

Mathematical Formulae
A Book of High School and Engineering Common Core
Mathematical Formulae

Agnij Mallick

December, 2020

Contents

I	Algebra	3
1	Logarithm	4
1.1	Basic Formulae	4
1.2	Series	4
2	Complex Numbers	5
2.1	Basic Formulae	5
2.2	Arithmetic Operation of Complex Number	5
2.3	Euler's Formula	5
2.4	Trigonometric Ratios in Complex Form	6
2.5	De Moivre's Formula	6
2.6	Application of Euler's and De Moivre's Formula	6
2.7	Roots of Unity	6
2.8	Important Relations of Complex Numbers	6
3	Progression	7
3.1	Arithmetic Progression (A.P.)	7
3.1.1	Sum of A.P. Series	7
3.1.2	Important Relation	7
3.2	Geometric Progression (G.P.)	7
3.2.1	The Value of 'r'	7
3.2.2	Sum of a G.P. Series	8
3.2.3	Important relations	8
3.3	Harmonic Progression (H.P.)	8
3.4	Arithmetico-Geometric Progression (A.G.P.)	8
3.4.1	Sum of A.G.P.:	8
3.5	Special Series	8
3.5.1	Riemann Zeta Function	9
3.5.2	Riemann's Infinite Series as an Integration	9
4	Test of Convergence of Infinite Series	10
4.1	Definition	10
4.2	Tests of Convergence	10
4.2.1	Comparison Test	10

4.2.2	Limit Form	10
4.2.3	Integral Test or Maclaurin-Cauchy Test	10
4.2.4	Ratio Test	11
4.2.5	D'Alembert's Ratio Test	11
4.2.6	Rabbe's Test	11
4.2.7	Cauchy's Root Test	11
4.2.8	Logarithmic Test	12
5	Determinants	13
5.1	Definition	13
5.1.1	Minor and Cofactor	13
5.2	Properties of Determinants	13
5.3	Cramer's Rule	14
5.3.1	Consistency Test	15
6	Matrices	16
6.1	Sum of Two Matrices	16
6.2	Multiplication of Two Matrices	
	16	
6.2.1	Multiplicative Properties	16
6.3	Adjoint of a Matrix	17
6.4	Martin's Rule	17
7	Binomial Theorem	18
7.1	Expansion of a binomial expression	18
7.2	Trinomial Expansion	18
7.3	Properties of Coefficients	18
7.4	Pascal's Rule	19
8	Boolean Algebra	20
9	Remainder Theorems	21
9.1	Remainder Theorem	21
9.2	Euler's Remainder Theorem	21
9.2.1	Euler's Totient Function	21
9.3	Wilson Theorem	22

Part I

Algebra

Chapter 1

Logarithm

1.1 Basic Formulae

For $a^x = b$:

$$\log_a x, \forall x \leq 0 \text{ is undefined} \quad (1.1)$$

$$\log_a b = x, \text{ if } a^x = b, a \neq 1 \quad (1.2)$$

$$\log_b a^m = m \log_b a, \text{ for } a^m = b \quad (1.3)$$

$$a^{\log_a x} = x \quad (1.4)$$

$$a^{\log_b c} = c^{\log_b a} \quad (1.5)$$

$$\frac{1}{\log_a b} = \log_b a \quad (1.6)$$

$$\log_c(ab) = \log_c a + \log_c b \quad (1.7)$$

$$\log_c \left(\frac{a}{b} \right) = \log_c a - \log_c b \quad (1.8)$$

$$|\log_a x| = \begin{cases} -\log_a x, & \text{if } 0 < x < 1 \\ \log_a x, & \text{if } 1 \leq x < \infty \end{cases} \quad (1.9)$$

1.2 Series

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots \infty = \lim_{n \rightarrow \infty} \sum_{i=0}^n \frac{x^i}{i!} \quad (1.10)$$

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots \infty = \lim_{n \rightarrow \infty} \sum_{i=1}^n (-1)^{(i-1)} \frac{x^i}{i} \quad (1.11)$$

Chapter 2

Complex Numbers

2.1 Basic Formulae

For $z = x + iy$,

$$|z| = \sqrt{x^2 + y^2} \quad (2.1)$$

$$\tan \theta = \frac{y}{x} \quad (2.2)$$

$$\bar{z} = x - iy \quad (2.3)$$

2.2 Arithmetic Operation of Complex Number

For two complex numbers $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$:

$$z_1 + z_2 = (x_1 + x_2) + i(y_1 + y_2) \quad (2.4)$$

$$z_1 z_2 = (x_1 x_2 - y_1 y_2) + i(x_1 y_2 + x_2 y_1) \quad (2.5)$$

$$|z_1 z_2| = |z_1| \cdot |z_2| \quad (2.6)$$

$$\frac{z_1}{z_2} = \frac{(x_1 x_2 + y_1 y_2) + i(x_2 y_1 - x_1 y_2)}{a_2^2 + b_2^2} \quad (2.7)$$

$$\left| \frac{z_1}{z_2} \right| = \frac{|z_1|}{|z_2|} \quad (2.8)$$

2.3 Euler's Formula

$$z = r e^{i\theta}, \text{ where} \quad (2.9)$$

$$r = |z| \quad (2.10)$$

$$e^{i\theta} = \cos \theta + i \sin \theta \quad (2.11)$$

$$\theta = \arctan \left(\frac{y}{x} \right) \quad (2.12)$$

2.4 Trigonometric Ratios in Complex Form

$$e^{i\theta} + e^{-i\theta} = 2 \cos \theta \quad (2.13)$$

$$\Rightarrow \cos \theta = \frac{e^{i\theta} + e^{-i\theta}}{2} \quad (2.14)$$

$$e^{i\theta} - e^{-i\theta} = 2 \sin \theta \quad (2.15)$$

$$\Rightarrow \sin \theta = \frac{e^{i\theta} - e^{-i\theta}}{2} \quad (2.16)$$

2.5 De Moivre's Formula

According to DeMoivre's Formula:

$$(\cos \theta + i \sin \theta)^n = \cos(n\theta) + i \sin(n\theta) \quad (2.17)$$

Proof

$$\begin{aligned} \cos \theta + i \sin \theta &= e^{i\theta} \\ \Rightarrow (\cos \theta + i \sin \theta)^n &= e^{n(i\theta)} \\ &= \cos(n\theta) + i \sin(n\theta) \\ &\text{Q.E.D.} \end{aligned}$$

2.6 Application of Euler's and De Moivre's Formula

For $z_1 = |r_1| e^{i\theta_1}$ and $z_2 = |r_2| e^{i\theta_2}$

$$z_1 z_2 = (r_1 r_2) e^{i(\theta_1 + \theta_2)} \quad (2.18)$$

$$\frac{z_1}{z_2} = \left(\frac{r_1}{r_2} \right) e^{i(\theta_1 - \theta_2)} \quad (2.19)$$

2.7 Roots of Unity

$$\sqrt[n]{1} = e^{i \frac{2k\pi}{n}}, \text{ where } k \in [0, n-1] \quad (2.20)$$

2.8 Important Relations of Complex Numbers

$$|z_1 + z_2| \leq |z_1| + |z_2| \quad (2.21)$$

$$|z_1 - z_2| \leq |z_1| + |z_2| \quad (2.22)$$

$$|z_1 - z_2| \geq ||z_1| - |z_2|| \quad (2.23)$$

$$|z_1 + z_2| \geq ||z_1| - |z_2|| \quad (2.24)$$

$$|z_1 + z_2|^2 = 2 \left(|z_1|^2 + |z_2|^2 \right) \quad (2.25)$$

Chapter 3

Progression

3.1 Arithmetic Progression (A.P.)

An arithmetic sequence is $a, a + n, a + 2n, \dots \infty$ or $t_n = a + (n - 1)d$, where a is the first term, d is the common difference, and n is the n^{th} -term.

An arithmetic series is $a + (a + d) + (a + 2d) + \dots \infty$.

3.1.1 Sum of A.P. Series

$$\begin{aligned} S_n &= a + (a + d) + \dots + (a + \overline{n - 2}d) + (a + \overline{n - 1}d) \\ S_n &= (a + \overline{n - 1}d) + (a + \overline{n - 2}d + \dots + (a + d) + a \\ &\Rightarrow 2S_n = n(2a + \overline{n - 1}d) \\ &\Rightarrow S_n = \frac{n}{2}(2a + \overline{n - 1}d) \end{aligned} \quad (3.1)$$

3.1.2 Important Relation

If the three terms a, b, c are in A.P., then

$$2b = a + c \quad (3.2)$$

3.2 Geometric Progression (G.P.)

An geometric sequence is $a, ar, ar^2, \dots \infty$ or $t_n = ar^{n-1}$, where a is the first term, r is the common ratio, and n is the n^{th} -term. An geometric series is $a + ar + ar^2 + \dots \infty$.

3.2.1 The Value of 'r'

$$r = \frac{t_2}{t_1} = \frac{t_3}{t_2} = \dots = \frac{t_n}{t_{n-1}} \quad (3.3)$$

3.2.2 Sum of a G.P. Series

For a definite G.P. series, where there are n terms in the series, the sum of the series is:

$$S_n = \frac{a|r^n - 1|}{|r - 1|} \quad (3.4)$$

For an infite G.P. series the sum of the series is defined for $r < 1$. Sum of such a series is:

$$S_\infty = \frac{a}{1 - r} \quad (3.5)$$

3.2.3 Important relations

If the three terms a, b, c are in G.P., then:

$$b^2 = ac \quad (3.6)$$

3.3 Harmonic Progression (H.P.)

If a, b, c are terms of an H.P. then $\frac{1}{a}, \frac{1}{b}, \frac{1}{c}$ are in A.P.

$$\frac{2}{b} = \frac{1}{a} + \frac{1}{c} \quad (3.7)$$

$$\Rightarrow b = \frac{2ac}{a + c} \quad (3.8)$$

3.4 Arithmetico-Geometric Progression (A.G.P.)

Sequence $a, (a+d)r, (a+2d)r^2, \dots, (a+\overline{n-1}d)r^{n-1}$, where $a \rightarrow$ first term of A.G.P., $d \rightarrow$ common difference, and $r \rightarrow$ common ratio.

3.4.1 Sum of A.G.P.:

For an infinite A.G.P. series, the sum is defined for $r < 1$:

$$S_\infty = \frac{a}{1 - r} + \frac{dr}{(1 - r)^2} \quad (3.9)$$

3.5 Special Series

For $n \in \mathbb{N}$

$$1 + 2 + 3 + \dots + (n - 1) + n = \frac{n(n - 1)}{2} \quad (3.10)$$

$$1^2 + 2^2 + 3^2 + \dots + (n - 1)^2 + n^2 = \frac{n(n + 1)(2n + 1)}{6} \quad (3.11)$$

$$1^3 + 2^3 + 3^3 + \dots + (n - 1)^3 + n^3 = \left[\frac{n(n - 1)}{2} \right]^2 \quad (3.12)$$

3.5.1 Riemann Zeta Function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad (3.13)$$

3.5.2 Riemann's Infinite Series as an Integration

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=r_1}^{r_2} f\left(\frac{i}{n}\right) = \int_{\frac{r_1}{n}}^{\frac{r_2}{n}} f(x) dx \quad (3.14)$$

Chapter 4

Test of Convergence of Infinite Series

If $a_1, a_2, a_3, \dots, a_n$ is a sequence by a_n and their sum of series is S_n , then the following apply.

4.1 Definition

If

$$\lim_{n \rightarrow \infty} S_n = l$$

where l is a finite value, the series S_n is said to converge. A non-convergent series is called a divergent series.

4.2 Tests of Convergence

4.2.1 Comparison Test

If u_n and v_n are two positive series, then:

1. (a) v_n converges
(b) $u_n \leq v_n \forall n$ Then u_n converges.
2. (a) v_n diverges
(b) $u_n \geq v_n \forall n$ Then u_n diverges.

4.2.2 Limit Form

If

$$\lim_{x \rightarrow \infty} \frac{u_n}{v_n} = l$$

where l is a finite quantity $\neq 0$, then u_n and v_n converge and diverge together.

4.2.3 Integral Test or Maclaurin-Cauchy Test

For a series

$$\sum_{i=N}^{\infty} f(x), \text{ where } N \in \mathbb{Z} \quad (4.1)$$

will only converge if the improper integral

$$\int_N^{\infty} f(x)dx \quad (4.2)$$

is finite.

If the improper integral is finite, the upper and lower limit of the infinite series is given by:

$$\int_N^{\infty} f(x)dx \leq \sum_{i=N}^{\infty} f(x) \leq f(N) + \int_N^{\infty} f(x)dx \quad (4.3)$$

4.2.4 Ratio Test

If, for two series $\sum u_n$ and $\sum v_n$:

1. (a) $\sum v_n$ converges
 (b) from or after a particular term $\frac{u_n}{u_{n+1}} > \frac{v_n}{v_{n+1}}$, then u_n converges.
2. (a) $\sum v_n$ diverges
 (b) from or after a particular term $\frac{u_n}{u_{n+1}} < \frac{v_n}{v_{n+1}}$, then u_n diverges.

4.2.5 D'Alembert's Ratio Test

$$\lim_{n \rightarrow \infty} \frac{u_n}{u_{n+1}} = \lambda \quad (4.4)$$

- series converges if $\lambda < 1$
- series diverges if $\lambda > 1$
- fails if $\lambda = 1$

4.2.6 Rabbe's Test

$$\lim_{n \rightarrow \infty} n \left[\frac{u_n}{u_{n+1}} - 1 \right] = \kappa \quad (4.5)$$

- series converges if $\kappa < 1$
- series diverges if $\kappa > 1$
- fails if $\kappa = 1$

4.2.7 Cauchy's Root Test

$$\lim_{n \rightarrow \infty} |u_n|^{\frac{1}{n}} = \lambda \quad (4.6)$$

- series converges for $\lambda < 1$
- series diverges for $\lambda > 1$
- test fails for $\lambda = 1$

4.2.8 Logarithmic Test

$$\lim_{n \rightarrow \infty} n \log \left(\frac{u_n}{u_{n+1}} \right) = \kappa \quad (4.7)$$

- series converges for $\kappa < 1$
- series diverges for $\kappa > 1$
- test fails for $\kappa = 1$

Chapter 5

Determinants

5.1 Definition

For a determinant:

$$\Delta = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = a_1 \begin{vmatrix} b_2 & c_2 \\ b_3 & c_3 \end{vmatrix} - b_1 \begin{vmatrix} a_2 & c_2 \\ a_3 & c_3 \end{vmatrix} + c_1 \begin{vmatrix} a_2 & b_2 \\ a_3 & b_3 \end{vmatrix} \quad (5.1)$$

5.1.1 Minor and Cofactor

For a third order determinant

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}$$

Minor

$$M(a_{11}) = M_{11} = \begin{vmatrix} b_2 & c_2 \\ b_3 & c_3 \end{vmatrix} \quad (5.2)$$

i.e., all the terms of determinant except those in the same row and columns as the one of which the minor is being calculated.

Cofactor

$$C_{ij} = (-1)^{i+j} M_{ij} \quad (5.3)$$

5.2 Properties of Determinants

1. Transposing a determinant does not alter its value.

$$\Delta = \Delta^T \quad (5.4)$$

2. If rows and columns are interchanges m times, the value of the new determinant is

$$\Delta' = (-1)^m \Delta \quad (5.5)$$

3. If two parallel lines are equal, then $\Delta = 0$

4. For $\Delta = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}$ and $\Delta_1 = \begin{vmatrix} ka_1 & kb_1 & kc_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}$, then $\Delta_1 = k\Delta$

5. For $\Delta = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}$ and $\Delta_1 = \begin{vmatrix} ka_1 & b_1 & c_1 \\ ka_2 & b_2 & c_2 \\ ka_3 & b_3 & c_3 \end{vmatrix}$, then $\Delta_1 = k\Delta$

6. For $C_n \rightarrow k_1 C_l + k_2 C_m + k_3 C_n$ or $R_n \rightarrow k_1 R_l + k_2 R_m + k_3 R_n$, $\Delta' = \Delta$

5.3 Cramer's Rule

For a system of equations:

$$a_1x + b_1y + c_1z = d_1$$

$$a_2x + b_2y + c_2z = d_2$$

$$a_3x + b_3y + c_3z = d_3$$

the following determinants are defined:

$$D = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}$$

$$D_x = \begin{vmatrix} d_1 & b_1 & c_1 \\ d_2 & b_2 & c_2 \\ d_3 & b_3 & c_3 \end{vmatrix}$$

$$D_y = \begin{vmatrix} a_1 & d_1 & c_1 \\ a_2 & d_2 & c_2 \\ a_3 & d_3 & c_3 \end{vmatrix}$$

$$D_z = \begin{vmatrix} a_1 & b_1 & d_1 \\ a_2 & b_2 & d_2 \\ a_3 & b_3 & d_3 \end{vmatrix}$$

The solution for the system of equations is:

$$x = \frac{D_x}{D} \quad (5.6)$$

$$y = \frac{D_y}{D} \quad (5.7)$$

$$z = \frac{D_z}{D} \quad (5.8)$$

5.3.1 Consistency Test

1. If $D \neq 0$, the system is consistent and has unique solutions.
2. If $D = D_x = D_y = D_z = 0$, the system may or may not be consistent and it will have infinite solutions and the system will be dependent.
3. If $D = 0$ and at least one of D_x, D_y, D_z is non zero, the system is inconsistent

Chapter 6

Matrices

For a matrix,

$$A_{m \times n} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

and where I_p is an identity matrix of the p^{th} order, the following relations are applicable.

6.1 Sum of Two Matrices

$$A_{m \times n} + B_{m \times n} = \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \cdots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{21} & \cdots & a_{2n} + b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \cdots & a_{mn} + b_{mn} \end{bmatrix} \quad (6.1)$$

6.2 Multiplication of Two Matrices

If

$$C_{m \times p} = A_{m \times n} \cdot B_{n \times p} \quad (6.2)$$

then,

$$c_{ik} = \sum_{j=1}^n a_{ij} \cdot b_{jk} \quad (6.3)$$

6.2.1 Multiplicative Properties

1. Multiplication of matrices is associative, hence $(AB)C = A(BC)$.
2. $AI = A$

3. $A \cdot A^{-1} = I$
4. $A \cdot (\text{adj } A) = (\text{adj } A) \cdot A = |A|I$
5. $A^{-1} = \frac{1}{|A|}(\text{adj } A)^t$
6. $(AB)^t = B^t A^t$

6.3 Adjoint of a Matrix

$$\text{adj } A = \begin{bmatrix} M_{11} & M_{12} & \cdots & M_{1n} \\ M_{21} & M_{22} & \cdots & M_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ M_{m1} & M_{m2} & \cdots & M_{mn} \end{bmatrix}^t, \text{ where } M_{ij} \text{ is the minor of } a_{ij} \quad (6.4)$$

6.4 Martin's Rule

For a system of equation,

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

The system can be written as:

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} \quad (6.5)$$

$$\Rightarrow AX = B \quad (6.6)$$

$$\Rightarrow X = A^{-1}B \quad (6.7)$$

Chapter 7

Binomial Theorem

For a binomial expansion $(a + b)^n$, there are $(n + 1)$ terms and $(a + b + c)^n$ has $\frac{(n + 1)(n + 2)}{2}$ terms.

7.1 Expansion of a binomial expression

$$\begin{aligned}
 (a + b)^n &= {}^nC_0 a^n b^0 + {}^nC_1 a^{n-1} b^1 + {}^nC_2 a^{n-2} b^2 + \cdots + {}^nC_n a^0 b^n \\
 &= \sum_{i=0}^n {}^nC_i a^{n-i} b^i \\
 &\forall n \in \mathbb{N}
 \end{aligned} \tag{7.1}$$

$$\begin{aligned}
 (a + b)^n &= a^n b^0 + n a^{n-1} b + \frac{n(n-1)}{2!} a^{n-2} b^2 + \cdots + \frac{n(n-1) \cdots 3 \cdot 2 \cdot 1}{n!} a^0 b^n + \cdots \infty \\
 &\forall n \in \mathbb{R}
 \end{aligned} \tag{7.2}$$

7.2 Trinomial Expansion

For $(a + b + c)^n$:

$$\begin{aligned}
 (a + b + c)^n &= \sum \frac{n!}{i!j!k!} a^i b^j c^k \\
 &\forall (i + j + k) = n; i, j, k, n \in \mathbb{N}
 \end{aligned} \tag{7.3}$$

7.3 Properties of Coefficients

$$\text{Sum of Co-efficients: } C_0 + C_1 + C_2 + \cdots + C_{n-1} + C_n = 2^n \tag{7.4}$$

$$\text{Sum of Odd Co-efficients: } C_0 + C_2 + C_4 + \cdots + C_{2n-3} + C_{2n-1} = 2^{n-1} \tag{7.5}$$

$$C_0 - C_1 + C_2 - \cdots + C_{2n-1} - C_{2n} = 0 \tag{7.6}$$

7.4 Pascal's Rule

For $1 \leq k \leq n$ and $k, n \in \mathbb{N}$:

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k} \quad (7.7)$$

Chapter 8

Boolean Algebra

Let B be a set of a, b, c with operations sum $(+)$ and product (\cdot) .
Then B is said to belong to the Boolean Structure if the following conditions are satisfied:

Table 8.1: Properties of Boolean Algebraic Structure

Property	Name of Property
$a + b \in B$ $a \cdot b \in B$	Closure Property
$a + b = b + a$ $a \cdot b = b \cdot a$	Associative Law
$a(b + c) = ab + ac$ $a + bc = (a + b)(a + c)$	Commutative Law
$\{0, 1\} \in B$ $a + 0 = a$ $a + 1 = 1$ $a \cdot 0 = 0$ $a \cdot 1 = a$	Laws of 1 and 0
$a + ab = a$ $a(a + b) = a$	Absorption Law
$(a + b)' = (a'b')$	De'Morgan's Law

Chapter 9

Remainder Theorems

9.1 Remainder Theorem

If a function $f(x)$ is divided by a binomial $x - a$, then the remainder is provided by $f(a)$.

$$\frac{f(x)}{x - a} \equiv f(a) \pmod{(x - a)} \quad (9.1)$$

Worked Example

Find the remainder when $f(x) = x^3 - 4x^2 - 7x + 10$ is divided by $(x - 2)$.
The remainder:

$$R = (x^3 - 4x^2 - 7x + 10) \pmod{(x - 2)}$$

is given by:

$$\begin{aligned} R = f(2) &= (2)^3 - 4(2)^2 - 7(2) + 10 \\ &= 8 - 16 - 14 + 10 = -12 \end{aligned}$$

9.2 Euler's Remainder Theorem

According to Euler's Remainder Theorem, if x and n are two co-prime numbers:

$$x^{\varphi(n)} \equiv 1 \pmod{n}, x, n \in \mathbb{Z}^+ \quad (9.2)$$

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

9.2.1 Euler's Totient Function

For a number defined as:

$$n = \prod_{i=1}^r a_i^{b_i} \quad (9.3)$$

then Euler's totient function is defined as:

$$\begin{aligned}\varphi(n) &= n \cdot \left[\left(1 - \frac{1}{a_1}\right) \cdot \left(1 - \frac{1}{a_2}\right) \cdot \left(1 - \frac{1}{a_3}\right) \cdots \right] \\ &= n \prod_{i=1}^r \left(1 - \frac{1}{a_i}\right)\end{aligned}\tag{9.4}$$

Worked Example

Find the remainder if 3^{76} is divided by 35.

Since:

$$35 = 5^1 \times 7^1$$

Hence the totient quotient of 35 is:

$$\begin{aligned}\varphi(35) &= 35 \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{7}\right) \\ &= 35 \times \frac{4}{5} \times \frac{6}{7} \\ &= 24\end{aligned}$$

Hence Euler's Theorem yields:

$$\begin{aligned}3^{24} &\equiv 1 \pmod{35} \\ 3^{76} &\equiv 3^{24 \times 3 + 4} \\ &\equiv (3^{24})^3 \times 3^4 \pmod{35} \\ &\equiv (1)^3 \times 3^4 \pmod{35} \\ &\equiv 81 \pmod{35} \\ &\equiv 11 \pmod{35}\end{aligned}$$

The remainder when 3^{76} is divided by 35 is 11.

9.3 Wilson Theorem

According to Wilson Theorem:

$$(n-1)! \equiv -1 \pmod{n}\tag{9.5}$$

Worked Example

Find the remainder when $28!$ is divided by 31.

By Wilson's Theorem:

$$\begin{array}{ll}
 30! & \equiv -1 \pmod{31} \\
 \Rightarrow 30 \cdot 29 \cdot 28! & \equiv -1 \pmod{31} \\
 \text{Let } 28! \pmod{31} & = x \\
 \Rightarrow (-1) \cdot (-2) \cdot x & \equiv 30 \pmod{31} \\
 \Rightarrow 2x & = 30 \\
 \Rightarrow x & = 15
 \end{array}$$

The remainder when $28!$ is divided by 31 is 15.