Algebraic Number Theory And Its Application To Rational Theory

Nitish Kumar Bharadwaj[1] & Ajay Kumar[2]

1. Research Scholar, University Department of Mathematics, T. M. Bhagalpur University, Bhagalpur, Email: nitishkrsbr@gmail.com
2. Research Scholar, University Department of Mathematics, T. M. Bhagalpur University, Bhagalpur, Email: Ajkr8407@gmail.com

ABSTRACT

In this paper we recall some nation connected with algebraic number theory and indicate some of its applications in the Gaussian field namely K(i) = √(–1).

A Gaussian rational number is complex number of the form a+bi, where a and b both are rational numbers. The set of all Gaussian rationals forms the Gaussian rational field, denoted by K(i).

Introduction

Numbers have fascinated man from a very early period of human civilization. Pythagoreans studied many properties of natural numbers 1, 2, 3 ..... . The famous theorem of Pythagoras (6^{th} century B.C) through geometrical has a pronounced number theoretic content. The early Babylonians had noted many Pythagorean triads e.g. 3, 4, 5; 5, 12, 13 which are natural number a, b, c satisfying the equation.

$$a^2 + b^2 = c^2 \quad \text{..... (1)}$$

In about 250 A.D Diophantus of Alexandria wrote treatise on polynomial equations which studied solution in fractions. Particular cases of these equations with natural number have been called Diophantine equations to this day.

The study of algebra developed over centuries. The Hindu mathematicians deals with and introduced the nation of negative numbers and zero.

In the 16^{th} century and owned negative and imaginary numbers were used with increasing confidence and flexibility.

Meanwhile the study of the theory of natural numbers went on side by side. It was known that all the Pythagorean triads i.e., the solution of (1) in natural number *a, b, c* is given by the formula $a = m^2 – n^2$, $b = 2mn$, $c = m^2 + n^2$

Where *m, n* are relatively prime positive integers of opposite quantity with $m > n$. The remarkable French mathematician P. Fermat (1601 – 1665) asserted (without proof) in strong contradiction to the case of Pythagorean triads, that the equation.

$$x^2 + y^2 = z^2 \quad \text{.....(2)}$$

In natural numbers if n is an integer ≥ 3. This is called the Fermat's theorem. A complete proof of it was given in 1994 by Andrew wiles (Princeton University) although it was attempted by Euler, Legendre Gauss, Abel, Dirichlet, Cauchy, kummer, etc, in the intervening period of over 350 years that Fermat has enunciated this theorem in about 1847 the German mathematician kummer tried to device his own proof of the Fermat's last theorem. As a result there grace the subject called algebraic number theory which is today a flourishing and important branch of mathematics.

(2′) Algebraic number theory: We give a brief resume of the algebraic number theory: (on detail see [1]).

An algebraic number a is any root of an algebraic equation

$$A_0x^n + a_1x^{n-1} + \ldots\ldots\ldots + a^n = 0$$

Were *a'*s are rational (i.e., ordinary) integers, not all zero.

If a satisfies an algebraic equation of degree n, but none of lower degree, we say that a is of degree n, if in particular $a_0 = 1$, we say that a is an algebraic integer.

An algebraic field is the aggregate of all numbers, $R(\alpha) = P(\alpha) / Q(\alpha)$

Where α is a given algebraic number, $P(\alpha)$ and $Q(\alpha)$ are polynomial in a with rational coefficients and $Q(\alpha) \neq 0$. We denote this field by $k(\alpha)$.

If $n = 1$, then α is rational and $k(\alpha)$ is the aggregate of all rationals. Hence for every rational a, $k(\alpha)$ denotes same aggregate which is called the field of rationals and is denoted by $k(1)$. This field is subfield of every field.

If $n = 2$ we say that a is quadratic. Then a is a root of a quadratic equation $a_0x^2 + a_1x + a_2 = 0$ and so $\alpha = \left[a + b\sqrt{m}\right]/c$ or $\sqrt{m} = \left[c\alpha - a\right]/b$ for some rational integers a, b, c, m. Without loss of generality we may suppose that m is square free. It is then easily verified that $k(\alpha)$ is the same aggregate as $k(\sqrt{m})$. Hence it is enough to consider the quadratic field $k(\sqrt{m})$ for every square free rational integer m, positive or negative, but not 1.

The two simplest classes of algebraic integers are thus

(a) The rational (ordinary) integers..., $-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5$, ... of the field of all rational $K(1)$. The unities of $K(1)$ are $\in = \pm 1$, i.e., the divisors of 1. The two numbers $\in m$ are called associates, the prime in $K(1)$ and the fundamental theorem of $K(1)$, as defined in rational theory, are well known and we do not repeat here.

(b) The complete or Gaussian integers are the numbers $\alpha = a + ib$, where a and b are rational integers. Since

$$a^2 - 2a\alpha + a^2 + b^2 = 0$$

a Gaussian integers is a quadratic integer. We call the Gaussian integers a integers of $K(i)$. Where $i = \sqrt{(-1)}$. In particular, any rational integer a is a Gaussian integer (since $\alpha = a + 1.0$). It is easily verified that the product of two Gaussian integers is a Gaussian integer.

(3′) Properties of the Gaussian Integers: From now onward, the word integer will mean Gaussian integer or integer of the set $K(i)$. We designate the element of the set by Greek letters. We state some properties of Gaussian integer which are remarkably similar to that already developed for rational theory.

(1) Divisibility and divisor: These terms is $K(i)$ are defined in the same way as in $K(i)$, i.e., a Gaussian integer a is said to divide a Gaussian integer 13 if there exists a Gaussian integer γ such that $\beta = \alpha\gamma$. We write this α / β. Since $1, -1, i, -i$ are all integer of $K(i)$, any α of $K(i)$ has the eight trivial divisor, namely $1, \alpha, -1, -\alpha, i, ia, -ia$.

(2) Unity: The integer $\in$ is said to be a unity of $K(i)$ if $\in/\alpha$ ($\in$ divides α) for every a of $K(i)$. Since $\in / \alpha$ and $1/\alpha$, implies $\in/\alpha$, we may also defined a unity as any integer which is a divisor of 1.

(3) Norm: The norm of any integer $\alpha = \underline{a} + \underline{ib}$ of $\underline{K}(\underline{i})$ is defined by

$$N(\alpha) = N(a + \underline{ib}) = \underline{a}^2 + \underline{b}^2$$

If $\alpha = a - ib$ is the conjugate of α, then

$$N(\alpha) = \alpha\ \alpha = |\alpha|^2$$

It is easily seen that the norm of a unity is 1 and any integers whose norm is 1 is a unity.

(4) The unities of $K(i)$ are the solution of $N(a + ib) = a^2 + b^2 = 1$; namely, $a = \pm 1, b = a, a = 0, b = \pm 1$, so that the unities of $K(i)$ are $\pm 1, \pm i$. It $\in$ is any unity then $\in \alpha$ is said to be an associate of α and so all the associates of α are $\alpha, i\alpha, -\alpha, -i\alpha$. In particular the associate of I are the unities.

(5) G.C.D: If α and β are Gaussian integers, not both zero then there exists a Gaussian integer δ such that $\delta/\alpha, \delta/\beta$ and if δ is any integer such that $\delta\backslash\alpha, \delta\backslash\beta$ and $\delta\backslash\delta$, the δ is called a G.C.D a and β and write $(\alpha, \beta) = \delta$. If $\delta = 1$, we say that α and β are relatively prime.

(6) **Prime:** A prime π is *K(i)* is an integer, not zero or a unity, divisible only by numbers associated with itself or with *1*. Thus a prime *n* has no divisors except the following eight trivial ones, namely $1, \pi, -1, -\pi, i, i\pi, -i, -i\pi$. The associates of a prime are clearly primes.

(7) **The fundamental theorem for *K(i)*:** The expression of an integer with norm > *1*, as a brodieas of prime is unique, except for the order of the prime and the presence of unities.

Simple field: A field in which the fundamental theorem is true is called a simple field.

(4′) **Euclidean field:** A quadratic field $K(\sqrt{m})$ is said to be Euclidean if its ring of integers *R* has the property that for any elements γ, δ of *R* such that $\alpha = \beta\gamma + \delta$ with $|N(\delta)| < |N(\beta)|$

For such field there exists a Euclidean algorithm analogous to that in the rational field. It is known [2] that there are precisely *21* Euclidean fields $K(\sqrt{m})$ given by $m = -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 19, 21, 29, 33, 37, 41, 57, 73$.

A Euclidean field has unique factorization property. Between $-7 \le m \le 7$, only in two non.

Euclidean fields, namely, K($\sqrt{-5}$) and K($\sqrt{-6}$) the integer do not have unique factorization property since $21 = 3.7 = \left(1+2\sqrt{-5}\right)\left(1-2\sqrt{(-5)}\right)$

Where all the four factors are prime in $K\sqrt{-5}$ and $6 = 2.3 = \left(\sqrt{-6}\right)\left(\sqrt{-6}\right)$,

Where all the four factors are prime in $K\sqrt{-6}$.

The field K$\sqrt{-10}$ has no unique factorization property since $6 = 2.3 = \left(4+\sqrt{10}\right)\left(4-\sqrt{10}\right)$ where the four factors are all primes in K($\sqrt{10}$).

(5′) **Some applications in K(i):** (1) Integer solution of the equation

$$X^2 + y^2 = zn, n^2, (x, y) = h, z > 0 \qquad \text{.....(1)}$$

Here $(x + iy)(x - iy) = z^n$

If $d = (x + iy, x - iy)$, then $d / (2x, 2y)$ and since $(x, y) = 1$, so $d / 2$. Thus $d = 1, 1 + I, 2$. If $d = 2$, then $4 / (x + iy)(x - iy)$ *i.e.*, $4 / (x^2 + y^2)$, which is impossible, since $(x, y) = 1$. If $d = 1 + i$, then

$$(x + iy) /1 + i - (x + iy)(1 - i) / (1 + i)(1 - 0) = x + y + i(-x + y) / 2$$

is an integer in $Z(i)$, i.e., a Gaussian integer. Hence $x \equiv y \pmod 2$ and since $(x, y) = 1$, we must have x, y both odd and then $z^n \equiv 2 \pmod 4$ which is impossible, hence $d = 1$ and so $(x + iy) = (a + ib)^n$

Where a, b are rational integer and $r = 0, 1, 2, 3$.

$x - iy = (-i)\, r\, (a - ib)^n$ $\qquad$ $x - iy = (-1)(a - ib)^n$

Then $(x + iy)(x - iy) = (-1)r \,.\, i^{2r}\, (a^2b^2)n = z^n$, we have $z = a^2 + b^2$.

As a special case we obtain solution of $x^2 + y^2 = z^2$.

Thus when $n = 2$. We have, since $(x, y) = a$, x and y are of opposite parity, z odd. Hence

$$x + iy = \pm(a + ib)^2 \text{ or } \pm 1(a + ib)^2$$

Equating the real and imaginary parts and taking x odd, y even and $a > b$ as a, b of opposite parity $(a, b) = 1$, we get positive integral solution as $x = a^2 - b^2$, $y = 2ab$, $z = m^2 + n^2$.

(2) There is no Pythagorean triangle whose area is a square.

Proof: Supposed that $x^2 + y^2 = z^2$ is a Pythagorean triangle whose area is a square. We may suppose that in the given triangle $(x, y) = 1$, $x > o$. Then from the solution of the triangle with x odd, y even

$$X = m^2 - n^2,\ y = 2mn,\ z = m^2 + n^2$$

Where m, n are relatively prime positive integers of opposite parity with $m > n$. We may suppose that m is odd and n is even.. now the area of the triangles is

$$\tfrac{1}{2}\, xy = mn(m^2 - n^2)$$

Suppose that $mn(m^2 - n^2) = t^2$

Then since $m, n, m^2 - n^2$ are prime to each other, so $m = a^2$, $n = b^2$, $m^2 - n^2 = c^2$ and

so $a^4 - b^4 = c^2$ .....(1)

Where a is odd and b even, $(a, b) = 1$, and so c is odd.

Now $a^4 = c^2 + b^4 = (c + ib^2)(c - ib^2)$

Since unique factorization holds in $K(i)$, $c + ib$ is associated with a fourth power.

Hence

Case 1. Either $(c + ib^2) = \pm i(d + ie)^4$ .....(1a)

Case 2. $(c + ib^2) = \pm i(d + ie)^4$

In case 1, $b^2 = \pm 4de(d^2 - e^2)$, $\pm c = d^4 - 6d^2e^2 + e^4$

It suffices to consider the upper sign in the expression for b^2, since d, e, d^2e^2 are prime to each other, so each of them is a perfect square.

References

[1] Artin, E. (1956): Theory of algebraic numbers, Gottigen.

[2] Baker, A. : A concise introduction to the theory of numbers, Cambridge university press, Cambridge (London).

[3] Hardy, G.H. and Wright, E. M. (1960): Introduction to the theorem of numbers, Oxford, at the Clarendon Press.

[4] Stewart and Tall, D. (1979): Algebraic number theory, Chapman and Hall. London.

[5] Uspensky, J. V. And Heasiet, M. A. (1939): Elementary number theory, Macmillan Book company, Inc. New York and London.

****