INTRODUCTION TO NUMBER THEORY

MATH 151

Maxwell A. Boateng (PhD)

Department of Mathematics, KNUST

February 13, 2021

Natural Number

Natural numbers are $1, 2, 3, \cdots$, also called positive integers, are used in counting members of a set.The symbols varied with the times, e.g., the Romans used I, II, III, IV,$\cdots$
The sum $a + b$ and product $a \cdot b$ or ab of any two natural numbers a and b is also a natural number. This is often expressed by saying that the set of natural numbers is closed under the operations of addition and multiplication, or satisfies the closure property with respect to these operations.

For any natural number a, b, c, we have

- $a + (b + c) = (a + b) + c$
- $a + b = b + a$
- $a(b + c) = ab + ac$
- $a(bc) = (ab)c$ Associativity
- $ab = ba$ Commutativity
- $(a + b)c = ac + bc$ Distributive

Real Numbers

Integers

Negative integers and zero denoted by $-1, -2, -3, \ldots$ and 0, respectively, arose to permit solutions of equations such as $x + b = a$, where a and b are any are any natural numbers. This leads to the operation of subtraction, or inverse of addition, and we write $x = a - b$ The set of positive and negative integers and zero is called the set of integers.
Properties of Integers

- Associativity
- Commutativity
- Distributive
- $a + 0 = a = 0 + a$
- $a.1 = a = 1.a$
- Transitivity: $a > b$ and $b > c \implies a > c$
- Trichotomy: $a > b, a < b$ or $a = b$
- Cancellation law: If $a.c = b.c$ and $c \neq 0$ then $a = b$

Real Numbers

Rational Numbers

Rational numbers or fractions such as $\frac{2}{3}, \frac{-5}{4}, \ldots$ arose to permit solutions of equations such as $bx = a$ for all integers a and b, where $b \neq 0$. This leads to the operation of division, or inverse of multiplication, and we write $x = \frac{a}{b}$ or $a \div b$ where a is the numerator and b the denominator.The set of integers is a subset of the rational numbers, since integers correspond to rational numbers where $b = 1$.

Irrational Numbers

Irrational numbers such $\sqrt{2}$ and π are numbers which are not rational, i.e., they cannot be expressed as a/b (called the quotient of a and b),where a and b are integers and $b \neq 0$.
The set of rational and irrational numbers is called the set of real numbers.

The Principle of Mathematical Induction

The principle of mathematical induction is an important property of the positive integers. It is especially useful in proving statements involving all positive integers when it is known for example that the statements are valid for $n = 1, 2, 3$ but it is suspected or conjectured that they hold for all positive integers. The method of proof consists of the following steps:

1. Prove the statement for $n = 1$ (some other positive integer).
2. Assume the statement true for $n = k$; where k is any positive integer.
3. From the assumption in 2 prove that the statement must be true for $n = k + 1$. This is part of the proof establishing the induction and may be difficult or impossible.
4. Since the statement is true for $n = 1$ [from step 1] it must [from step 3] be true for $n = 1 + 1 = 2$ and from this for $n = 2 + 1 = 3$, and so on, and so must be true for all positive integers. (This assumption, which provides the link for the truth of a statement for a finite number of cases to the truth of that statement for the infinite set, is called The Axiom of Mathematical Induction)

The Principle of Mathematical Induction

Example:

Prove that $1 + 2 + ... + n = \frac{n(n+1)}{2}$

Proof

This formula is easily verified for small numbers such as $n = 1; 2; 3;$ or 4, but it is impossible to verify for all natural numbers on a case-by-case basis. To prove the formula true in general, a more generic method is required. Suppose we have verified the equation for the first k cases. We will attempt to show that we can generate the formula for the $(k + 1)th$ case from this knowledge.

The formula is true for

$n_o = 1$, since $1 = \frac{1(1+1)}{2}$

Proof (con't)

If we have verified the first k cases, then

$$1+2+...+k+(k+1) = \frac{k(k+1)}{2} + k + 1$$

$$= \frac{k^2+3k+2}{2}$$

$$= \frac{(k+1)[(k+1)+1]}{2}$$

This the exactly the formula for the $(k+1)th$ case.

Example 2

Prove that all integers $n \leq 3, 2^n > n+4$

Proof

Since $8 = 2^3 > 3+4 = 7$; the statement is true for $n_o = 3$.

Assume that $2^k > k+4$ for $k \geq 3$

then ,$2^{k+1} = 2 \cdot 2^k > 2(k+4)$

But $2(k+4) = 2k+8 > k+5 = (k+1)+4$

Since k is positive. Hence, by induction, the statement holds for all integers $n \leq 3$

Real Numbers

Definition 1

A non-empty subset S of $\mathbb{Z}$ is well-ordered if S contains a least element.
Notice that the set $\mathbb{Z}$ is not well-ordered since it does not contain a smallest element. However, the natural numbers are well-ordered

Principle of Well Ordering.

Every non-empty subset of the natural numbers is well-ordered.
The Principle of Well-Ordering is equivalent to the Principle of Mathematical Induction.

Theorem 1.

- If $x \in \mathbb{R}$, and $x > 0$, then there is a positive integer n such that

  $nx > y$

- If $x \in \mathbb{R}$, and $x < y$, then there is a $p \in \mathbb{Q}$ such that $x < p < y$
  The first part is usually referred to as the Archimedean property of $\mathbb{R}$.
  Second Part may be stated by saying that $\mathbb{Q}$ is dense in $\mathbb{R}$: Between any two real numbers there is a rational one.

Exercise:

1. Prove that $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$
2. Prove that $2^n < n!$ for $n \geq 4$
3. $1^3 + 2^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$
4. Show that $n^3 + 2n$ is divisible by 3.
5. Prove Bernoulli's inequality $(1 + x)^n > 1 + nx$ for $n = 2, 3, \cdots$ if $x > -1, x \neq 0$

Algebra of Complex Numbers

Although complex numbers occur in many branches of mathematics, they arise most directly out of solving polynomial equations.We examine a specific quadratic equation as an example.

Consider the quadratic equation

$$z^2 = 4z - 5 \tag{1}$$

Equation (1) has two solutions, z_1 and z_2, such that

$$(z - z_1)(z - z_2) = 0 \tag{2}$$

Using the familiar formula for the roots of a quadratic equation,the solutions z_1 and z_2, written in brief as

$$z_{1,2} = \frac{4 \pm \sqrt{(-4)^2 - 4(1 \times 5)}}{2} = 2 \pm \frac{\sqrt{-4}}{2} \tag{3}$$

Algebra of Complex Numbers

Both solutions contain the square root of a negative number. However, it is not true to say that there are no solutions to the quadratic equation. The fundamental theorem of algebra states that a quadratic equation will always have two solutions and these are in fact given by (2).The second term on the R.H.S of (3) is called an imaginary term since it contains the square root of a negative number; the first term is called a real term. The full solution is the sum of a real term and an imaginary term and is called a complex number.The choice of the symbol z for the quadratic variable was not arbitrary; the conventional representation of a complex number is z, where z is the sum of a real part x and i times an imaginary part y, i.e.

$$z = x + iy \tag{4}$$

where i is used to denote the square root of -1. The real part x and the imaginary part y are usually denoted by Rez and Imz respectively. We note at this point that some physical scientists, engineers in particular, use j instead of i. However,for consistency, we will use i this book. In our particular example $\sqrt{-4} = 2\sqrt{-1} = 2i$,and hence the two solutions of (3) are;

Algebra of Complex Numbers

$$z_{1,2} = 2 \pm \frac{2i}{2} = 2 \pm i \tag{5}$$

Thus, here $x = 2$ and $y = \pm 1$ For compactness a complex number is sometimes written in the form

$$z = (x, y)$$

where the components of z may be thought of as coordinates in an xy-plot. Such a plot is called an Argand diagram and is a common representation of complex numbers.

Addition And Subtraction

The addition of two complex numbers z_1 and z_2 ,in general gives another complex number. The real components and the imaginary components are added separately and in a like manner to the familiar addition of real numbers:

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

$$= (x_1 + x_2) + (y_1 + y_2)i, = z_1 + z_2 = (x_1, y_1) = (x_1 + x_2, y_1 + y_2).$$

By straightforward application of the commutativity and associativity of the real and imaginary parts separately, we can show that the addition of complex numbers is itself commutative and associative, i.e

$$z_1 + z_2 = z_2 + z_1$$

$$z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3$$

Thus it is immaterial in what order complex numbers are added.

Example

1. Sum the complex numbers $1+2i, 3-4i, -2+i$
   Summing the real terms we obtain

   $$1+3-2=2$$

   and summing the imaginary terms we obtain

   $$2i-4i+i=-i$$

   Hence
   $1+2i, 3-4i, -2+i = 2-i$
2. $(2+3i)+(3-4i) = 2+3i+3-4i = 5-i$
3. $(2+3i)-(3-4i) = 2+3i-3+4i = -1+7i$
4. $(-4+7i)+(5-10i) = 1-3i$
5. $(4+12i)-(3-15i) = 4+12i-3+15i = 1+27i$
6. $5i-(-9+i) = 5i+9-i = 9+4i$

Algebra of Complex Numbers

Equality

Let $z_1 = x_1 + y_1 i$ and $z_2 = x_2 + y_2 i$ be complex numbers, then:
$z_1 = z_2$ If and only if $x_1 = x_2$ and $y_1 = y_2$

Exercises:

Given $z_1 = 2 + 4i, z_2 = 3 - i$ and $z_3 = -3i$
Determine:

1. $z_1 + z_2$
2. $z_1 - z_2$
3. $z_2 + z_3$
4. $z_2 - z_3$
5. $z_1 + z_3$
6. $z_1 - z_3$

Modulus and Argument:

The modulus of the complex number z is denoted by $|z|$ and is defined as;

$$|z| = \sqrt{x^2 + y^2} \tag{6}$$

Hence the modulus of the complex number is the distance of the corresponding point from the origin in the Argand diagram. The argument of the complex number z is denoted by arg z and is defined as;

$$argz = tan^{-1}\left(\frac{y}{x}\right) \tag{7}$$

It can be seen that arg z is the angle that the line joining the origin to z on the Argand diagram makes with the positive $x-$ axis. The anticlockwise direction is taken to be positive by convention.Account must be taken of the signs of x and y individually in determining in which quadrant arg z lies.Thus, for example, if x and y are both negative then arg z lies in the range $-\pi <$ arg $z < \frac{-\pi}{2}$ rather than in the first quadrant $0 <$ arg $z < \frac{\pi}{2}$, though both cases give the same value for the ratio of y to x.

Examples

a Find the modulus and the argument of the complex number $z = 2 - 3i$. Using (6), the argument is given by

$$|z| = \sqrt{(2)^2 + (-3)^2} = \sqrt{13}$$

Using (7), the argument is given by

$$argz = \theta = tan^{-1}\left(\frac{-3}{2}\right) = -56.31^o$$

Since $x = 2$ and $y = -3, z$ clearly lies in the fourth quadrant;(i.e. the argument must be measured from the positive real axis). therefore, arg $z = 56.31^o$ is the appropriate answer.

Examples

b Determine the modulus and argument of the complex number $z = 3 + 4i$

$$|z| = r = \sqrt{(3)^2 + (4)^2} = 5$$

$$argz = \theta = tan^{-1}\left(\frac{4}{3}\right) = 53.13^o$$

Since $x = 3$ and $y = 4, z$ clearly lies in the first quadrant.

c Determine the modulus and argument of the complex number $z = -3 + 4i$

$$|z| = r = \sqrt{(-3)^2 + (4)^2} = 5$$

$$argz = \theta = tan^{-1}\left(\frac{4}{3}\right) = 53.13^o$$

Since $x = -3$ and $y = 4, z$ clearly lies in the second quadrant;
Argument $= 180 - 126.87$ (i.e. the argument must be measured from the positive real axis)

Example

d Determine the modulus and argument of the complex number$z = -3 - 4i$

$$|z| = r = \sqrt{(-3)^2 + (-4)^2} = 5$$

$$argz = \theta = tan^{-1}\left(\frac{4}{3}\right) = 53.13^o$$

Since $x = -3$ and $y = -4, z$ clearly lies in the third quadrant; Argument $= 180 + 53.13 = 233.13$ (i.e. the argument must be measured from the real axis)

Algebra of Complex Numbers

Multiplication

Complex numbers may be multiplied together and in general give a complex number as the result. The product of two complex numbers z_1 and z_2 is found by multiplying them out in full and remembering that $i_2 = -1$,i.e.

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

$$= x_1 x_2 + x_1 y_2 i + y_1 x_2 i + y_1 y_2 i^2$$

$$= (x_1 x_2 - y_1 y_2) + (x_1 y_2 + y_1 x_2) i$$

Example

a Multiply the complex numbers $z_1 = 3 + 2i$ and $z_2 = -1 - 4i$.
By direct multiplication we fine
$z_1 z_2 = (3 + 2i)(-1 - 4i) = -3 - 2i - 12i - 8i^2 = 5 - 14i$

Example (Con't)

b If $z_1 = 7i$ and $z_2 = -5 + 2i$
Determine $z_1 z_2$.
$7i(-5 + 2i) = -35i + 14(-1) = -14 - 35i$

c If $z_1 = 1 - 5i$ and $z_2 = -9 + 2i$
Determine $z_1 z_2$.
$(1-5i)(-9+2i) = -9+2i+45i-10i^2 = -9+47i-10(-1) = 1+47i$

d Find $(1 - 8i)(1 + 8i)$
$(1 - 8i)(1 + 8i) = 1 + 8i - 8i - 64i^2 = 1 + 64 = 45$
The multiplication of complex numbers is both commutative and associative i.e

$$z_1 z_2 = z_1 z_2 \tag{8}$$

$$(z_1 z_2) z_3 = z_1 (z_2 z_3) \tag{9}$$

Algebra of Complex Numbers

The product of two complex numbers also has the simple properties

$$|z_1 z_2| = |z_1||z_2| \tag{10}$$

$$arg(z_1 z_2) = arg(z_1) + arg(z_2) \tag{11}$$

Example

Verify that (10) holds for the product of $z_1 = 3 + 2i$ and $z_2 = -1 - 4i$.

Solution

$$|z_1 z_2| = |5 - 14i| = \sqrt{5^{+}(-14)^2} = \sqrt{221}$$

We also find

$$|z_1| = \sqrt{3^2 + 2^2} = \sqrt{13}$$
$$|z_1| = \sqrt{(-1)^2 + (-4)^2} = \sqrt{17}$$

and hence

$$|z_1||z_2| = \sqrt{13}\sqrt{17} = \sqrt{221} = |z_1 z_2|$$

Complex Conjugate

If z has the convenient form $x + yi$ then the complex conjugate, denoted by z may be found simply by changing the sign of the imaginary part, i.e. if $4z = x + yi$ then $z = x - yi$. More generally, we may define the complex conjugate of z as the (complex) number having the same magnitude as z that when multiplied by z leaves a real result, i.e. there is no imaginary component in the product. In the case where z can be written in the form $x + yi$ it is easily verified, by direct multiplication of the components, that the product $z\bar{z}$ gives a real result:

$$z\bar{z} = (x + yi)(x - yi)$$

$$= x^2 - xyi + xyi - y^2 i^2$$

$$x^2 + y^2 = |z|^2$$

Example

Find the complex conjugate of $z = a + 2i + 3ib$

Solution

The complex number is written in the standard form

$$z = a + i(2 + 3b)$$

Then, replacing i by $-i$, we obtain

$$\bar{z} = a - i(2 + 3b)$$

In some cases, however, it may not be simple to rearrange the expression for z into the standard form $x + yi$.Nevertheless, given two complex numbers, z_1 and z_2,it is straightforward to show that the complex conjugate of their sum (or difference) is equal to the sum (or difference) of their complex conjugates, i.e.$\overline{(z_1 \pm z_2)} = \bar{z}_1 \pm \bar{z}_1$.Similarly, it can be shown that the the complex conjugate of the product (or quotient) of z_1 and z_2 is equal to the product (or quotient) of their complex conjugate, i.e. $\overline{(z_1 z_2)} = \bar{z}_1 \bar{z}_2$ and $\overline{(z_1/z_2)} = \bar{z}_1/\bar{z}_2$. Using these results, it can be deduced that, no matter how complicated the expression, its complex conjugate may always be found by replacing every i by $-i$. To apply this rule, however, we must always ensure that all complex parts are first written out in full,

Example

Find the complex conjugate of the complex number $z = w^{(3y+2ix)}$ where $w = x+5i$

Solution

In this case w itself contains real and imaginary components and so must be written out in full, i.e.

$$z = w^{(3y+2ix)} = (x + 5i)^{3y+2ix}$$

Now we can replace each i by $-i$ to obtain

$$\bar{z} = (x - 5i)^{3y-2ix}$$

It can be shown that the product zz is real, as required. The following properties of the complex conjugate are easily proved and others may be derived from them.
If $z = x + yi$
then

(a) $\bar{\bar{z}} = z$

(b) $z + \bar{z} = 2Re\, z = 2x$

(c) $z - \bar{z} = 2i\, Im\, z = 2yi$

Example Con't

(d) $\frac{z}{\bar{z}} = \left(\frac{x^2-y^2}{x^2+y^2}\right) + i\left(\frac{2xy}{x^2+y^2}\right)$

Division

The division of two complex numbers z1 and z2 bears some similarity to their multiplication. Writing the quotient in component form we obtain

$$\frac{z_1}{z_2} = \frac{x_1 + y_1 i}{x_2 + y_2 i} \tag{12}$$

In order to separate the real and imaginary components of the quotient, we multiply both numerator and denominator by the complex conjugate of the denominator. By definition, this process will leave the denominator as a real quantity

$$\frac{z_1}{z_2} = \frac{(x_1 + y_1 i)(x_2 - y_2 i)}{(x_2 + y_2 i)(x_2 - y_2 i)} = \frac{(x_1 x_2 + y_1 y_2) + (x_2 y_1 - x_1 y_2)i}{x_2^2 + y_2^2} \tag{13}$$

Division Con't

$$= \frac{x_1x_2 + y_1y_2}{x_2^2 + y_2^2} + \frac{x_2y_1 - x_1x_2}{x_2^2 + y_2^2}\, i \tag{14}$$

Hence we have separated the quotient into real and imaginary components, as required.

Example 1

Express z in the form $x + iy$,when

$$z = \frac{3 - 2i}{-1 + 4i}$$

Solution

Multiplying numerator and denominator by the complex conjugate of the denominator we obtain

$$z = \frac{(3 - 2i)(-1 - 4i)}{(-1 + 4i)(-1 - 4i)} = \frac{-11 - 10i}{17}$$

$$= \frac{-11}{17} - \frac{10i}{17}$$

Division of Complex Numbers

Properties

a $\left|\frac{z_1}{z_2}\right| = \frac{|z_1|}{|z_2|}$

b $\arg\left(\frac{z_1}{z_2}\right) = \arg\ z_1 - \arg\ z_2$

Examples

Write each of the following in standard form

1. $\frac{3-i}{2+7i}$
2. $\frac{3}{9-i}$
3. $\frac{8i}{1+2i}$
4. $\frac{5-9i}{2i}$

Polar Representation of Complex Numbers

Although considering a complex number as the sum of a real and an imaginary part is often useful, sometimes the polar representation proves easier to manipulate.This makes use of the complex exponential function, which is defined by

$$e^z = exp(z) = 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \cdots \tag{15}$$

Strictly speaking it is the function exp(z) that is defined by (15).The number e is the value of exp(1), i.e. it is just a number. However, it may be shown that e^z and exp(z) are equivalent when z is real and rational and mathematicians then define their equivalence for irrational and complex z. For the purposes of this book we will not concern ourselves further with this mathematical nicety but,rather, assume that(15),is valid for all z. We also note that using(15),by multiplying together the appropriate series we may show that

$$e^{z_1} e^{z_2} = e^{z_1 + z_2} \tag{16}$$

which is analogous to the familiar result for exponentials of real numbers. From (15),It immediately follows that for $z = i\theta$, θ real,

Polar Representation of Complex Numbers (Con't)

$$e^{i\theta} = 1 + i\theta - \frac{\theta^2}{2!} - \frac{i\theta^3}{3!} + \cdots \tag{17}$$

$$= 1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} - \cdots + i(\theta - \frac{\theta^3}{3!} + \frac{\theta^5}{5!} - \cdots) \tag{18}$$

and hence that

$$e^{i\theta} = cos(\theta) + isin(\theta) \tag{19}$$

where the last equality follows from the series expansions of the sine and cosine functions.This last relationship is called Eulers equation.
It also follows from (19)

$$e^{in\theta} = \cos(\theta) + i\sin(n\theta) \tag{20}$$

for all n. From Eulers equation (19) we deduce that

$$re^{i\theta} = r(\cos(\theta) + i\sin(\theta)) \tag{21}$$

$$= x + yi \tag{22}$$

Polar Representation of Complex Numbers (Con't)

Thus a complex number may be represented in the polar form

$$z = re^{i\theta} \tag{23}$$

Now we can identify r with $|z|$ and θ with argz. The simplicity of the representation of the modulus and argument is one of the main reasons for using the polar representation. The angle θ lies conventionally in the range $-\pi < \theta \leq \pi$,but, since rotation by θ is the same as rotation by $2n\pi + \theta$, where n is any integer,

$$re^{i\theta} \equiv re^{i(\theta+2n\pi)} \tag{24}$$

The algebra of the polar representation is different from that of the real and imaginary component representation, though, of course, the results are identical.Some operations prove much easier in the polar representation, others much more complicated. The best representation for a particular problem must be determined by the manipulation required.

Multiplication and Division in Polar Form

Multiplication and division in polar form are particularly simple. The product of $z_1 = r_1 e^{i\theta_1}$ and $z_2 = r_2 e^{i\theta_2}$ is given by

$$z_1 z_2 = r_1 e^{i\theta_1} r_2 e^{i\theta_2} \tag{25}$$

$$= r_1 r_2 e^{i(\theta_1+\theta_2)} \tag{26}$$

$$= r_1 r_2[\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2)] \tag{27}$$

The relations $|z_1 z_2| = |z_1||z_2|$ and arg $(z_1 z_2) =$ arg $z_1 +$ arg z_1 follow immediately. Division is equally simple in polar form; the quotient of z_1 and z_2 is given by

$$\frac{z_1}{z_2} = \frac{r_1 e^{i\theta_1}}{r_2 e^{i\theta_2}} = \frac{r_1}{r_2} e^{i(\theta_1-\theta_2)} \tag{28}$$

$$\frac{r_1}{r_2}[\cos(\theta_1 - \theta_2) + i\sin(\theta_1 - \theta_2)] \tag{29}$$

The relations $|z_1 = z_2| = |z_1| = |z_2|$ and arg $(z_1 = z_2) =$ arg $z_1 -$ argz_1 are again immediately apparent

De Moivre's Theorem

We now derive an extremely important theorem. Since $(e^{i\theta})^n = e^{in\theta}$, we have

$$(\cos(\theta) + i\sin(\theta))^n = \cos(n\theta) + i\sin(n\theta) \tag{30}$$

where the identity $e^{in\theta} = \cos(n\theta) + i\sin(n\theta)$ follows from the series definition of $e^{in\theta}$.This result is called de Moivres theorem and is often used in the manipulation of complex numbers. The theorem is valid for all n whether real, imaginary or complex. There are numerous applications of De Moivres theorem but this section examines just three: proofs of trigonometric identities; finding the nth roots of unity; and solving polynomial equations with complex roots.

Trigonometric Identities

The use of de Moivres theorem in finding trigonometric identities is best illustrated by example. We consider the expression ofa multiple-angle function in terms of a polynomial in the single-angle function, and its converse.

Examples

i Express $\sin(3\theta)$ and $\cos(3\theta)$ in therms of powers of $\cos(\theta)$ and $\sin(\theta)$ Using De Moivres theorem,

$$\cos(3\theta) + i\sin(3\theta) = (\cos(\theta) + i\sin(\theta))^3$$

$$= (\cos^3(\theta) - 3\cos(\theta)\sin^2(\theta)) + i(\sin(\theta)\cos^2(\theta) - \sin^3(\theta))$$

We can equate the real and imaginary coefficients separately,i.e.

$$\cos(3\theta) = \cos^3(\theta) - 3\cos(\theta)\sin^2(\theta)$$

$$= 4\cos^3(\theta) - 3\cos(\theta)$$

and

$$\sin(3\theta) = 3\cos(\theta)\sin^2(\theta) - \sin^3(\theta)$$

$$= 3\sin(\theta) - 4\sin^3(\theta)$$

Example (Con't)

This method can clearly be applied to finding power expansions of $\cos(n\theta)$ and $\sin(n\theta)$ for any positive integer n. The converse process uses the following properties of $z = e^{i\theta}$,

$$z^n + \frac{1}{z^n} = 2\cos(n\theta) \tag{31}$$

$$z^n - \frac{1}{z^n} = 2i\sin(n\theta) \tag{32}$$

These qualities follow from simple applications of de Moivres theorem, i.e.

$$\begin{aligned} z^n + \frac{1}{z^n} &= (\cos(\theta) + i\sin(\theta))^n + (\cos(\theta) + i\sin(\theta))^{-n} \\ &= \cos(n\theta) + i\sin(n\theta) + \cos(-n\theta) + i\sin(-n\theta) \\ &= \cos(n\theta) + i\sin(n\theta) + \cos(n\theta) - i\sin(n\theta) = 2\cos(n\theta) \end{aligned}$$

and

$$\begin{aligned} z^n - \frac{1}{z^n} &= (\cos(\theta) + i\sin(\theta))^n - (\cos(\theta) + i\sin(\theta))^{-n} \\ &= \cos(n\theta) + i\sin(n\theta) - \cos(-n\theta) - i\sin(-n\theta) \\ &= \cos(n\theta) + i\sin(n\theta) - \cos(n\theta) + i\sin(n\theta) = 2i\sin(n\theta) \end{aligned}$$

Example (Con't)

In the particular case where $n = 1$,

$$z + \frac{1}{z} = e^{i\theta} + e^{-i\theta} = 2\cos(\theta) \tag{33}$$

$$z - \frac{1}{z} = e^{i\theta} - e^{-i\theta} = 2i\sin(\theta) \tag{34}$$

ii Find an expression for $\cos^3(\theta)$ in terms of $\cos(3\theta)$ and $\cos(\theta)$

$$\begin{aligned}\cos^3(\theta) &= \frac{1}{2^3}(z + \frac{1}{z})^3 \\ &= \frac{1}{8}(z^3 + 3z + \frac{3}{z} + \frac{1}{z^3}) \\ &= \frac{1}{8}(z^3 + \frac{1}{z^3}) + \frac{3}{8}(z + \frac{1}{z})\end{aligned}$$

we find

$$\cos^3(\theta) = \frac{1}{4}\cos(3\theta) + \frac{3}{4}\cos(\theta)$$

Finding the *nth* Roots of Unity

The equation $z^2 = 1$ has the familiar solutions $z \pm 1$.However, now that we have introduced the concept of complex numbers we can solve the general equation $z^n = 1$.Recalling the fundamental theorem of algebra, we know that the equation has n solutions. In order to proceed we rewrite the equation as

$$z^n = e^{2ik\pi} \tag{35}$$

where k is any integer. Now taking the nth root of each side of the equation we find

$$z^n = e^{\frac{2ik\pi}{n}} \tag{36}$$

Hence, the solutions of $z^n = 1$ are

$$z_{1,2,3,\cdots,n} = 1, e^{\frac{2i\pi}{n}}, \cdots, e^{\frac{2i(n-1)\pi}{n}} \tag{37}$$

corresponding to the values $0; 1; 2; \cdots; n-1$ for k. Larger integer values of k do not give new solutions, since the roots already listed are simply cyclically repeated for $k = n, n+1, n+2$, etc.

Examples

i Find the solution to the equation $z^3 = 1$

Solution

By applying the above method we find

$$z = e^{\frac{2ik\pi}{3}}$$

Hence the three solutions are $z_1 = e^{0i} = 1, z_2 = e^{\frac{2i\pi}{3}}, z_3 = e^{\frac{4i\pi}{3}}$. We note that, as expected,the next solution, for which $k = 3$,gives $z_4 = e^{\frac{6i\pi}{3}} = 1 = z_1$, so that there are only three separate solutions. Not surprisingly, given that $|z^3| = |z|^3$ all the roots of unity have unit modulus, i.e. they all lie on a circle in the Argand diagram of unit radius.

Solving Polynomial Equations

A third application of de Moivres theorem is to the solution of polynomial equations. Complex equations in the form of a polynomial relationship must first be solved for z in a similar fashion to the method for finding the roots of real polynomial equations. Then the complex roots of z may be found.

Solving Polynomial Equations

1. Solve the equation $z^6 - z^5 + 4z^4 - 6z^3 + 2z^2 - 8z + 8 = 0$ **Solution**
We first factorize to give

$$(z^3 - 2)(z^2 + 4)(z - 1) = 0$$

Hence $z^3 = 2$ or $z^2 = -4$ or $z = 1$.The solutions to the quadratic equation are $z = \pm 2i$; to find the complex cube roots, we first write the equation in the form

$$z^3 = 2 = 2e^{2ik\pi}$$

where k is any integer. If we now take the cube root, we get

$$z = 2^{1/3} e^{\frac{2ik\pi}{3}}$$

To avoid the duplication of solutions, we use the fact that $-\pi < \arg z \leq \pi$ and find

$$z_1 = 2^{1/3}$$

$$z_2 = 2^{1/3} e^{\frac{2\pi i}{3}} = 2^{1/3} \left(-\frac{1}{2} + \frac{\sqrt{3}}{2} i \right)$$

Solving Polynomial Equations (Con't)

$$z_2 = 2^{1/3} e^{\frac{-2\pi i}{3}} = 2^{1/3}\left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)$$

The complex numbers z_1, z_2, and z_3 together with $z_4 = 2i, z_5 = -2i$ and $z_6 = 1$ are the solutions to the original polynomial equation. As expected from the fundamental theorem of algebra, we find that the total number of complex roots (six, in this case) is equal to the largest power of z in the polynomial. A useful result is that the roots of a polynomial with real coefficients occur in conjugate pairs (i.e. if z_1 is a root, then z_1 unless z_1 is real). This may be proved as follows. Let the polynomial equation of which z is a root be

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

Taking the complex conjugate of this equation,

$$\overline{a_n}(\bar{z})^n + \overline{a_{n-1}}(\bar{z})^{n-1} + \cdots + a_1 z + a_0 = 0$$

But the an are real, and so $\bar{z}$ satisfies

$$a_n(\bar{z})^n + a_{n-1}(\bar{z})^{n-1} + \cdots + a_1 z + a_0 = 0,$$

and is also a root of the original equation.

Complex Logarithm and Complex Powers

The concept of a complex exponential has already been introduced, where it was assumed that the definition of an exponential as a series was valid for complex numbers as well as for real numbers. Similarly we can define the logarithm of a complex number and we can use complex numbers as exponents. Let us denote the natural logarithm of a complex number z by $w = Lnz$, where the notation Ln will be explained shortly. Thus, w must satisfy

$$z = e^w \tag{38}$$

we see that $z_1 z_2 = e^{w_1} e^{w_2} = e^{w_1 + w_2}$, and taking logarithms of both sides we find

$$Ln(z_1 z_2) = w_1 + w_2 = Lnz_1 + Lnz_2 \tag{39}$$

which shows that the familiar rule for the logarithm of the product of two real numbers also holds for complex numbers. We may want to investigate further the properties of lnz. We have already noted that the argument of a complex number is multi-valued, i.e. $\arg z = \theta + 2n\pi$ where n is any integer. Thus, in polar form, the complex number z should strictly be written as

Complex Logarithm and Complex Powers

$$z = re^{i(\theta+2n\pi)}$$

Taking the logarithm of both sides, and using (39), we find

$$Ln(z) = ln(r) + i(\theta + 2n\pi) \tag{40}$$

where $ln(r)$ is the natural logarithm of the real positive quantity r and so is written normally. Thus from (40) we see that lnz is itself multi-valued. To avoid this multi-valued behavior it is conventional to define another function $ln(z)$, the principal value of $ln(z)$, which is obtained from $ln(z)$ by restricting the argument of z to lie in the range $-\pi < \theta \leq \pi$.

a Evaluate $Ln(-i)$
By rewriting i as a complex exponential, we find

$$Ln(-i) = Ln\left[e^{i(-\pi/2+2n\pi)}\right] = i(-\pi/2 + 2n\pi)$$

where n is any integer. Hence $Ln(-i) = \frac{-\pi}{2}, \frac{3i\pi}{2}, \cdots$ We note that $ln(i)$, the principal value of $Ln(i)$,is given by $ln(i) = \frac{\pi}{2}$.