Chapter-I

Numbers and Quantification

Learning Objectives :

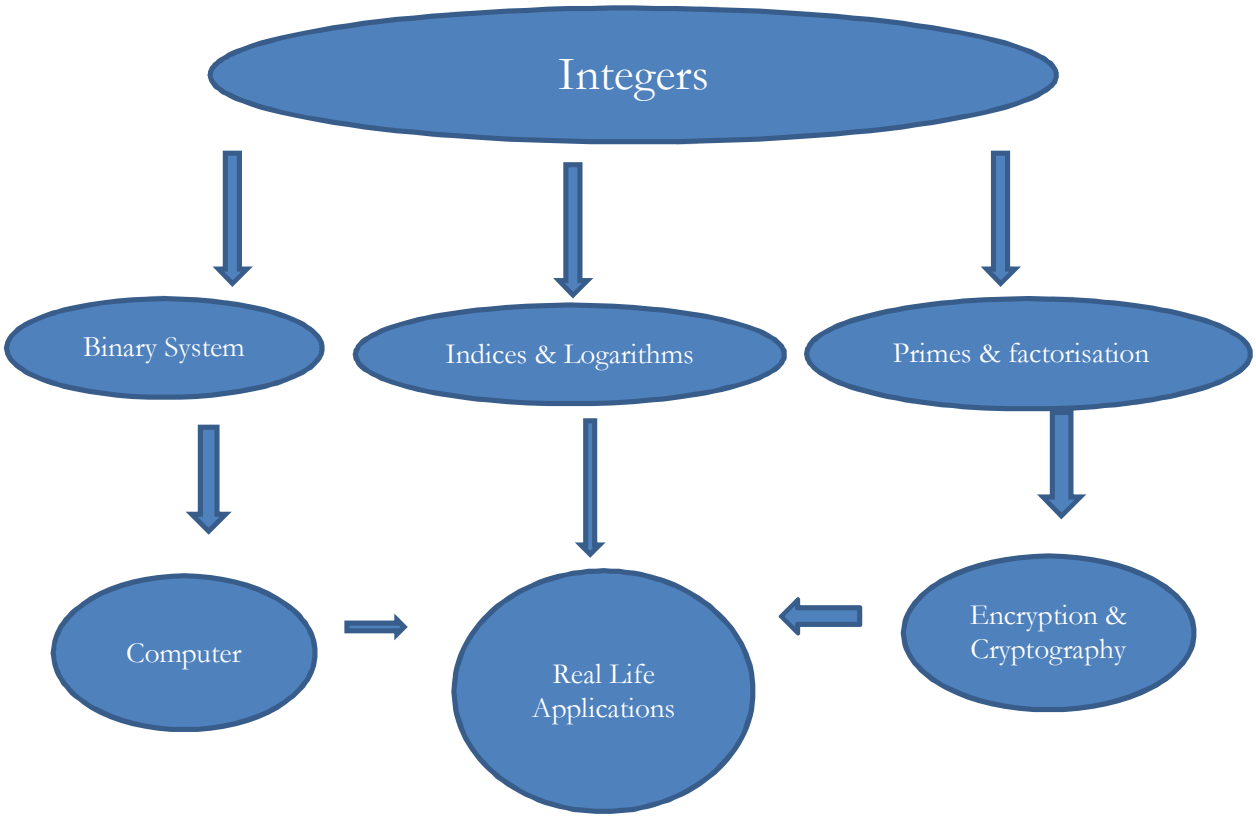
Students will be able to:

- identify prime numbers;
- explain the importance of prime numbers particularly in encryption;
- write numbers in binary system;
- explain basic notions of complex numbers and why are they introduced;
- use logarithms in different applications;
- above ideas in the day to day life.

Previous Knowledge:

The ideas and concepts are self contained and based on Secondary Mathematics.

Concept Map



1.1 Introduction:

In this modern age of computers, primes play an important role to make our communications secure. So understanding primes are very important. In Section 1.1., we give an introduction to primes and its properties and give its application to encryption in 1.2. The concept of binary numbers and writing a number in binary and converting a number in binary to decimal is presented in 1.3. The Section 1.4 introduces the concept of complex numbers with some basic properties. In Sections 1.5, 1.6 and 1.7. logarithms, its properties and applications to real life problems are introduced. Finally in Section 1.8 we give a number of word problems which we come across in everyday life.

1.2 Prime Numbers

We say integer a divides b, and write a | b in symbols, if b = ac with c ∈ Z. For example 9 | 27. If a | b, we say a is a factor or a is divisor of b. And we also say b is a multiple of a. It is easy to see that 1 and –1 are divisors of any integer and every non-zero integer is a divisor of 0. We write a ∤ b if a does not divide b. For example 5 ∤ 13.

Prime numbers are the building blocks of number system. A positive integer p > 1 is called a prime if 1 and p are the only positive divisors of p. For example, 2, 3, 5, 7, 11, 13, ... are primes. We say a positive integer n > 1 is composite if it is not a prime. Thus a composite number n > 1 has a positive divisor different from 1 and n itself. For example, 4, 6, 8, 9, 10, ... are composites. The number 1 is neither a prime nor a composite.

One of the important properties of positive integers for which the primes play an important role is The Fundamental Theorem of Arithmetic. This theorem states that every positive integer n > 1 can be written as product of primes and it is unique upto order of primes. Hence every n ∈ N can be written uniquely in the form

$$n = P_1^{a_1} P_2^{a_2} P_3^{a_3} \ldots\ldots P_r^{a_r}$$

where $p_1 < p_2 < \ldots\ldots < p_r$ are distinct primes and $a_1, a_2, \ldots\ldots, a_r$ are positive integers. This is called the unique factorization of n. For example

$10 = 2 \cdot 5$

$36 = 2^2 \cdot 3^2$

$105 = 3 \cdot 5 \cdot 7$

$104568 = 2^3 \cdot 3 \cdot 4357.$

For a prime p, the factorization of p is just p = p. Now you can answer why 1 is not considered a prime. If 1 is a prime, then

$$10 = 1 \cdot 2 \cdot 5 = 1^2 \cdot 2 \cdot 5 = 1^3 \cdot 2 \cdot 5 = \ldots\ldots = 1^r \cdot 2 \cdot 5$$

for any r > 1, thereby giving a number of factorization of 10, thereby violating

the Fundamental Theorem of Arithmetic. Also 1 cannot be a considered a composite number. (Why?)

A consequence of the Fundamental Theorem of Arithmetic is that every $n > 1$ has a prime divisor p. Clearly n itself is the unique prime divisor p if n is a prime and $1 < p < n$ if n is composite. This consequence implies one of the first theorem in Mathematics, which is well-known as Euclid's Theorem.

Theorem 1.1.1. Euclid's Theorem: There are infinitely many prime numbers.

Proof. Suppose there are finitely many prime numbers, viz., $p_1, p_2, \ldots\ldots, p_r$. Consider the number.

$$N = p_1p_2 \ldots\ldots p_r + 1$$

Clearly $N > 1$. Hence by the Fundamental Theorem of Arithmetic, it has prime divisor p. Then $p = p_i$ for some $1 \leq i \leq r$. However none of the primes $p_i \mid N$ for each $1 \leq i \leq r$.

Also $N \neq p_i$ for any i. This is a contradiction which proves that there are infinitely many primes.

Though Euclid's Theorem tells us that there are infinitely many primes, finding large numbers is a challenge. In fact the largest known prime number as of today is the 24862048 digit prime

$$2^{82589933} - 1$$

which was discovered in 2018. This is a special kind of primes called Mersenne Primes.

One of the ways to check whether a given number is a prime is the well-known Sieve of Erasthosthenes. This works on the principle that $n > 1$ is composite if has a prime divisor $p \leq \sqrt{n}$. We illustrate this Sieve and find all primes upto 100. We list all positive integers upto 100. A numbers $1 < n \leq 100$ is a composite if n has a prime divisor $\leq \sqrt{n} = \sqrt{100} = 10$.

The primes upto 10 are 2, 3, 5, 7. We start by crossing 1. Since 2 is a prime, we circle 2 and strike off all numbers divisible by 2.

~~1~~	②	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~
51	~~52~~	53	~~54~~	55	~~56~~	57	~~58~~	59	~~60~~
61	~~62~~	63	~~64~~	65	~~66~~	67	~~68~~	69	~~70~~
71	~~72~~	73	~~74~~	75	~~76~~	77	~~78~~	79	~~80~~
81	~~82~~	83	~~84~~	85	~~86~~	87	~~88~~	89	~~90~~
91	~~92~~	93	~~94~~	95	~~96~~	97	~~98~~	99	~~100~~

3 is the first number among the remaining ones. We circle 3 now and strike off all numbers divisible by 3. 5 is the first among the remaining numbers which we circle and strike off all numbers divisible by 5. Next 7 is the first number left which we circle now and strike off all numbers divisible by 7.

~~1~~	②	③	~~4~~	⑤	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

The remaining numbers are all primes. In fact all the primes upto 100 are

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

which are 25 in number. This method to find primes is not suitable when the numbers are very large.

Suggested Project: Find all prime numbers upto 10000 by using the Sieve of Erasthosthenes.

Srinivasa Ramanujan is one of Indian genius who is very much well-known for his contributions to Mathematics, particularly prime numbers. Given n ≥ 1, we define the n-th Ramanujan Prime to be the least positive integer Rn such that there are at least n primes between $\pi(\frac{x}{2})$ and $\pi x \forall x \geq R_n$. It turns out that Rn are all primes. The first ten Ramanujan primes are

$R_1 = 2, R_2 = 11, R_3 = 17, R_4 = 29, R_5 = 41, R_6 = 47, R_7 = 59, R_8 = 67, R_9 = 71, R_{10} = 97.$

1.3 Why prime numbers are important?: Encryptions using Prime Numbers

Primes are one of the most useful numbers nowadays as they have lots of applications in the current digital world. In fact, prime numbers are used to make our online communications secure. In this section, we will explain how prime numbers are used in Cryptography.

Cryptography is the science of using mathematics to encrypt and decrypt data. It enable us to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. Cryptanalysis is the science of analyzing and breaking secure communication. It involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Basically Cryptanalysts are attackers and Cryptographers are defenders. Cryptology is the science which involves both Cryptography and Cryptanalysis.

In Cryptography, we have the notion of Encryption and Decryption. Encryption is the method of disguising plaintext (or the message in Data format which can be read and understood without any special measures) in such a way as to hide its substance. Encrypting plaintext results in unreadable gibberish called Cipher text. Encryption ensures that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. Decryption is the process of reverting cipher text to its original plaintext.

Cryptography works by using a cryptographic algorithm which is a mathematical function used in encryption and decryption process. It works in combination with a key (a word, number or phrase) to encrypt the plaintext.

Same plaintext encrypts to different ciphertext with different keys. The security of encrypted data depends entirely on two things. The strength of the cryptographic algorithm and the secrecy of the key. A Cryptosystem is a cryptographic algorithm plus all possible keys and all the protocols that make it work. Following are the requirements for a good cryptosystem.

(a) Authentication: Provides the assurance of some ones identity.

(b) Confidentiality : Protects against disclosure to unauthorized identities.

(c) Non-Repudiation: Protects against communications originator to later deny it.

(d) Integrity: Protects from unauthorized data alteration.

Some of the Cryptosystems are RSA, Diffie-Hellman, ElGamal, Elliptic Curve Cryptosystems. RSA which was invented in 1978 is one of the most popular and widely used cryptosystem. It is named after its inventors Ron Rivest, Adi Shamir and Richard Adleman. This cryptosystem is based on the property of primes. We will now explain the RSA Cryptosystem and illustrate how the prime numbers are used. For that we need some basics.

Definition: A positive integer d is the greatest common divisor or highest common factor of two numbers a and b if d is the largest positive common divisor of a and b, i.e.,

$d \mid a$ and $d \mid b$,

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

We write d = gcd(a, b) or simply d = (a, b) if d is the greatest common divisor of a and b. For example

gcd (10, 25) = 5

gcd (3, 17) = 1

gcd (4680, 15708) = 12.

We say a and b are relatively prime or coprime if gcd(a, b) = 1. For example, 3

and 17 are relatively prime. Note that gcd(a, b) = gcd(b, a). If a | b. then gcd(a, b) = a.

One of the ways to find gcd(a, b) is to compute the unique factorization of a and b. If we know the factorizations

$$a = P_1^{a_1} P_2^{a_2} \ldots\ldots P_r^{a_r} \quad \text{and}$$
$$b = P_1^{b_1} P_2^{b_2} \ldots\ldots P_r^{b_r}$$

then

$$d = \gcd(a, b) = p_1^{\min(a1, b1)} p_2^{\min(a2, b2)} \ldots\ldots p_r^{\min(ar, br)}$$

For example, let a = 4680 and b = 15708. Then

$$a = 4680 = 2^3 \cdot 3^2 \cdot 5 \cdot 13 = 2^3 \cdot 3^2 \cdot 5^1 \cdot \cdot 7^0 \cdot 11^0 \cdot 13^1 \cdot 17^0$$

$$b = 15708 = 2^2 \cdot 3 \cdot 7 \cdot 11 \cdot 17 = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^1 \cdot 13^0 \cdot 17^1$$

so that

$$\gcd(4680, 15708) = 2^{\min(2, 3)} \cdot 3^{\min(2, 1)} \cdot 5^{\min(1, 0)} \cdot 7^{\min(0, 1)} \cdot 11^{\min(0, 1)} \cdot 13^{\min(1, 0)} \cdot 17^{\min(0, 1)}$$

$$= 2^2 \cdot 3^1 = 12.$$

For large numbers, finding factorization is not easy. For that we use Euclid's GCD Algorithm.

Given positive integers a > 0 and b, there exist unique quotient q and remainder r with

$$b = aq + r, \quad 0 \leq r < |b|.$$

Note that r = 0 if and only if b | a. Also q = r = 0 when b = 0 and we have 0 = a . 0 + 0. We use the following fact.

$$\gcd(a, b) = \gcd(a, b - aq) \quad \text{for any } q$$

Now we define Euclid's GCD Algorithm and also illustrate with an example. Let b > a and a | b. Then

$b = aq + r,$	$0 < r < a$	$a = 4680, b = 15708$	
$a = rq_1 + r_1,$	$0 < r_1 < r$	$15708 = 3 \cdot 4680 + 1668,$	$0 < 1668 < 4680$
$r = r_1q_2 + r_2,$	$0 < r_2 < r_1$	$4680 = 2 \cdot 1668 + 1344,$	$0 < 1344 < 1668$
$r_1 = r_2q_3 + r_3,$	$0 < r_3 < r_2$	$1668 = 1 \cdot 1344 + 324,$	$0 < 324 < 1344$
$r_2 = r_3q_4 + r_4,$	$0 < r_4 < r_3$	$1344 = 4 \cdot 324 + 48,$	$0 < 48 < 324$
$r_3 = r_4q_5 + r_5,$	$0 < r_5 < r_4$	$324 = 6 \cdot 48 + 36,$	$0 < 36 < 48$
$r_4 = r_5q_6 + 0$		$48 = 1 \cdot 36 + 12,$	$0 < 12 < 36$
		$36 = 3 \cdot 12 + 0.$	

Here the last non-zero remainder, namely r_5 is the gcd (a, b). The novelty of this method is that we do not need to factor a and b.

We now introduce modular arithmetic. Let $m \geq 1$. We say a is congruent to b modulo m and write $a \equiv b \pmod{m}$ if $a - b$ is divisible by m or $a = b + km$ for some integer k. For example, $17 \equiv 2 \pmod{5}$ since $17 - 2 = 15$ is divisible by 5. It is easy to see that if a b (mod m), then b a (mod m). Basically a b (mod m) means both a and b has the same remainder when divided by b. One of the properties of modular arithmetic is the following:

If $a \equiv b \pmod{m}$ and $t \geq 1$, then $a^t \equiv b^t \pmod{m}$.

We can now state Euler's Theorem.

Theorem 1.2.1. Euler's Theorem: Let $m > 1$ be an integer and a be any integer coprime to m. Then

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

where $\varphi(m)$ is the Euler-totient function given by

$$\varphi(m) = m \prod_{\substack{p|M \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$$

For instance, let m = 35. Then we have $\varphi(m) = 35\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right) = 24$. Hence for

any a coprime to 35, we have $a^{24} \equiv 1 \pmod{35}$. In particular 3^{24} has a remainder 1 when divided by 35. For our application in RSA, we will be considering m of the form m = pq where p, q are distinct primes. Then $\varphi(m) = \varphi(pq) = (p-1)(q-1)$. We state the RSA Cryptosystem now.

RSA Cryptosystem: Alice creates a public and private key as follow.

1. Choose two large prime numbers p and q and compute n = pq.
2. Keep p and q secret, known only to yourself, but make n public.
3. Choose an integer $1 < e < \varphi(n) = (p-1)(q-1)$ with the property that $(e, \varphi(n)) = 1$.
4. e is called the enciphering key.
5. The pair (n, e) is the Public key and is made known to everyone.
6. Compute the deciphering key d by solving the congruence $ed \equiv 1 \{\text{mod } \varphi(n)\}$ with $1 < d < (p-1)(q-1)$.
7. Deciphering key d must be kept private, known only to Alice

Sending a message to Alice:

1. Bob converts the message into a string of numbers M.
2. Bob uses public key (n, e) of Alice and compute $C \equiv M^e \pmod{n}$. C is the ciphertext.
3. The ciphertext C is transmitted to Alice.
4. Alice uses her private key d to get back the original message M by computing C^d(modulo n).

This works since $ed \equiv 1 \pmod{\varphi(n)}$ implies $ed = 1 + k\varphi(n)$ for some integer k and hence

$$C^d \equiv (M^e)^d = M^{ed} = M^{1+k\varphi(n)} = M^{(M\varphi(n))k} \equiv M \pmod{n}$$

by using Euler's Theorem.

We illustrate this with an example.

An Example:

1. Choose large primes p = 71 and q = 101. Then n = 7171 and φ (n) = 70 100 = 7000.

2. Choose an enciphering key e = 37; Check that (37, 7000) = 1.

3. Compute the deciphering key d by finding a solution to 37d $\equiv$ 1 (modulo 7000). The solution d with 1 < d < 7000 is given by d = 3973 which is the deciphering key d = 3973.

3. (7171, 37) is the Public Key and 3973 is the private key.

Let message M = 117. The Ciphertext is

$$C = 117^{37} \equiv 227 \pmod{7171}.$$

This can be safely transmitted to me. Anyone who intercepts it will have to factor 7171 to decrypt it. Now use the decryption key by raising C to the 3973rd power and taking the result modulo 7171 to find

$$M = 227^{3973} \equiv 117 \pmod{7171}.$$

which is the original message M .

Suggested Project: Square and Multiply algorithm to compute $a^k \pmod{m}$ faster.

1.4 Binary Numbers

Binary numbers are base 2 numbers which are made up of only 0!s and 1!s. For example,

110100

is an example of a binary number. Like the usual numbers which are in base 10, the binary numbers are in base 2. Let us look for an example. Consider the number 123456. We have

$23456 = 2^5(1 + 732) = 2^5 + 2^5 \times 2^2(1 + 182) = 2^5 + 2^7 + 2^7 \times 2(1 + 91)$

$= 2^5 + 2^7 + 2^8 + 2^8(1 + 90) = 2^5 + 2^7 + 2^8 + 2^8 \times 2(1 + 44)$

$= 2^5 + 2^7 + 2^8 + 2^9 + 2^9 \times 2^2(1 + 10) = 2^5 + 2^7 + 2^8 + 2^9 + 2^{11} + 2^{11} \times 2(1 + 4)$

$= 2^5 + 2^7 + 2^8 + 2^9 + 2^{11} + 2^{12} + 2^{12} \times 2^2 = 2^5 + 2^7 + 2^8 + 2^9 + 2^{11} + 2^{12} + 2^{14}$

Writing 23456 as

$0 \times (2^0 + 2 + 2^2 + 2^3 + 2^4) + 2^5 + 0 \times 2^6 + 2^7 + 2^8 + 2^9 + 0 \times 2^{10} + 2^{11} + 2^{12} + 0 \times 2^{13} + 2^{14}$

we get the binary expansion of 23456 as

$23456 = (101101110100000)_2$

The digits are 0 and 1 and they are written starting with the coefficient of highest power of 2 on the right upto the coefficient of 2^0 on the right. The number of 0's on the right of binary expansion gives the exact power of 2 dividing the number. For example 5 is the exact power of 2 dividing 23456, we have five 0's on the right of the binary expansion of 23456.

Again, given a number in binary form as $N = (x_n x_{n-1} \ldots . x_1 x_0)_2$, we get the decimal expansion of N by

$N = x_0 + x_1 2 + \cdots + x_{n-1} 2^{n-1} + x_n{}^{2n}$.

For example, $N = (1010101010)_2$ in decimal notation is given by

$N = 0 + 1 \times 2^1 + 0 \times 2^2 + 1 \times 2^3 + 0 \times 2^4 + 1 \times 2^5 + 0 \times 2^6 + 1 \times 2^7 + 0 \times 2^8 + 1 \times 2^9$

$= 2^1 + 2^3 + 2^5 + 2^7 + 2^9 = 682.$

While writing in decimal notation, we can only sum the powers of 2 for which the corresponding coefficient is 1.

Exercises:

1. Write the following numbers in decimal notation.

   $(1010101100110)_2$, $(101011000110)_2$, $(101111100110)_2$, $(1000000000110)_2$

2. Write the following numbers in decimal notation.

654321, 1000001, 56237801, 2468097531, 963258741

3. Simplify the following and write in decimal notation.

$(1000101111100)_2 + (1100101000100)_2 (11101100100)_2$

4. Simplify the following and write in binary notation.

$(1111000110000)_2 \times 5642371$

1.5 Complex Numbers (Preliminary Idea only)

Complex numbers arise from trying to find square roots of real numbers. It is clear that the equation $x^2 + 1 = 0$ has no solution in real numbers. In other other words, -1 does not have a real square root. To overcome this problem, the concept of real and imaginary components of a numbers are introduced.

Let us denote by i a square root of 1 so that $i^2 = 1$. Then $(i)^2 = i^2 = 1$. The number i, called iota, has the property that

$$i^{4n} = 1, \qquad i^{4n+1} = i, \qquad i^{4n+2} = -1, \qquad i^{4n+3} = -i \qquad \text{for all } n \geq 0.$$

We define the set of Complex Numbers C as follow.

$$C = \{z = a + bi : a, b \in R\}$$

For $z = a + bi \in C$, we say a is the real part of z, denoted by Re(z), and b is the imaginary part of z, denoted by Im(z). For example, $1 + i$ is a Complex number with both real and imaginary parts equal to 1. Writing every real number $r \in R$ as $r = r + oi$, we see that the set of Real numbers is a subset of the set of Complex numbers.

We can view $z = a + bi$ as a polynomial $a + bx$ computed at $x = i$. Using the properties of powers of i, given two complex numbers $z_1 = a_1 + b_1i$ and $z_2 = a_2 + b_2i$, we can define the sum $z_1 + z_2$ and product z_1z_2 as

$$z_1 + z_2 = (a_1 + b_1i) + (a_2 + b_2i) = (a_1 + a_2) + (b_1 + b_2)i$$

and

$$z_1z_2 = (a_1 + b_1i)\,(a_2 + b_2i) = a_1a_2 + a_1b_2i + b_1a_2i + b_1b_2i^2$$

$= a_1a_2 + (a_1b_2 + a_2b_1)i - b_1b_2 = (a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1)i$

For example, $(1 + i) + (2 + 3i) = 3 + 4i$ and $(1 + i)(2 + 3i) = 2 + 3i + 2i + 3i^2 = (2 - 3) + (3 + 2)i = -1 + 5i$

Given a complex number $z = a + bi$, we define the complex conjugate $\bar{z} = a - bi$. This is the complex number whose imaginary part is negative of the imaginary part of z. For example, $2 - 5i = 2 + 5i$. For $\bar{z} = r \in R$, we have $\bar{z} = z = r$ as the $Im(z) = 0$ in that case.

For complex numbers z_1 and z_2, we have

$$\overline{z_1 + z_2} = \bar{z_1} + \bar{z_2} \qquad \text{and} \qquad \overline{z_1 z_2} = \bar{z_1}\,\bar{z_2}$$

Also for $z = a + bi$, we have

$$z\bar{z} = (a + bi)(a - bi) = a^2 + b^2 \geq 0$$

since a, b are reals. Define the absolute value or modulus of $z = a + bi$, denoted by $|z|$, as

$$\sqrt{z\bar{z}} = \sqrt{a^2 + b^2}$$

where we take the non-negative square root $a^2 + b^2$. For example, $|1 + i| = \sqrt{1^2 + 1^2} = \sqrt{2}$.

Following are some properties of the absolute value of complex numbers. Here z, z_1, z_2 are complex numbers.

1. $|z| = |-z| = |\bar{z}| \geq 0$ for all $z \in C$.
2. $|z| = 0$ if and only if $z = 0 = 0 + 0i$.
3. $|z_1z_2| = |z_1|\,|z_2|$ for all $z_1, z_2 \in C$.
4. Triangle inequality: $|z_1 + z_2| \leq |z_1| + |z_2|$ for all $z_1, z_2 \in C$.

For $z = a + bi \neq 0$, we have

$$z^{-1} = \frac{1}{z} = \frac{\bar{z}}{z\bar{z}} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} - \frac{bi}{a^2 + b^2}$$

For example, $(2 + 3i)^{-1} = \frac{2}{13} - \frac{3i}{13}$. For $z_1 - 1, z_2 \in C$ with $z_2 \neq 0$, we have

$$\frac{z_1}{z_2} = z_1 z_2^{-1} = \frac{z_1 \bar{z}_2}{|z_2|^2}$$

As an example, we have

$$\frac{2+3i}{4-5i} = \frac{(2+3i)(4+5i)}{4^2+5^2} = \frac{-7+22i}{41} = \frac{-7}{41} + \frac{22i}{41}$$

Given $z \in C, z \neq 0$, we have

$$\frac{z}{|z|} = \frac{a+bi}{a^2+b^2} = \frac{a}{a^2+b^2} + \frac{bi}{a^2+b^2}$$

Let $0 \leq \theta < 2\pi$ be such that $\sin \theta = \frac{b}{a^2+b^2}$ and $\cos \theta = \frac{a}{a^2+b^2}$. The angle θ is called the argument of z and we have

$$z = |z|(\cos \theta + \sin \theta\, i) = |z| e^{\theta i}$$

which is called the Euler formula for the complex number z. For example,

$$1 + i = \sqrt{2}\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right) = |z|\left(\cos \frac{\pi}{4} + \sin \frac{\pi}{4} i\right) = \sqrt{2} e^{\frac{\pi}{4} i}$$

Exercises:

1. Find the complex conjugates and modulus of the following complex numbers.

   $1 - i$, $10 + 4i$, $(3 + 5i)(4 + 6i)$, $\frac{2+7i}{5+4i}$

2. Compute z, z^2, z^3, z^{-1} for the following z:

   $1-i$, $3 + i$, $4 + 6i$, $\frac{9+2i}{2+9i}$, $1 + \pi i$, $\sqrt{3} + \sqrt{6i}$

1.6 Indices, Logarithm and Antilogarithm

Indices

A power of a number is the product of a certain number of factors, all of which are the same. For example, 5^9 is a power, in which the number 5 is called the base and the number 9 is called the index or exponent. In fact, for any a, we have

$a^1 = a$

$a^2 = a \cdot a$

$a^3 = a \cdot a \cdot a$

.....

$a^n = a \cdot a \cdot a \cdot a \cdot a.....$ n times

for any n. We have $2^4 = 2.2.2.2 = 16$ for example.

Let a and b be real numbers and m and n be integers. The Indices satisfy the following rules:

1. A Zero power is given by $a^0 = 1$ for $a \neq 0$. For example $4^0 = 1$. We note that 0^0 is not defined. It is sometimes called an indeterminant form.

2. For a positive n, the negative power a^{-n} is defined by

$$a^{-n} = \frac{1}{a^n}$$

For example, $a^{-3} = \frac{1}{a^3}$. In particular $2^{-1} = \frac{1}{2}$, $2^{-2} = \frac{1}{2^2} = \frac{1}{4}$, $2^{-3} = \frac{1}{2^3} = \frac{1}{8}$ and so on.

3. A Fractional power, denoted by $a^{\frac{1}{n}} = \sqrt[n]{a}$, is given by

$$\left(\sqrt[n]{a}\right)^n = a$$

For example, $9^{\frac{1}{2}} = \sqrt{9} = 3$ and $8^{\frac{1}{3}} = \sqrt[3]{8} = 2$

All indices satisfy the following laws. Let a and b be real numbers and m and n be rational numbers.

1. To multiply powers with the same base, add the indices.

   $a^m a^n = a^{m+n}$

   For example, $2^3 \cdot 2^2 = 2^5 = 32$

2. To divide powers with the same base, subtract the indices.

   $$\frac{a^m}{a^n} = a^{m-n}$$

   For Example, $\frac{2^3}{2^2} = 2^{3-2} = 2$ and $\frac{2^2}{2^3} = 2^{2-3} = 2^{-1} = \frac{1}{2}$. Note $\frac{a^m}{a^m} = a^{m-m} = a^0 = 1$ for $a \neq 0$

3. To raise a power to a power, multiply the indices.

   $(a^m)^n = a^{mn}$

   For example, $(2^2)^3 = 2^6 = 64$

4. A power of a product is the product of the powers.

   $(ab)^m = a^m b^m$

   For example, $3^2 \cdot 4^2 = (3 \cdot 4)^2 = 12^2 = 144$.

5. A power of a quotient is the quotient of the powers.

   $$\left(\frac{a}{b}\right)^m = \frac{a^m}{b^m} \quad \text{when } b \neq 0$$

   For example, $\frac{6^2}{2^2} = \left(\frac{6}{2}\right)^2 = 3^2 = 9$

Simplify the following by the above rules.

1. $a = x^{\frac{1}{5}} . x^{\frac{4}{5}}$

2. $a = x^2 \div x^{\frac{3}{2}}$

3. $a = \left(x^{\frac{5}{3}}\right)^6$

4. $a = \frac{x^3 y^4}{x^5 y^2}$

1.7 Logarithms

The Logarithm is the inverse image of an index. The logarithm of any positive number to a given base (a positive number not equal to 1) is the index of the power of base which is equal to that number. If N and b ≠ 1 are any two positive real numbers and for some real x, $b^x = N$, then x is called the logarithm of N to the base b. It is written as $\log_b N = x$. That is, if $N = b^x$, then $\log_b N = x$. Since $3^4 = 81$, the value of $\log_3 81 = 4$. Some examples:

1. $\log_{10} 0.01 = -2$ since $10^{-2} = 0.01$
2. $\log_2 \sqrt{2} = \frac{1}{2}$ since $\sqrt{2} = 2^{\frac{1}{2}}$
3. $\log_b b = 1$ since $b^1 = b$ for any $b > 0, b \neq 1$.
4. $\log_b 1 = 0$ since $b^0 = 1$ for any $b > 0, b \neq 1$.

From the definition of logarithms(logs), we obtain the following for $a > 0, b > 0, b \neq 1$.

$$\log_b b^n = n \quad \text{and} \quad b^{\log_b a} = a$$

System of logarithms: There are two systems of logarithms, natural logarithm and common logarithms which are used most often.

1. **Natural Logarithm:** These were discovered by Napier. They are calculated with respect to the base e which is approximately equal to 2.718. We usually denote $\log_e x$ by ln x
2. **Common Logarithms:** Logarithms to the base 10 are known as common logarithms.

Here we list some facts about logarithms:

1. Logs are defined only for positive real numbers.
2. Logs are defined only for positive bases different from 1.

3. In $\log_b a$, neither a nor b is negative but the value of $\log_b a$ can be negative. For example, $\log_{10}0.01 = -2$ since $10^{-2} = 0.01$.

4. Logs of different numbers to the same base are different, i.e. if $a \neq c$, then $\log_b a \neq \log_b c$.

   In other words, if $\log_b a = \log_b c$, then $a = c$.

5. Logs of the same number to different bases have different values i.e. if $a \neq b$, then $\log_a c \neq \log_b c$. In other words, if $\log_a c = \log_b c$, then $a = b$.

Some important properties of logarithms:

1. Logarithm of a Product:

   $$\log_b (MN) = \log_b M + \log_b N$$

   This follows from the property $b^{m+n} = b^m b^n$. As an example, we have $\log_2 (4 \cdot 8) = \log_2 4 + \log_2 8 = 2 + 3 = 5$. If the product has many factors, we just add the individual logarithms:

   $$\log_b(ABCD) = \log_b A + \log_b B + \log_b C + \log_b D$$

2. In particular, we get the Logarithm of a power:

   $$\log_b(a^n) = n \log_b a$$

   Hence for example $\log_2(3^{100}) = 100 \log 2_3$

3. Logarithm of a quotient:

   $$\log_b \left(\frac{M}{N}\right) = \log_b M - \log_b N$$

   This also follows from the property $b^{m-n} = \frac{b^m}{b^n}$. For example

   $$\log_3 \left(\frac{81}{8}\right) = \log_3 81 - \log_3 2^3 = 4 - 3 \log_3 2$$

4. Logarithm in two different bases b_1 and b_2:

   $$\log_{b2} N = (\log_{b1} N)(\log_{b2} b_1)$$

   In particular, when $b_1 = e$ and $b_2 = 10$, we have

$\log_{10} N = (\log_e N)(\log_{10} e) = 0.434 \log_e N$ and $\log_e N = (\log_{10} N)(\log_e 10)$

$= 2.303 \log_{10} N$

Exercises:

1. Expand $\log_b \left(\frac{a^a b^b}{c^c d^d} \right)$

2. Expand $\log_b \left(\frac{4x^6}{9y^7} \right)$

3. Simplify $\log_{10} a + \log_{10} b^2 + \log_{10} c^3$

4. Simplify $\log_a a - \log_b b^2 + \log_c c^3 - \log_d d^4$

Anti-logarithm

The anti-logarithm of a number is the inverse process of finding the logarithms of the same number. If x is the logarithm of a number y with a given base b, then y is the anti-logarithm of (antilog) of x to the base b.

If $\log_b y = x$, then y = antilog of x.

Natural Logarithms and Anti-Logarithms have their base as 2.7183. The Logarithms and Anti-Logarithms with base 10 can be converted into natural Logarithms and Anti-Logarithms by multiplying it by 2.303.

The Zero Index

We have $\frac{9^7}{9^7} = 1$. On the other hand, applying the above index law 2 and ignoring the condition m > n, we have $\frac{9^7}{9^7} = 9^0$. If the index laws are to be applied in this situation, then we need to define 9^0 to be 1. More generally, if $a \neq 0$, then we define $a^0 = 1$. We note that 0^0 is not defined. It is sometimes called an indeterminant form.

The index laws are also valid for the zero index. And for any non-zero a and b, we have

$(7a^3b^2)^0 = 1$

Negative Exponents

Let's look at the decreasing powers of 2. We have

$2^5 = 3^2, 2^4 = 16, 2^3 = 8, 2^2 = 4, 2^1 = 2, 2^0 = 1, 2^{-1} = ?, 2^{-2} = ?$

As we can see, at every step when we decrease the index, the number is halved. Therefore it makes sense to define

$$2^{-1} = \frac{1}{2}$$

Further, continuing the pattern, we define

$$2^{-2} = \frac{1}{4} = \frac{1}{2^2}, 2^{-3} = \frac{1}{8} = \frac{1}{2^3}, \quad \text{and soon}$$

1.8 Laws and Properties of Logarithms

Logarithms are useful in may domains, particularly in solving exponential equations. For example, we use logarithms to measure Richter scale in earthquakes, decibel measures in sound, pH balance in Chemistry and the brightness of stars, to name a few.

Let us look at the example of how logarithms are in used in measuring the magnitude of earthquakes. The energy released by an earthquake gives the magnitude of the earthquake.

The Richter magnitude scale (commonly known as Richter scale) is used to measure this magnitude of an earthquake. Seismographs detect movement in the earth's surface and measures the amplitute of the earthquake wave. Let λ be the measure of the earthquake wave amplitute and λ_0 be the measure of smallest detectable wave (or the standard wave).
Then the Richter Scale is given by the formula

$$R = \log_{10}\left(\frac{\lambda}{\lambda_0}\right)$$

Higher the Richter scale, more is the intensity of the earthquake and damages caused. Usually earthquakes of Richter scale up to 4.9 does not cause damage. The earthquakes of Richter scale 6-6.9 and above cause major damages. The strongest earthquake till date was recorded in Chile in 1960 with Richter Scale of 9.5 which caused severe damage.

Example 1: There was an earthquake with a wave amplitude 2020 times the wave. Calculate the Richter scale with two decimal digits?

Solution: We have $\lambda = 2020\lambda_0$ This gives

$$R = \log_{10}(\frac{\lambda}{\lambda_0}) = \log_{10} 2020 = 3.3.$$

Hence the Richter scale of the earthquake is 3:3.

Example 2: A scientist running an experiment finds that a particular bacterial colony doubles its population every 20 hours. He starts with 200 bacteria cells.

She expects the number of cells to be given by the formula $b = 200(\sqrt{2})^{\frac{t}{20}}$ where t is the number of hours for which the experiment is running. Find the number of hours after which there will be 500 bacteria cells.

Solution: Taking logarithms on both sides of $b = 200(\sqrt{2})^{\frac{t}{20}}$ and putting b = 500, we get

$$\log 500 = \log b = \log 200 + \log(\sqrt{2})^{\frac{t}{20}} = \log 200 + \frac{t}{20}\log\sqrt{2} = \log 200 + \frac{t}{40}\log 2.$$

This gives

$$t = 40 \times \frac{\log 500 - \log 200}{\log 2} = \frac{40\log\frac{500}{200}}{\log 2} = \log\frac{40\log\frac{5}{2}}{\log 2} = 22.964.$$

Therefore after 23 hours, there will be 500 bacteria cells.

Exercises: Let the population of the world in t years after 2010 be given by the formula $P = 4.7(1.02)^t$ billions.

i) Calculate the total population of the world in the year 2029 to the nearest million.

ii) Find the year in which the population will be double of the population of 2020.