Complex Prime Numbers

T. Muthukumar
tmk@iitk.ac.in

31 May 2014

We say a complex number $a + ib$ is *complex integer* or *Gaussian integer* if both $a, b \in \mathbb{Z}$, the set of real integers. The set of all Gaussian integers is denoted by $\mathbb{Z}[i]$. Intuitively, the notation means adjoining $i = \sqrt{-1}$ to real integers. What are complex prime numbers?

Recall that a real integer p is prime if $p > 1$ and is divisible only by 1 and p (itself). Let us extend the definition of primes to complex numbers. Suppose we define a Gaussian integer $z \in \mathbb{Z}[i]$ to be a complex prime if $|z| > 1$ and is divisible only by 1 and z (itself). Note that, with such a definition, no Gaussian integer can be a complex prime.

1. Note that i is a factor of 1 in $\mathbb{Z}[i]$ and hence will divide all Gaussian integer $a + ib$. This motivates the definition of *unit*. An *unit* is a Gaussian integer which is a factor of 1 in $\mathbb{Z}[i]$. There are exactly four units in $\mathbb{Z}[i]$, viz., $1, -1 = i^2, i, -i = i^3$. This is an outcome of the fact that, in real integers, there are exactly two units, viz., 1 and -1. It can also be shown that units are, precisely, those elements whose modulus is exactly 1.

2. Even if units are included as factors in the definition of complex prime, we still notice that no Gaussian integer can be a complex prime. This is because if z is a Gaussian integer such that $|z| > 1$ then all its multiples by units, viz., $-z, iz$ and $-iz$ are all factors of z. This motivates the definition of *associate*. An *associate* of a Gaussian integer is a multiple of the units in $\mathbb{Z}[i]$.

Definition 1. *A* complex prime *or* Gaussian prime *is a Gaussian integer z such that $|z| > 1$ and is divisible only by its units and associates in $\mathbb{Z}[i]$.*

A simple observation from the definition is that if a Gaussian integer is a Gaussian prime then all of its associates are also Gaussian prime. Further, the conjugate $\bar{z}$ of a Gaussian prime z is also a Gaussian prime because if w is a factor of $\bar{z}$ then $\bar{w}$ is a factor of z.

We define the map $N : \mathbb{Z}[i] \to \mathbb{N} \cup \{0\}$ as $N(z) = a^2 + b^2$ where $z = a + ib$. Note the following properties of N:

1. $N(z) = N(\bar{z})$.
2. $N(z) = z\bar{z}$.
3. $N(zw) = zwz\bar{w} = z\bar{z}w\bar{w} = N(z)N(w)$. The map N is multiplicative.

If w divides z in $\mathbb{Z}[i]$, then $N(w)$ divides $N(z)$ in $\mathbb{N}$ because $z = ww_1$, for some $w_1 \in \mathbb{Z}[i]$, and $N(z) = N(w)N(w_1)$.

Let $z := a + ib$ be a Gaussian integer such that either $a = 0$ or $b = 0$ and the non-zero, say a, satisfies $a^2 > 1$, i.e., $z = a$ or $z = ia$. Without loss of generality, we shall assume $a > 1$. When is z prime? Equivalently, what are the positive real integers which are Gaussian prime? Obviously, every positive real composite is not a Gaussian prime. Therefore, the question reduces to asking if every real prime is a Gaussian prime. A real prime p can fail to be a Gaussian prime only if there is a non-zero, non-real Gaussian integer w that divides p, i.e., $p = N(w)$. Thus, a real prime fails to be a Gaussian prime only if it is sum of two squares. For instance, the first real prime $2 = 1^2 + 1^2$ is not a Gaussian prime because $2 = (1 + i)(1 - i)$.

Is every odd prime expressible as sum of squares of integers? For instance, 3 is not expressible as sum of squares of two integers. Therefore, 3 is a Gaussian prime. What are the odd primes which can be expressed as sum of two squares? Observe that any odd prime is either 1 modulo 4 or 3 modulo 4.

Theorem 1 (Fermats theorem on sums of two square)**.** *An odd prime p is uniquely expressible as $p = a^2 + b^2$, for some $a, b \in \mathbb{N}$, iff $p \equiv 1 (\mathrm{mod}\ 4)$.*

Proof. Let us suppose $p = a^2 + b^2$, for some $a, b \in \mathbb{N}$. p being odd is either 1 modulo 4 or 3 modulo 4. Any perfect square is either 0 modulo 4 or 1 modulo 4. Thus $a^2 + b^2$ is either 0, 1 or 2 modulo 4. Therefore p is 1 modulo 4. The converse part of the proof is quite involved, so we skip it. □

Therefore, we conclude that any odd prime that is 3 modulo 4 is a Gaussian prime. For example, $3, 7, 11, 19, \ldots$ are all Gaussian primes. Alternately, any odd prime that is 1 modulo 4 is not a Gaussian prime. For example, $2, 5, 13, 17, 29, \ldots$ are all not Gaussian primes. So, what are the complex primes other than these real primes?

Theorem 2. *A Gaussian integer z with $|z| > 1$ and non-zero real and imaginary parts is a Gaussian prime iff $N(z)$ is a prime in $\mathbb{N}$.*

Proof. Let z be a Gaussian prime. Then $\bar{z}$ is also a Gaussian prime. If $N(z)$ is not a prime in $\mathbb{N}$ then it has a positive divisor $1 < d < N(z)$ which also divides either z or $\bar{z}$ because $N(z) = z\bar{z}$ contradicting the Gaussian primality of z. Conversely, let $N(z)$ be a prime in $\mathbb{N}$. Suppose z is not a Gaussian prime. Then it has non-trivial factors v and w and, hence, $\bar{v}$ and $\bar{w}$ are non-trivial factors of $\bar{z}$. Thus, $z\bar{z}$ and $w\bar{w}$ are non-trivial real factors of $N(z)$, a contradiction. □

Now that we have understood complex primes, we ask: is any Gaussian integer decomposable as product of Gaussian primes? In other words, we seek the analogues of the prime factorization theorem and the fundamental theorem of arithmetic for positive real integers.

Theorem 3 (Prime Factorization Theorem)**.** *Any number $n \in \mathbb{N}$ such that $n > 1$ is either prime or can be decomposed as a product of prime numbers.*

The decomposition in to product of primes is unique and is called the *fundamental result of arithmetic*.

Do we have similar results for Gaussian integers? The answer is in affirmative, as long as, we bear in mind that unique factorisation is uniqueness up to multiplication with units $1, i, i^2, i^3$. The unique prime factorization is obvious for Gaussian integers on real and imaginary line. For instance, any real non-prime positive integer has the unique factorisation $n = p_1^{a_1} \ldots p_k^{a_k}$. If any of the real prime p_is are not Gaussian prime then they have a Gaussian prime decomposition as discussed above and this factorization is unique up to multiplication by units. For negative integers $-n$ with $n > 0$, the factorization is the unit -1 multiplied with the factorization of n. For in with $n \in \mathbb{Z}$ it is still a multiple of the unit i or $-i$. The unique factorisation can also be shown for any Gaussian integer. Therefore, we have the general result:

Theorem 4 (Unique Factorization Theorem)**.** *Any Gaussian integer z with $N(z) > 1$ can be decomposed as a product of Gaussian primes and the decomposition is unique up to associated Gaussian primes.*

The discussion in this article are protoypes of algebraic entites like rings, prime ideals, unique factorization domains, class number etc. Class number 1 corresponds to unique factorization property (UFP). $\mathbb{Z}[i]$ is also related to Pythagorean triples. Similar to $\mathbb{Z}[i]$, one may consider other quadratic ring $\mathbb{Z}[\sqrt{m}]$, for $m \in \mathbb{Z}$. Note that $m = 0$ corresponds to $\mathbb{Z}$ and $m = -1$ corresponds to $\mathbb{Z}[i]$. The quadratic rings $\mathbb{Z}[\sqrt{m}]$ are useful in the study of Pell's equation

$$x^2 - my^2 = 1.$$

The solution to Pell's equation are the unit norm elements od $\mathbb{Z}[\sqrt{m}]$. For $m > 0$, $\mathbb{Z}[\sqrt{m}] \subset \mathbb{R}$ and, for $m < 0$, $\mathbb{Z}[\sqrt{m}] \subset \mathbb{C}$ We know, for both $m = 0$ and $m = -1$ the corresponding ring of integers satisfies UFP. Thus, one is tempted to conjecture that $\mathbb{Z}[\sqrt{m}]$ satisfies the UFP, for all $m \in \mathbb{Z}$. But the answer is in negation. For instance, $\mathbb{Z}[\sqrt{-5}]$ do not satisfy UFP. The number $6 \in \mathbb{Z}[\sqrt{-5}]$ has two different prime decomposition, viz., $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Check that each of the four factors is a prime in $\mathbb{Z}[\sqrt{-5}]$. In fact, it has been shown that there are exactly nine negative integers, viz., $-1, -2, -3, -7, -11, -19, -43, -67, -163$ for which the UFP holds true. These are called *Heegner numbers*. It is an open problem whether there are finite number of positive integers for which UFP is true in $\mathbb{Z}[\sqrt{m}]$.