find some solutions to a linear homogeneous recurrence, then any linear combination of them will also be a solution to the linear homogeneous recurrence. Geometric sequences come up a lot when solving linear homogeneous recurrence. So, try to find any solution of the form $a_n = r^n$ that satisfies the recurrence relation.

Therefore, given a recurrence Eq.4.9, we try to find a solution of the form:

$$\begin{aligned}
r^n &= c_1 r^{n-1} + c_2 r^{n-2} + \cdots + c_k r^{n-k} \\
0 &= r^n - c_1 r^{n-1} - c_2 r^{n-2} - \cdots - c_k r^{n-k} \\
0 &= r^k - c_1 r^{k-1} - c_2 r^{k-2} - \cdots - c_k r^k \,(\text{by dividing both sides by } r^{n-k})
\end{aligned}$$

This equation is called the **characteristic equation**.

If, after factoring, the equation had $m+1$ factors of $(r - r_1)$, for example, r_1 is called a **solution of the characteristic equation with multiplicity** $m+1$. When this happen, not only r_1^n is a solution, but also nr_1^n, $n^2 r_1^n, \cdots, n^m r_1^n$ are solutions of the recurrence.

Examples

1. What is the solution of the recurrence relation $a_n = a_{n-1} + a_{n-2}$, with $a_0 = 0$ and $a_1 = 1$

   Since it's a linear homogeneous recurrence, we first find its characteristic equation.

$$\begin{aligned}
a_n &= a_{n-1} + a_{n-2} \\
\implies r^n &= r^{n-1} + r^{n-2} \\
r^2 &= r + 1 \\
0 &= r^2 - r - 1
\end{aligned}$$

$$r_1 = \frac{1+\sqrt{5}}{2} \text{ and } r_2 = \frac{1-\sqrt{5}}{2}$$

$$\text{Hence } a_n = c_1\left(\frac{1+\sqrt{5}}{2}\right)^n + c_2\left(\frac{1-\sqrt{5}}{2}\right)^n \text{ satisfies the recurrence}$$

Now, we should find c_1 and c_2 by using initial conditions.

For $n = 0$, $a_0 = 0 = c_1 + c_2$

For $n = 1$, $a_1 = 1 = c_1\left(\frac{1+\sqrt{5}}{2}\right) + c_2\left(\frac{1-\sqrt{5}}{2}\right)$

$\implies c_1 = \frac{\sqrt{5}}{5}$ and $c_2 = -\frac{\sqrt{5}}{5}$

Therefore, $a_n = \frac{\sqrt{5}}{5}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{\sqrt{5}}{5}\left(\frac{1-\sqrt{5}}{2}\right)$ is a solution

Note: The generated equation should be proved for all n by using either induction principle or other mathematical methods.

2. What is the solution of the recurrence relation $a_n = -a_{n-1} + 4a_{n-2} + 4a_{n-3}$ with $a_0 = 8$, $a_1 = 6$, and $a_2 = 26$

   The characteristic equation of our recurrence is:

   $r^3 + r^2 - 4r - 4 = 0$

   $(r-2)(r+2)(r+1) = 0$

   Therefore $r_1 = 2$, $r_2 = -2$, $r_3 = -1$

   Hence $a_n = c_1(2)^n + c_2(-2)^n + c_3(-1)^n$

   By using the initial conditions:

   $a_0 = 8 = c_1 + c_2 + c_3$

   $a_1 = 6 = 2c_1 - 2c_2 - c_3$

   $a_2 = 26 = 4c_1 + 4c_2 + c_3$

   From the above, $c_1 = 5$, $c_2 = 1, c_3 = 2$

   $\implies a_n = 5(2)^n + (-2)^n + 2(-1)^n$

4.3.3 Linear non-homogeneous recurrence

A linear non-homogeneous recurrence relation with constant coefficients is a recurrence relation of the form

$$a_n = c_1a_{n-1} + c_2a_{n-2} + \cdots + c_ka_{n-k} + d(n) \tag{4.10}$$

where $c_1, c_2, \cdots, c_k$ are real numbers, and $d(n)$ is a function depending only on n.

For solving linear non-homogeneous recurrence, we try to find another recurrence, i.e. $b_n = c_1b_{n-1} + c_2b_{n-2} + \cdots + c_kb_{n-k} + d(n)$ such that there exist an associated homogeneous recurrence

$$f_n = a_n - b_n = c_1(a_{n-1} - b_{n-1}) + c_2(a_{n-2} - b_{n-2}) + \cdots + c_k(a_{n-k} - b_{n-k})$$

For many common recurrences, b_n is similar to a_n. Then, we should find solution $f_n = a_n - b_n$ that satisfies both recurrences and initial conditions.

Examples

1. What is the solution of the recurrence relation $a_n = a_{n-1} + a_{n-2} + 3n + 1$ for $n \geq 2$ with $a_0 = 2$ and $a_1 = 3$?

   Given that

$$a_n = a_{n-1} + a_{n-2} + 3n + 1 \tag{4.11}$$

$$\text{Trying } n = n + 1 \implies a_{n+1} = a_n + a_{n-1} + 3n + 4 \tag{4.12}$$

   By finding the difference between Eqs.4.11 and 4.12, we get

$$a_{n+1} - 2a_n + a_{n-2} = 3 \tag{4.13}$$

$$\text{Again trying } n = n + 1 \implies a_{n+2} - 2a_{n+1} + a_{n-1} = 3 \tag{4.14}$$

   The difference between Eqs.4.13 and 4.14 becomes

$$a_{n+2} - 3a_{n+1} + 2a_n + a_{n-1} - a_{n-2} = 0$$

   which is an associated linear homogeneous recurrence that can be solved like other homogeneous recurrence.

2. What is the solution of the recurrence relation $a_n = 2a_{n-1} - a_{n-2} + 2^n$ for $n \geq 2$, with $a_0 = 1$ and $a_1 = 2$?

   Given that

$$a_n = 2a_{n-1} - a_{n-2} + 2^n \tag{4.15}$$

   Doubling both sides gives us

$$2a_n = 4a_{n-1} - 2a_{n-2} + 2^{n+1} \tag{4.16}$$

   Assuming $n = n + 1$ in Eq.4.15, we get

$$a_{n+1} = 2a_n - a_{n-1} + 2^{n+1} \tag{4.17}$$

   By comparing Eqs.4.16 and 4.17, we get

$$a_{n+1} - 4a_n + 5a_{n-1} - 2a_{n-2} = 0 \tag{4.18}$$

   Its characteristic equation becomes

$$\begin{aligned} r^3 - 4r^2 + 5r - 2 &= 0 \\ (r-1)^2(r-2) &= 0 \end{aligned}$$

   Hence $r_1 = r_2 = 1$ and $r_3 = 2$

   Therefore, since $r_1 = r_2$, $a_n = c_1(1)^n + c_2 n(1)^n + c_3(2)^n$

   By using initial conditions

$$\begin{aligned} a_0 &= 1 = c_1 + c_3 \\ a_1 &= 2 = c_1 + c_2 + 2c_3 \\ a_2 &= 7 = c_1 + 2c_2 + 4c_3 \end{aligned}$$

   which give us $c_1 = c_2 = -3$ and $c_3 = 4$

   Hence, $a_n = 2^{n+2} - 3n - 3$

4.3.4 Exercises

1. Let $\{a_n\}$ be a sequence such that, $a_0 = 2, a_1 = 25, a_n = 10a_{n-1} - 25a_{n-2}$ $\forall n \geq 2$, $n \in \mathbb{N}$. Find a_n.

2. Solve the following recurrence relation: $a_n = 3a_{n-1} + 2 - 2n^2$, $n \geq 1$, $a_0 = 3$

3. Solve the recurrence relation $a_n = 6a_{n-1} - 9a_{n-2} + 2^n$, $n \geq 2$, $a_0 = 1$, $a_1 = 4$

4. Let $a_n = 5a_{n-1} + 29b_{n-1}$, $n \geq 2$, $b_n = a_{n-1} + 5b_{n-1}$, $n \geq 2$, $a_1 = 5$, and $b_1 = 1$. Find a_n and b_n.

5. The sequence $\{a_n\}$ is given by $a_0 = 3$, $a_n = 2 + a_0 a_1 \cdots a_{n-1}$ $\forall n \geq 1$.

   (a) Prove that any two term of $\{a_n\}$ are relatively prime.

   (b) Find a_{2007}

   [Croatia MO, 2007]

6. The sequence $\{x_n\}$ is defined by $z_1 = a$, $x_2 = b$, $x_{n+2} = 2008x_{n+1} - x_n$. Prove that there exist a, b such that $1 + 2006x_{n+1}x_n$ is a perfect square for all $n \in \mathbb{N}$

   [Turkey MO, 2008]

4.4 BIJECTION

4.4.1 Definition

Using Bijection to solve combinatorics' problems is one of the trickiest way to escape some difficult counting problems. It basically deals with finding two sets which are equal and count using the easiest set to get hang of the hardest one.
let

$$A = \{a_1, a_2, \ldots, a_n\} \text{ and } B = \{b_1, b_2, \ldots, b_m\}$$

If f : A $\rightarrow$ B is an injective function then $n \leq m$.
If f : A $\rightarrow$ B is a surjective function then $n \geq m$.
If f : A $\rightarrow$ B is injective and surjective, then f is known to be a bijective function. For a bijective function, n = m. [3]

I know this last paragraph may seem to be alien to you, but it is just an elengant way to communicate what is in its antecedant paragraph. An injective function is one which map an element from domain to a different one in the range; that is to say when executing that function, no input can be equal to it's output. A surjective function is the one which map elements from the domain to the entire set of range. Notice that when all of the above conditions are met, the set of domain must quantitatively be equal to the set of range and counting the elements of the domain becomes similar to counting the elements of the range. The functions that behave in this way, we typically call them bijective functions.

4.4.2 Examples

1. **What is the total number of subsets of a set containing exactly n elements?**

   solution:
   Let

   $$S = \{a_1, a_2, a_3, \ldots, a_n\}$$

   be a set of exactly n elements. Let P be the set of all subsets of S and Q be the set of all binary sequences of n elements.

   Let A $\in$ P. Let f : P $\rightarrow$ Q be a function that associates a binary sequence with A as follows:

$a_i \in$ **A, if $\mathbf{i^{th}}$ term of the sequence Q is 1.**

For example, subset

$$\{a_2, a_4, \ldots, an - 1\}$$

corresponds to binary sequence $0, 1, 0, 1, 0, 0, \ldots, 0, 1, 0$

Observe that, for every subset A, there is a binary sequence of n terms and for every binary sequence of n terms as stated above, there is a subset A of S.
Therefore f is a bijection between P and Q. Hence, the number of subsets = number of binary sequences $= 2^{\mathrm{n}}$
.

2. For every positive integer n, prove that
$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \ldots + (-1)^{\mathrm{n}}\binom{n}{n} = 0$

   Solution: The identity is equivalent to the fact that, for every positive integer n,
$\sum_{\text{k odd}} \binom{n}{k} = \sum_{\text{k even}} \binom{n}{k}$
If S is a set with n elements, the left-hand side counts the number of subsets of S with an odd number of elements while the right-hand side counts the number of subsets of S with an even number of elements. Now that we have a combinatorial interpretation for both sides of the equation, it makes sense to look for a one-to-one correspondence—a bijection to use more precise terminology—between the objects described by the left-hand side and the objects described by the right-hand side.

   In other words, we want to find a rule for turning a subset of S with an odd number of elements into a subset of S with an even number of elements, and vice versa.
We start by picking some fixed s ∈ S. The rule is to add the element s to your set if it doesn't already contain it, and to remove the element s from your set if it does already contain it. Since we are either adding or subtracting a single element, this rule certainly turns a subset of S with an odd number of elements into a subset of S with an even number of elements, and vice versa. It is a bijection because the rule can be reversed. In fact, the rule is its own inverse! This completes our combinatorial proof.

3. For every positive integer n, prove that
$\binom{n}{1} - 2\binom{n}{2} + 3\binom{n}{3} - \ldots + n\binom{n}{n} = n2^{\mathrm{n-1}}$

   Solution: The idea is to find a set of objects which can be counted in two ways—one of which produces the left-hand side while the other produces the right-hand side. In this particular case, the form of the left-hand side gives a strong hint as to what that set might be.

   Each term of the left-hand side is of the form $k\binom{n}{k}$ which suggests that, from a set of n people, we would like to choose a committee of k people. This can be done in $\binom{n}{k}$ ways. Furthermore, we would like to choose a president from this committee. This can be done in k ways. As k ranges from 1 up to n, we are choosing committees of every possible size. So what we have shown is that the left-hand side counts the number of ways to choose a committee, with one person designated the president, from a set of n people.

   Of course, all that remains is to show that the number of ways to choose a committee, with one person designated the president, from a set of n people also happens to be $\mathrm{n}2^{\mathrm{n-1}}$. Whereas we earlier counted by choosing the committee first and then the president, we will now count by choosing the president first and then the remainder of the committee. But this is easy, because there are n choices for the president and for each of the remaining n - 1 people, there are two choices. Each person is either in the committee or is not. Thus the number of ways of choosing a committee with president is $\mathrm{n}2^{\mathrm{n-1}}$. This completes our combinatorial proof.

4.4.3 Exercises

1. In the congress, three disjoint committees of 100 congressmen each are formed. Every pair of congressmen may know each other or not. Show that there are two congressmen from different committees such that in the third committee there are 17 congressmen that know both of them or there are 17 congressmen that know neither of them

2. (APMO 2006) In a circus there are n clowns. Every clown may dress or paint himself using at least 5 out of 12 possible colors. We know that there are no two clowns with exactly the same colors and that no color is used by more than 20 clowns. Find the largest possible value of n.

3. (Iran 2011) A school has n students and there are some extra classes they can participate in. A student may enter any number of extra classes. We know there are at least two students in each class. We also know that if two different classes have at least two students in common, then their numbers of students are different. Show that the total number of classes is not greater than $(n\text{-}1)^2$.

4.5 PIGEONHOLE PRINCIPLE

4.5.1 Definition

Let k, n $\in$ N. If at least $k^n + 1$ objects are distributed among k boxes, then at least one of the box, must contain at least n + 1 objects. In particular, if at least n + 1 objects are put into n boxes, then at least one of the box must contain at least two objects. For arbitrary n objects and m boxes this generalizes to at least one box will contain at least $\lfloor \frac{n-1}{m+1} \rfloor$ objects. [3]

4.5.2 Examples

1. Divide the numbers 1, 2, 3, 4, 5 into two arbitrarily chosen sets. Prove that one of the sets contains two numbers and their difference.

   Solution: Let us try to divide 1, 2, 3, 4, 5 into two sets in such a way that neither set contains the difference of two of its numbers. 2 cannot be in the same set as 1, 4, because if 2 and 1 are in the same sets, 2 - 1 = 1 belongs to the set; again if 2 and 4 are in the same set then 4 - 2 = 2 belongs to the set and hence, if we name the sets as A and B, and if 2 $\in$ A, then 1, 4 both belong to B. We cannot put 3 in set B as 4 - 3 = l belongs to B, so 3 belongs to A.

   Now, 5 is the only number left out. Either 5 should be in set A or in B, but then
   if $5 \in A \implies 5 - 3 = 2 \in A$. So, 5 cannot be in A. However, if 5 is put in set B, then $5 - 4 = 1 \in B$. So, 5 cannot be in set B.
   Thus, we cannot put 5 in either set and hence completing the proof.

2. Show that for any set of 10 points chosen within a square whose sides are of length 3 units, there are two points in the set whose distance is at most 2.

   Solution: Divide the square into 9 unit squares. Out of the 10 points distributed in the big square, at least one of the small squares must have at least two points by the Pigeon hole principle. These two points being in a unit square, are at the most $\sqrt{2}$ units distance apart as $\sqrt{2}$ is the length of the diagonal of the unit square.

3. If repetition of digits is not allowed in any number (in base 10), show that among three four-digit numbers, two have a common digit occurring in them. Also show that in base 7 system any two four-digit number

   Solution: In base 10, we have ten digits 0, 1, 2, 3, 4, 5, 6, 7, 8 and 9. Thus, for 3 four-digit numbers without repetition of digits, we have to use in all 12 digits, but in base 10 we have just 10 digits.

Thus, at least any two of the three four-digit numbers have a common number occurring in their digits by Pigeon hole principle. Again for base 7 system, we have seven digits 0, 1, 2, 3, 4, 5, 6. For two four-digit numbers without repetition we have to use eight digits and again by Pigeon hole Principle, they have at least one common number in their digits.

4.5.3 Exercises

1. There are 90 cards numbered 10 to 99. A card is drawn and the sum of the digits of the number in the card is noted; show that if 35 cards are drawn, then, there are some three cards, whose sum of the digits are identical.
2. If in a class of 15 students, the total of the marks in a subject is 600, then show that, there is a group of 3 students, the total of whose marks is at least 120.
3. 5 points are plotted inside a circle. Prove that, there exist two points, which form an acute angle with the centre of the circle.
4. Prove that, there exist two powers 3, which differ by a multiple of 2005
5. All the points in the plane are coloured, using three colours. Prove that, there exists a triangle with vertices, having the same colour, such that, either it is isosceles or its angles are in geometric progression
6. (OMM 2003) There are n boys and n girls in a party. Each boy likes a girls and each girl likes b boys. Find all pairs (a,b) such that there must always be a boy and a girl that like each other.
7. Show that given a subset of n + 1 elements of $1, 2, 3, ..., 2n$, there are two elements in that subset such that one is divisible by the other.
8. (IMO 1964) 17 people communicate by mail with each other. In all their letters they only discuss one of three possible topics. Each pair of persons discusses only one topic. Show that there are at least three persons that discussed only one topic.
9. Show that if an infinite number of points in the plane are joined with blue or green segments, there is always an infinite number of those points such that all the segments joining them are of only one color.

4.6 DOUBLE COUNTING

4.6.1 Definition

Double counting is short for counting similar things in two different ways [1].

4.6.2 Examples

1. At a party each person knew exactly 22 others. For any pair of people X and Y who knew one another, there was no other person at the party whom they both knew. For any pair of people X and Y , who did not know one another, there were exactly 6 other people whom they both knew. How many people were at the party?

   Solution: This problem has an obvious graph theory interpretation, where vertices represent people and edges represent a mutual acquaintanceship between two persons. Define a vee to be a triple of persons such that exactly two of the three pairs of acquaintances know each other. We count the number of vees in two different ways.

   Suppose there are n people at the party. Concentrating on vertices we see that each vertex contributes $\binom{22}{2} = 231$ vees since each vertex has 22 edges emanating from it. Thus the total number of vees is $231n$.

On the other hand adding the degrees of each vertex gives 22n, but this overcounts the number of edges by a factor of two. Therefore, the total number of edges is 11n. This means that the total number of pairs of vertices not connected by an edge is
$\binom{n}{2} - 11n$
Each such non-edge makes a vee with 6 other vertices. Thus the total number of vees is
$6(\binom{n}{2} - 11n)$
Equating the two expressions for the number of vees yields
$231n = 6(\binom{n}{2} - 11n)$
This is easily solved for n and yields $n = 100$.

4.7 GRAPH THEORY

4.7.1 Definition

Graph theory is a truly remarkable area of mathematics. In one sense, the concept of a graph is so easy that every human being has some innate understanding of it. On the other hand, graph theory offers some notoriously difficult problems and is the site of much active mathematical research today. In between the very simple and the very complicated lies a vast region of interesting and amazing results, some of which we'll soon see.
When we use the word graph in this chapter, we don't mean a complicated representation of a function on a set of coordinate axes or anything like that. We simply mean a diagram obtained by joining dots.
In the usual graph theory terminology, the dots are called vertices while the lines connecting them are called edges. The edges of a graph merely represent relationships between the vertices. In particular, we usually don't care how a graph is drawn in the plane.

Graph theory is said to have started in 1736, with Euler. However, the first book on graph theory was published by König in the twentieth century (1936). Even though graph theory had an accelerated growth in that century, it is still possible to find open problems that do not require a lot of theory to understand (and, in some cases, solve). This does not mean in any way that such problems are easy, though. [4]

4.7.2 Terminology

A graph G is a pair (V,E), where V is a non-empty set and E is a multiset of unordered pairs of elements of V . The elements of V are called the vertices and the elements of E are called the edges of G. The reason why E is a multiset is to allow G to have an edge more than once; however, we will not deal with this kind of graphs.
A subgraph g of G = (V,E) is a pair (v ,e), where v is a subset of V, e is a subset of E and (v ,e) is also a graph.

Given a graph G, the **set of vertices** is usually denoted by v(G) and the (multi) **set of edges** is denoted by e(G). Each graph has a geometric representation. One places one point in the plane for each vertex, and a pair of points are joined with a line segment whenever the corresponding vertices form an edge. Sometimes in the geometric representation edges have a common point, this does not mean that there is a new vertex there.

Given a graph G, we say G is **simple** if there are no edges of only one vertex and there are no multiple edges.
From now on, all graphs are simple unless specified otherwise.
The term **multigraph** usually refers to graphs that are not simple. Given a graph G and its vertex v_0, we say that an edge A is incident in v_0 if v_0 is one of its vertices. We also say that two vertices v_0 and v_1 are adjacent if they form an edge. We say that v_0 has degree k if it is adjacent to exactly k vertices, and then we write $d(v_0) = k$.

In a graph, a **walk** is a sequence of vertices $(v_0, v_1, v_2, ..., v_k)$ such that v_i is adjacent to v_{i+1} for all $1 \leq i \leq k-1$. In a walk, vertices may be repeated.
A path is a walk where no vertices are repeated. In the previous graph.
We say that a walk is **closed** if the first and last vertices are the same.
A cycle is a closed walk where the only two vertices that coincide are the first and the last.
Two cycles (walks, closed walks, paths) are said to be **disjoint** if they share no vertices.
The **length of a path** is equal to the number of edges it has or, equivalently, the number of vertices it has minus one.
The **length of a cycle** is equal to the number of edges it has or, equivalently, the number of vertices it has.
We say that a graph G is **connected** if given any two vertices v_0 and v_1 of G there is a walk that starts in v_0 and ends in v_1. In other words, we can get from any vertex in G to any other vertex in G by moving only along edges in the graph.
A tree is a graph without a cycle.
A leaf refers to a vertex in a graph that has only one edge connecting it to the rest of the graph, making it resemble a leaf on a tree. In other words, a leaf is a vertex with a degree equals to one.

4.7.3 Examples

1. **In a graph G, every vertex has degree at least $k \leq 2$. Show that G has a cycle whose length is at least $k+1$.**

   Solution: We construct a sequence of vertices $(v_0, v_1, v_2, \ldots)$ in the following way: v_0 is any vertex and, if we have constructed $v_0, v_1, \ldots, v_{t-1}$, then we choose v_t to be adjacent to v_{t-1} and different from $v_{t-2}, v_{t-3}, \ldots, v_{t-k}$. This can be done since $d(v_{t-1}) \geq k$. Since G is a finite graph, the sequence cannot go on indefinitely without repeating vertices: there must be two vertices v_t and v_{t-l} such that $v_t = v_{t-l}$.

   We can suppose that t is the first moment when this happens. Given the construction of the sequence, we have that $l \geq k+1$. Thus, $(v_{t-l}, v_{t-l+1}, \ldots, v_{t-1}, v_t = v_{t-l})$ is the cycle we were looking for. It is important that t was the first moment when this happened in order for the cycle not to repeat vertices (otherwise it would simply be a closed walk).

4.7.4 Exercises

1. What is the maximum degree of a vertex?

2. Prove that a walk from v_o to v_1 exists if and only if a path exists from $v_o tov_1$.

3. Let deg(v) denote a degree of a vertex v and n denote the total number of edges of a graph.prove that $\sum$ deg(v) $= 2 \times n$

4. Show that at a party of 6 people, there are either 3 people who know each other or 3 people none of which know each other.

5. Prove that, at any party with six people, there must exist three mutual friends or three mutual strangers.

6. (PAMO 2007) In a country, towns are connected by roads. Each town is directly connected with exactly 3 other towns. Show that there exist a town from which you make a round trip without using the dame road more than once, and for which the number of roads used is not divisible by 3. (Not all towns need to be visited)

7. (BMO 1987) At an international meeting, 1985 persons participated. In each subset of three participants, there were at least two people who spoke the same language. Show that if each person speaks at most five languages, then at least 200 people spoke the same language.

4.8 COULORING

4.8.1 Definition

This involves partitioning of a set into a finite number of subsets. The partitioning is done by coloring each element of a subset by the same color.

4.8.2 Examples

1. **Is it possible to form a rectangle with the five different tetraminoes? (Check the meaning of tetramino in RwMO Glossary.)**

   Solution: Any rectangle with 20 squares can be colored like a chessboard with 10 black and 10 white squares. Four of the tetrominoes will cover 2 black and 2 white squares each. The remaining 2 black and 2 white squares cannot be covered by the T-tetromino. A T-tetromino always covers 3 black and one white squares or 3 white and one black squares.

4.8.3 Exercises

1. Prove that An 8×8 chessboard cannot be covered by 15 T-tetrominoes and one square tetromino.

2. Prove that a 10 $\times$ 10 board cannot be covered by 25 straight tetrominoes.

3. Consider an n $\times$ n chessboard with the four corners removed. For which values of n can you cover the board with L-tetrominoes.

4. Is there a way to pack 250 $1 \times 1 \times \times 4$ bricks into a 10 $\times$ 10 $\times$10 box?

5. One corner of a $(2n+1) \times (2n+1)$ chessboard is cut off. For which n can you cover the remaining squares by 2 $\times$ 1 dominoes, so that half of the dominoes are horizontal?

6. Given an $m \times n$ rectangle, what minimum number of cells (1×1) squares must be colored, such that there is no place on the remaining cells for an L-tetromino?

7. The positive integeres are colored black and white. The sum of two differently colored numbers is black, and their product is white. What is the product of two white numbers? Find all such colorings.

4.9 PROBLEMS

1. Three bins are labelled A, B and C, and each bin contains four balls numbered 1, 2, 3, and 4. The balls in each bin are mixed, and then a student chooses one ball at random from each of the bins. If a, b and c are the numbers on the balls chosen from bins A, B and C, respectively, the student wins a toy helicopter when $a = b + c$. There are 64 ways to choose the three balls.
   What is the probability that the student wins the prize?

   (A) $\frac{12}{39}$ (B) 1 (C) $\frac{4}{49}$ (D) $\frac{3}{32}$ (E) $\frac{2}{9}$

2. A deck of 100 cards is numbered from 1 to 100. Each card has the same number printed on both sides. One side of each card is red and the other side is yellow. Barsby places all the cards, red side up, on a table. He first turns over every card that has a number divisible by 2. He then examines all the cards, and turns over every card that has a number divisible by 3. How many cards have the red side up when Barsby is finished?

   (A) 83 (B) 17 (C) 66 (D) 50 (E) 49

3. How many integers can be expressed as a sum of three distinct numbers if chosen from the set4, 7, 10, 13 ,..., 46?

   (A) 45 (B) 37 (C) 36 (D) 43 (E) 42

4. A square array of dots with 10 rows and 10 columns is given. Each dot is coloured either blue or red. Whenever two dots of the same colour are adjacent in the same row or column, they are joined by a line segment of the same colour as the dots. If they are adjacent but of different colours, they are then joined by a green line segment. In total, there are 52 red dots. There are 2 red dots at corners with an additional 16 red dots on the edges of the array. The remainder of the red dots are inside the array. There are 98 green line segments. The number of blue line segments is

   (A) 36 (B) 37 (C) 38 (D) 39 (E) 40

5. The set 1, 4, n has the property that when any two distinct elements are chosen and 2112 is added to their product, the result is a perfect square. If n is a positive integer, the number of possible values for n is

   (A) 8 (B) 7 (C) 6 (D) 5 (E) 4

6. The art Gallery has the shape of a simple n-gon. Find the minimum number of watchmen needed to survey the building, no matter how complicated its shape.

   (A) $\lfloor \frac{n}{1} \rfloor$ (B) $\lfloor \frac{12}{n} \rfloor$ (C) $\lfloor \frac{n}{6} \rfloor$ (D) $\lfloor \frac{n}{3} \rfloor$(E) $\lfloor \frac{43}{n} \rfloor$

7. 17 people communicate by mail with each other. within their letters, they only discuss one of three possible topics. Each pair of persons discusses only one topic. At least how many persons that discussed only one topic?

   (A) 7 (B) 5 (C) 6 (D) 3 (E) 4

8. if we are given 50 segments in a line, then there are n of them which are pairwise disjoint or n of them with a common point; n is equal to:

   (A) 8 (B) 7 (C) 6 (D) 5 (E) 4

Bibliography

[1] Daniel Mathews Angelo Di Pasquale, Norman Do. *PROBLEM SOLVING TACTICS*. AMT Publishing, 2014.

[2] Samin Riasat. *Basics of Olympiad Inequalities*.

[3] Vikash Tiwari & V. Seshan. *Pathfinder for Olympiad Mathematics*. Pearson.

[4] Pablo Soberon. *Problem-Solving Methods in Combinatorics*. Springer, 2013.

Part II

RWANDA MATH OLYMPIAD GLOSSARY

1st edition May 2022

Rwanda Math Olympiad Glossary

May 2022

Preface

Glossary is an alphabetical list of words relating to specific dialect with explanations. Rwanda Math Olympiad (RwMO) Glossary seeks to explain to Rwandan students unfamiliar words and symbols that are found in math olympiad competitions to boost their interest in mathematics and problem solving excellence.

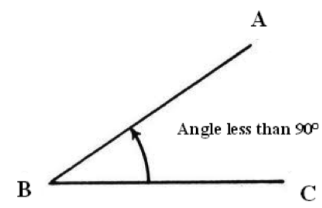
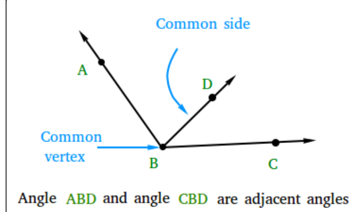
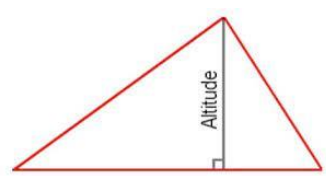
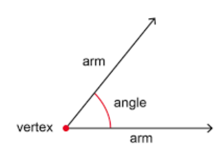
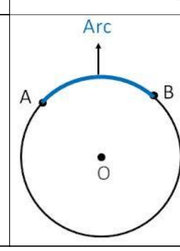
Ijambo ry' ibanze

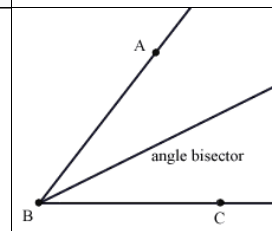
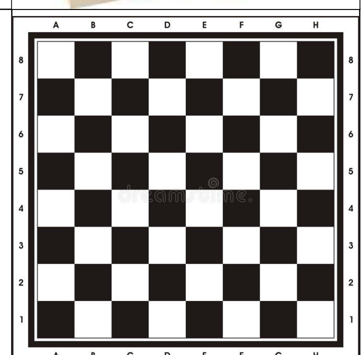
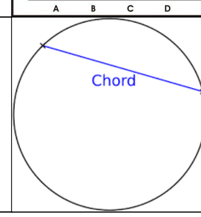
Inkoranyamagambo ni urutonde rw' amagambo ajyanye n' imvugo yihariye hamwe n' ibisobanuro. Iyi nkoranya magambo igamije gusobanurira abanyeshuri bo mu Rwanda amagambo atamenyerewe dusanga mu marushanwa ya olipiyadi (olympiad) y' imibare, hagamijwe kubongerera ubumenyi bujyanye n' imibare no gukora neza ibibazo babajijwe.

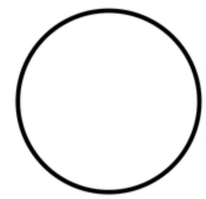
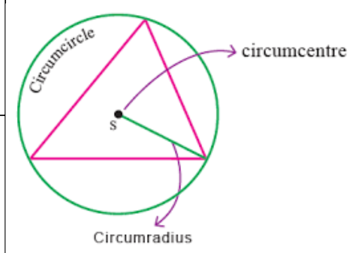
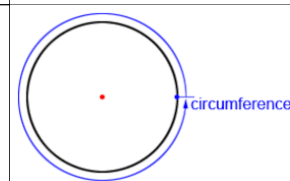
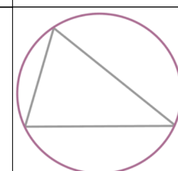
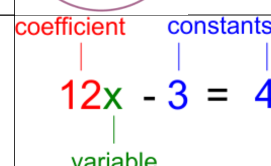
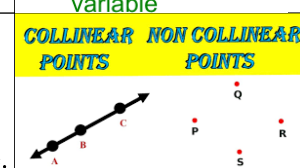
Notice: blue-colored words in english definitions section are explained in this glossary.

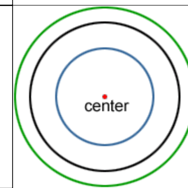
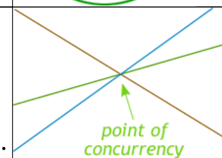
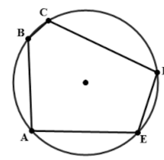
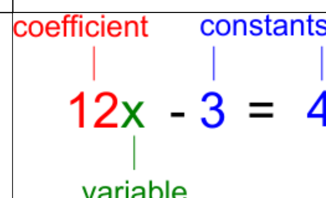
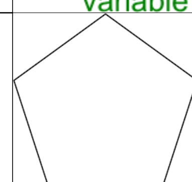
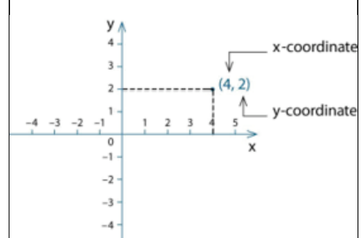
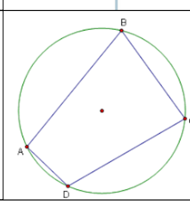
contacts: rwandamathsolympiad@gmail.com

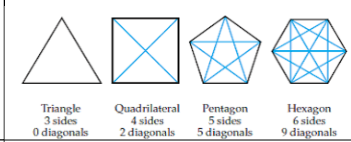
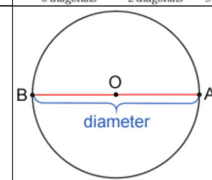
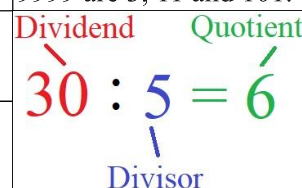
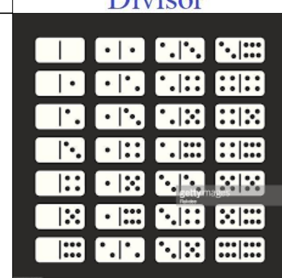
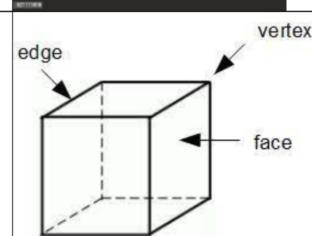
Prepared by Arnold Hategekimana Hirwa

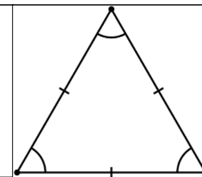
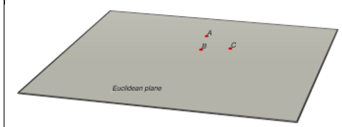
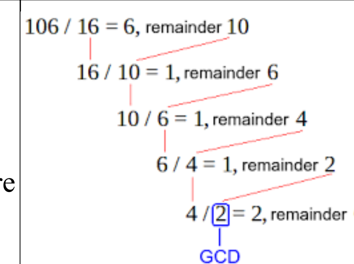
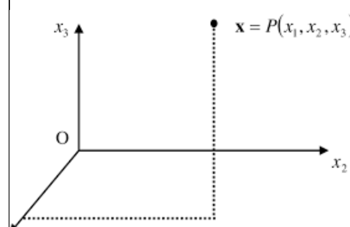
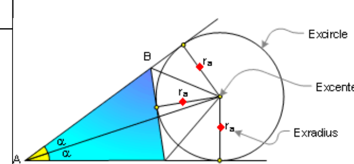
MATHEMATICAL TERMS	**ENGLISH DEFINITIONS**	**KINYARWANDA DEFINITIONS/ TERMS**	**IMAGE/EXAMPLE**
absolute value	the magnitude of a real number without regard to its sign. The absolute value of a number may also be thought as its distance from zero along real number line.	ubunini bwumubare nyawo utitaye ku kimenyetso cyawo.	$\lvert -3 \rvert = 3$
acute-angle	less than 90°	imfuruka iri hagati ya dogere 0 na dogere 90	
adjacent angles	two angles that have a common side and a common vertex.	Inguni ebyiri zihujwe n' uruhande rumwe.	
Altitude	perpendicular line from a vertex to the opposite side of a figure.	uburebure bwumurongo wa perpendicular kuva kuri vertex kugera kuruhande rwigishushanyo.	
angle	the space (usually measured in degrees) between two intersecting lines or surfaces at or close to the point where they meet.	imfuruka	
arc	a part of a curve, especially a part of the circumference of a circle.	igice cy' umurongo, cyane cyane igice cyumuzingi.	

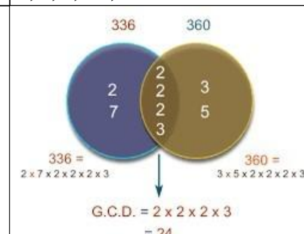
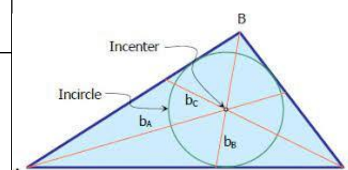
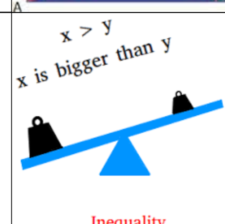
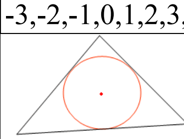
arithmetic progression	a sequence of numbers in which each differs from the preceding one by a constant quantity.	urukurikirane rw'imibare aho buri umwe utandukanywa n' undi hifashishijwe umubare udahinduka.	-6,-4,-2,0,2,4,6,...
arithmetic(mean)	the average of a set of numerical values, as calculated by adding them together and dividing by the number of terms in the set.	impuzandengo y' uruhererekane rw' imibare, ubarwa nyuma yo guteranya imibare yose hanyuma ukagabanya igiteranyo cyayo n' ingano y' iyo mibare.	$\text{arithmetic mean} = \frac{\sum_{n=1}^{k} x_n}{k}$
bisector	The line that divides something into two equal parts.	Umurongo ugabanya ikintu mo ibice bibiri bingana.	
chess	a board game of strategic skill for two players, played on a chessboard on which each playing piece is moved according to precise rules. The object is to put the opponent's king under a direct attack from which escape is impossible (checkmate).	umukino wibibaho byubuhanga bukomeye ku bakinnyi babiri, ukinirwa ku kibaho cyagenzuwe kuri buri gice cyo gukinisha. Intego ni ugushyira umwami wuwo bahanganye mu bitero bitaziguye aho guhunga bidashoboka (cheque).	
chessboard	a square board divided into sixty-four alternating dark and light squares (conventionally called 'black' and 'white'), used for playing chess or draughts (checkers).	ikibaho cya kare kigabanyijemo ibice mirongo itandatu na bine bisimburana byijimye kandi byerurutse (bisanzwe byitwa 'umukara n' umweru'), bikoreshwa mu gukina chess.	
chord	a straight line joining the ends of an arc.	umurongo ugororotse ukora ku mpande zombi z' uruziga.	

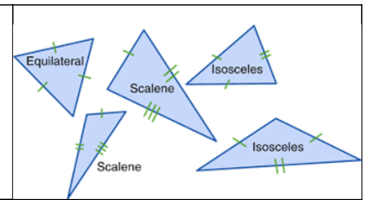
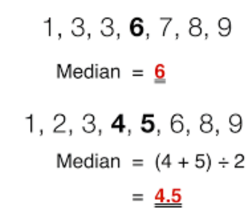
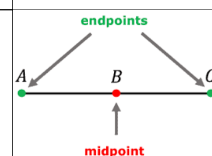
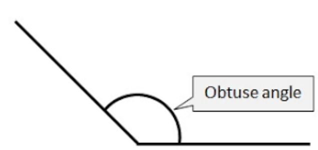
circle	a round plane figure whose boundary (the circumference) consists of points equidistant from a fixed point (the centre).	uruziga	
circumcentre	centre of circumcircle		
circumcircle	a circle touching all the vertices of a triangle or polygon.	uruziga rukora kuri buri nguni y' igishushanyo rurimo.	
circumference	the distance around a circle.	intera ikikije uruziga.	
circumscribe	round another, touching it at points but not cutting it.	kuzenguruka ikindi kintu ugikoraho ariko utakirenga.	
coefficient	a numerical or constant quantity placed before and multiplying the variable in an algebraic expression.	umubare ukuba ikintu gihinduka.	
collinear	lying in the same straight line.	ibintu biri ku murongo umwe.	
complement (set)	the members of a set or class that are not members of a given subset.	ibigize itsinda rinini bitari mu rindi tsinda rito runaka.	Set U = {2,4,6,8,10,12} and set A = {4,6,8}, then the complement of set A, A′ = {2,10,12}
complement (geometry)	the amount in degrees by which a given angle is less than 90°.	ingano muri dogere ibura kugira ngo imfuruka yatanzwe igere kuri 90°.	complement of 50° is 40°
composite number	a number that is a multiple of at least two numbers other than itself and 1.	umubare utarimo ibice ushobora kugabanywa n' imibare ibiri itandukanye.	4,8,9,12,25,...

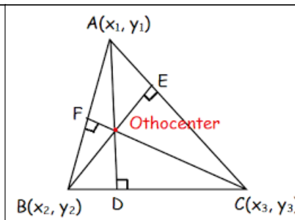
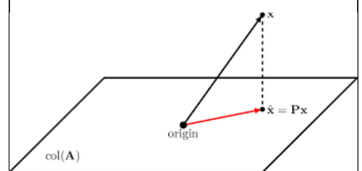
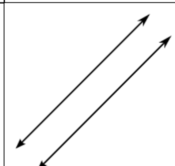
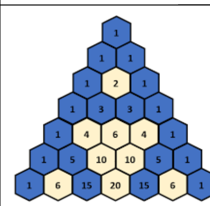
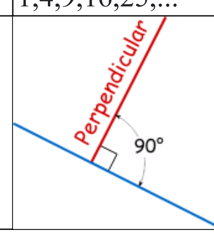
concave polygon	internal angle can be more than 180°.	inguni y' imbere ishobora kuruta dogere 180°.	
concentric circles	circles with a common centre.	inziga zihuje akadomo k' impuzandengo.	
concurrent (of three or more lines)	meeting at or tending towards one point.	guhura kw' imirongo myinshi.	
concyclic points	points that lay on the circumference of a circle.	utudomo turi ku muzingi.	
configuration	an arrangement of parts or elements in a particular form, figure, or combination.	gutondekanya ibintu mu buryo runaka.	
constant	a quantity or parameter that does not change its value whatever the value of the variables, under a given set of conditions.	umubare cyangwa ikintu kidahinduka.	
convex polygon	all interior angles are less than or equal to 180 degrees	inguni z' imbere zose ziri munsi ya dogere 180°	
co-ordinate	each of a group of numbers used to indicate the position of a point, line, or plane.	itsinda ry' imibare rigaragaragaza akadomo, umurongo, cyangwa ikindi kintu.	
cyclic polygon	a polygon having all its vertices lying on a circle.	aho imfuruka z' igishushanyo ziremerwa haba hakora ku ruziga.	

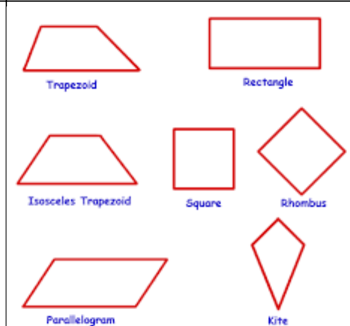
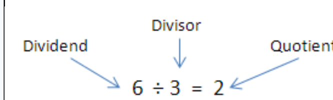
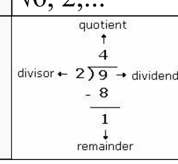
denominator	the number below the line in a vulgar fraction; a divisor.	icyitarusange	2 is denominator in this fraction: 1/2
diagonal	a straight line joining two opposite corners of a square, rectangle, or other straight-sided shape.	umurongo uhuza inguni ebyiri z' ikinyampande runaka.	
diameter	a straight line passing from side to side through the centre of a body or figure, especially a circle or sphere.	umurongo ugabanyamo uruziga cyangwa ikindi gishushanyo mo ibice bibiri bingana.	
digit	any of the numerals from 0 to 9, especially when forming a part of number.	umwe mu mibare uhereye kuri 0 ukageza ku 9.	0,1,2,3,4,5,6,7,8,9
distinct prime numbers	prime numbers without any repeats.		distinct prime factors of 9999 are 3, 11 and 101.
dividend	a number that is being divided.	umubare wagabanyishijwe undi.	
divisor	a number that divides another without returning a remainder.	umubare ugabanya undi ntihagire igisaguka.	
domino	any of 28 small oblong pieces marked with 0–6 pips in each half.	kamwe mu mu duce 28 twerekanwe haruguru.	
edge (geometry)	line segment joining two vertices.	igice cy' umurongo gihuza utudomo tubiri.	
equation	a statement that shows that the values of two mathematical expressions are equal.	inyandiko yerekana ko ibintu bibiri bingana.	2x-2=0

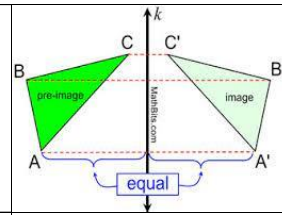
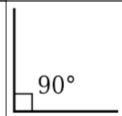
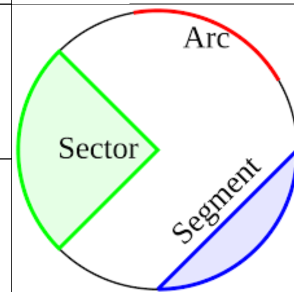
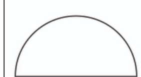
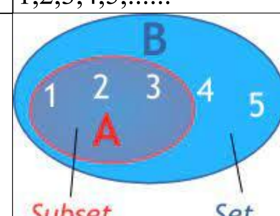
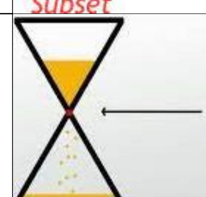
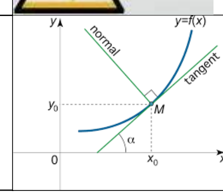
equilateral	having all its sides of the same length.	impande zose ziba zingana.	
euclidean plane	two dimensional part of the euclidean space.		
euclidean algorithm	an efficient method for computing the greatest common divisor (GCD) of two integers (numbers).	uburyo bwo gushaka umubare ugabanya imibare ibiri runaka.	
euclidean space	a space in any finite number of dimensions, in which points are designated by coordinates (one for each dimension) and the distance between two points is given by a distance formula.		
even number	a number that returns zero as a remainder when divided by two.	umubare w'imbangikane.	2:2=1; 4:2=2; 12:2=6,... bivuzeko 2,4,... hakubiyemo na 0 ni imibare y'imbangikane.
excentre	centre of excircle		
excircle	a circle tangent to the extensions of two sides of a triangle and the third side.	uruziga rukora ku kwaguka kw' impande ebyiri za mpandeshatu no ku ruhande rwa gatatu.	
factor	a number or algebraic expression that divides another number or expression evenly—i.e. with no remainder.	umubare ugabanya undi ntihagire igisaguka.	3 and 6 are factors of 12.

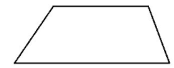
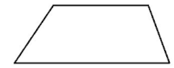
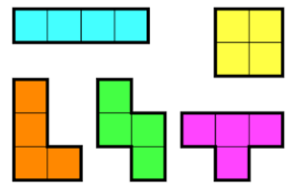
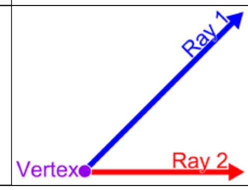
finite set	a set that has a finite number of elements.	itsinda rifite ingano.	For example, {1,3,5,7} is a finite set with four elements.
function	a relation or expression involving one or more variables.	isano iba irimo ikintu kimwe cyangwa byinshi bihinduka.	y = x + 3
geometric mean	the central number in a geometric progression.		for a given set of two numbers such as 8 and 1, the geometric mean is equal to $\sqrt{(8\times1)} = \sqrt{8} = 2\sqrt{2}$
geometric progression	a sequence of non-zero numbers where each term after the first is found by multiplying the previous one by a fixed, non-zero number called the common ratio.	urukurikirane rw' imibare itari zeru, aho umubare uba wikubyi inshuro zidahinduka runaka uwurinyuma.	2,4,8,16,...
greatest common divisor	the largest integer or the polynomial of highest degree that is an exact divisor of each of two or more integers or polynomials.	umubare cyangwa ikintu kinini gishobora kugabanya ibintu bibiri.	
incentre	the intersection of the three interior angle bisectors of a triangle.		
incircle	an inscribed circle of a polygon that is tangent to each of the polygon's side.		
inequality	difference in size, degree, circumstances, etc.	itandukaniro riri hagati y' ibintu runaka.	
infinite sequence	an infinite ordered set of numerical quantities.	urutonde rutarangira.	-3,-2,-1,0,1,2,3,4,5,...
inscribe	draw (a figure) within another so that their boundaries touch but do not intersect.	gushushanya mw' imbere y' ikindi gishushanyo, ugikoraho ariko utakirenga.	
integer	a number which is not a fraction; a whole number.	umubare utarimo ibice.	...,-2,-1,0,1,2,...

isosceles	having two sides of equal length.	hari impande ebyiri zingana muri iyo mpandeshatu.	
linear factors	The linear factors of a polynomial are the first-degree equations that are the building blocks of more complex and higher-order polynomials.		
median	denoting or relating to a value or quantity lying at the midpoint of a frequency distribution of observed values or quantities, such that there is an equal probability of falling above or below it.	icyakabiri cy' umubare cyangwa ikintu runaka.	
mid-point	a point in the middle of something.	ni muri kimwe cya kabiri.	
multiple	a product that we get when one number is multiplied by another number; a number that may be divided by another a certain number of times without a remainder.	igisubizo tubona iyo umubare umwe wikubye undi.	if we say $4 \times 5 = 20$, here 20 is a multiple of 4 and 5
natural numbers	the positive [integers]().	imibare yose itarimo ibice uhereye kuri rimwe ukazamuka.	1,2,3,4,5,...
numerator	the number above the line in a vulgar fraction.		3 is numerator in this fraction: 3/4
obtuse angle	[angle]() greater than 90°	inguni iruta dogere 90°	
odd	having one left over as a remainder when divided by two.	Umubare w'igiharwe.	5 ugabanyije 2 = 2.5 bivuze ko 5 ari umubare w' igiharwe.

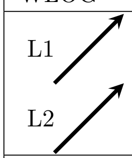
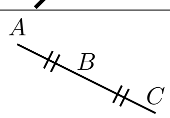
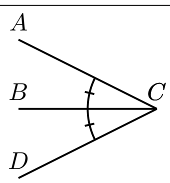
orthocenter of a triangle	the common intersection of the three altitudes of a triangle.		
orthogonal projection	A projection of a figure onto a line or plane so that each element of the figure is mapped onto the closest point on the line or plane.		
pairwise	refers to all subsets of a given set that contain exactly two elements.	bivuze gukora amatsinda mato yose agizwe n' imibare cyangwa ibintu bibiri by' itsinda rinini runaka.	the set {1,2,3} all possible pairs are (1,2),(2,3),(1,3).
pairwise disjoint	If the intersection of two events is the empty set, then the events are called pairwise disjoint events.	n' igihe amatsinda abiri aba adafite aho ahuriye.	{1, 2, 3} and {4,5,6} are pairwise disjoint sets.
parallel	(of lines, planes, or surfaces) side by side and having the same distance continuously between them.	imirongo cyangwa ibintu bibiri runaka biba bifite intera imwe hagati yabyo kuburyo bidashobora guhura.	
pascal traingle	Pascal's triangle, in algebra, is a triangular arrangement of numbers that gives the coefficients in the expansion of any binomial expression.		
perfect square	a number that can be expressed as the square of an integer.	umubare ushobora kwandikwa nk' umubare umwe wikubye inshuro zingana nka wo.	1,4,9,16,25,...
perpendicular	at an angle of 90° to a given line, plane, or surface or to the ground.	gukora imfuruka ya dogere 90° hagati y' ibintu 2 runaka.	

polynomial	an expression of more than two algebraic terms, especially the sum of several terms that contain different powers of the same variable(s).		2xy-3x
prime number	a number that has exactly 2 factors, i.e: divisible only by itself and unity. N.B: 1 is not a prime number and negative integers can not be prime.	umubare ugabanywa na rimwe cyangwa wo ubwawo utabariyemo rimwe n' imibare iri munsi ya zeru.	7,11,13,17,...
quadrilateral	a four-sided figure	ikinyampande enye	
quotient	the number resulting from the division of one number by another.	umubare uturuka ku kugabanya umubare umwe ukoresheje undi.	
ratio	the quantitative relation between two amounts showing the number of times one value contains or is contained within the other.	isano iri hagati y' imibare ibiri yerekana inshuro umubare umwe wikubye uwundi.	if there is 1 boy and 3 girls you could write the ratio as: 1 : 3 (for every one boy there are 3 girls).
rational number	Any number that can be written as a fraction with integers is called a rational number.	umubare ushobora kugaragazwa n' imibare ibiri, aho umwe uba ugabanya undi.	-1/30,-7/13,1/2, 1/5, 3/4,...
real numbers	a quantity that can be expressed as an infinite decimal expansion.	imibare yose ibaho harimo n' irimo ibice.	-22.22565, 3,13.335451,1/3, √6, 2,...
remainder	the amount left over when one quantity is divided by another.	umubare usigara nyuma yuko umubare umwe ugabanyije undi.	

reflection	a mirror image of a shape or an object, obtained from flipping the image/object.	uburyo bwo kugaragaza ishosha y' kintu uvuye ku murongo cyangwa ahantu runaka.	
right angle	angle that is exactly equal to 90°	inguni ingana nka dogere 90°	
sector(circle)	the plane figure enclosed by two radii of a circle or ellipse and the arc between them.		
segment	a part of a figure cut off by a line or plane intersecting it.	igice cy' igishushanyo cyatandukanyijwe n' ikindi hifashishijwe umurogo.	
semi-circle	a half of a circle.	kimwe cya kabiri cy' uruziga.	
sequence	a list of things (usually numbers) that are in order.	urutonde rw' ibintu (ubusanzwe ni imibare).	muri uru rutonde: 2,4,6,8,... umubare umwe ugenda urusha uwuri imbere ho imibare ibiri.
strictly positive(integer)	The strictly positive integers are the set defined as: Z>0:= {x∈Z:x>0} That is, all the integers that are strictly greater than zero: Z>0.	imibare itarimo ibice kandi isumba zeru.	1,2,3,4,5,......
subset	a set of which all the elements are contained in another set.	Itsinda rigizwe n' ibintu biri mu rindi tsinda ryisumbuyeho.	
symmetric point	The central point that splits the object or shape into two parts.	akadomo kagabanya ikintu mo ibice bibiri.	
tangent	a straight line or plane that touches a curve or curved surface at a point, but if extended does not cross it at that point.	Umurongo ugororotse ukora ku muzenguruko w' ikintu kiburungushuye (curve, circle).	

trapezium	a four-sided polygon with at least two sides parellel.	Ikinyampande enye gifite nibura impande ebyiri ziteganye.	
trapezoid	a four-sided polygon with at least two sides parellel.	Ikinyampande enye gifite nibura impande ebyiri ziteganye.	
tetramino	a geometric shape composed of four connected squares.	imiterere igizwe na kare enye zihuje.	
vertex	each angular point of a polygon, polyhedron, or other figure.	aho imirongo ibiri ihurira maze ikarema imfuruka.	

SYMBOLS

symbol	meaning	example / explanation
$\forall$	for all	$n+2$ is odd $\forall$n is an odd number
$\exists$	exists	if x$^2+x-2=0, \exists\; x\; in$ R
ϵ	belongs	$2n+1$ is odd $\forall n \epsilon$N
$\notin$	does not belong	if $x^2+1=0$, x $\notin$R
$\wedge$	intersects	if plane 1 is not parallel to plane 2, then plane 1 $\wedge$ plane 2
$\vert$	divides	5$\vert$ 25 and n $\vert$n^2+n
$\not\vert$	does not divide	2$\not\vert$21
$\approx$	is approximately equal to; is almost equal to.	3.01 $\approx$ 3 and $\pi\approx$ 3.14
$\neq$	is not equal to	$2\neq 3$
Δ	triangle	we say that ΔABC is equilateral if all sides are equal
gcd	greatest common divisor	$\gcd(17,170)=17$
LCM	lowest common multiple	LCM (15,6)=30
IE	this means that	$2\not\vert n+1$ IE n is an odd number
etc	and so on	4$\vert$ $n+2\;\forall\; n=2,6,10,14,18,22,etc$
WLOG	without loss of generality	for $x+y-2xy>1$ suppose WLOG $x\geq y$
	line 1 is parallel to line 2	
	AB=BC	
	angle ACB = angle BCD	
$\therefore$	Therefore	$x+2=5\quad\therefore$ x=3
Q.E.D.	that which was to be demonstrated	it is often placed at the end of a mathematical proof to indicate its completion
$\cap$	intersection	A= $\{a,b,c,d,e\}$, B= $\{b,c,f\}$, A$\cap B$ ={b,c}
$\cup$	union	A= $\{a,b,c,d,e\}$, B= $\{b,c,f\}$, A$\cup B$ ={a,b,c,d,e,f}
$[x,y[\; or\; [x,y)$	real numbers between x and y including x but not y.	
...	and so on	$\frac{1}{3}=0.3333333$...

$x!$	the product of all positive integers less than or equal to x	4!=4x3x2x1=24
$\lfloor x \rfloor$	the greatest integer less than or equal to x	$\lfloor 3.6 \rfloor = 3; \lfloor -2.3 \rfloor = -3$
$\lceil x \rceil$	the least integer greater than or equal to x	$\lceil 3.6 \rceil = 4; \lceil -2.3 \rceil = -2$
$\subseteq$	is a subset of	A= $\{a, b, c, d, e\}$, B= $\{b, c\}$ IE B$\subseteq A$
$\nsubseteq$	is not a subset of	A= $\{a, b, c, d, e\}$, B= $\{f, g, h\}$ IE B$\nsubseteq A$
∞	infinity	
$\propto$	is proportional to	$\frac{a}{b} = k$ where k is a positive number, $\therefore a \propto b$
:	ratio	if there are three dogs for every two cats, we would say the ratio of dog to cats is 3:2.
$\equiv$	equivalent to/ is congruent to	$3 \equiv 1 \mod 2$
$\emptyset$	empty set	A= $\{a, b, c, d, e\}$, B= $\{f, g, h\}$; A$\cap B = \emptyset$
N	natural numbers	
Z	integers	
Q	rational numbers	
R	real numbers	
$$\sum_{n=i}^{k} n \quad (1)$$	$i + ... + k$	given that n$\epsilon\mathbb{Z}$, $$\sum_{n=1}^{3} 2^n = 2 + 2^2 + 2^3 = 14 \quad (2)$$
$$\prod_{n=i}^{k} n \quad (3)$$	$i \times ... \times k$	given that n$\epsilon\mathbb{Z}$, $$\prod_{n=1}^{3} 2^n = 2 \times 2^2 \times 2^3 = 64 \quad (4)$$
π	the ratio of the circumference of a circle to its diameter; it is an irrational number.	$\pi = 3.141592653589793238...$
$\sim$	similar to	$\Delta ABC \sim \Delta DEF$, if their corresponding angles are congruent and their corresponding sides are in proportion.
$\perp$	perpendicular t0	If angle between line L$_1$and line $L_2$is equal to $90^{\circ}, L_1 \perp L_2$.
$\rightarrow$	implies(if...then...)	p:The triangle PQR is isosceles. q: Two of the angles of the triangle PQR have equal measure. $\therefore p \rightarrow q$
$\surd$	square root	$\sqrt{25} = 5$