Int. J. Contemp. Math. Sci., Vol. 1, 2006, no. 8, 397 - 405

PRIMES IN $\mathbf{Z}\left[e^{\frac{2\pi i}{3}}\right]$

Dilek NAMLI

Balıkesir Üniversitesi
Fen-Edebiyat Fakültesi, Matematik Bölümü
10100 Balıkesir, Turkey
dnamli@balikesir.edu.tr

Abstract

In this work, the primes in the ring Z[ω], where $\omega = e^{\frac{2\pi i}{3}}$ is a cubic root of unity, are classified, and some results related to the use of them in the calculation of cubic residues are obtained. Some of the results appearing in literature in an uncomplete way are completed.

Mathematics Subject Classification: 11A41, 11A15

Keywords: Rational prime, complex prime, primary prime, secondary prime, cubic root of unity

1. Introduction

Let $\omega = (-1+\sqrt{-3})/2$ be a cubic root of unity. Consider the ring $Z[\omega] = \{a+b\omega : a,b \in \mathbb{Z}\}$. The elements $\alpha = a+b\omega$ are called Eisenstein integers as this ring had been used by Eisenstein in the study of cubic reciprocity law. We denote the ring $Z[\omega]$ by D for the ease of notation.

Definition 1.1. *If $\alpha = a+b\omega \in D$, then the norm of α is denoted by $N\alpha$ and defined as $N\alpha = \alpha\bar{\alpha}$.*

Theorem 1.1. *If $\alpha = a+b\omega \in D$, then the norm of α is*

$$N\alpha = a^2 - ab + b^2.$$

Proof. As $\omega\bar{\omega} = |\omega|^2 = 1$ and $\omega + \bar{\omega} = 2\,\mathrm{Re}(\omega) = -1$, the proof follows by the definition of the norm. ∎

$N\alpha$ is, by the definition, a positive integer.
We now find all the units in D.

Theorem 1.2. *The necessary and sufficient condition for an element α of D to be a unit is $N\alpha = 1$. The units in D are $\mu 1$, $\mu\omega$ and $\mu\omega^2$.*

Proof. If $\alpha \in D$ is so that $N\alpha = 1$, then $\alpha\bar{\alpha} = 1$.As $\bar{\alpha} \in D$ α is a unit.

Now if $\alpha \in D$ is a unit, then there is a $\beta \in D$ so that $\alpha\beta = 1$. Than $N(\alpha\beta) = 1$ giving

$$N(\alpha)N(\beta) = N\alpha.N\beta = 1$$

and considering that $N(\alpha)$ and $N(\beta)$ are positive integers, we conclude that $N(\alpha) = 1$ Let now $\alpha = a + b\omega$ be a unit. Then $N(\alpha) = 1$ and equivalently

$$a^2 - ab + b^2 = 1$$

Multiplying both sides by 4, we get

$$(2a - b)^2 + 3b^2 = 4$$

There are two cases to consider.
i) $(2a - b) = \mu 1$ and $b = \mu 1$,
ii) $(2a - b) = \mu 2$ and $b = 0$.
In the first case we have the following possibilities.
(a)If and $2a - b = 1$and $b = 1$,then $a = 1$ and $\alpha = 1 + \omega$
(b)If and $2a - b = 1$and $b = -1$,then $a = 0$ and $\alpha = -\omega$
(c)If and $2a - b = -1$and $b = 1$,then $a = 0$ and $\alpha = \omega$
(d)If and $2a - b = -1$and $b = -1$,then $a = -1$ and $\alpha = -1 - \omega$
As ω satisfies

$$\omega^2 = -1 - \omega$$

$\alpha = -\omega^2$ in a) and $\alpha = \omega^2$ in d).

Now consider ii). $(2a - b) = 2$ and $b = 0$ then $a = 1$ and $\alpha = 1$. If $(2a - b) = -2$ and $b = 0$, then $a = -1$ and $\alpha = -1$. ∎

Definition 1.2. *Two elements α and β are called associates if $\alpha = \beta u$ where $u \in D$ is a unit. If α and β are associates, this situation is denoted by $\alpha \sim \beta$.*

Definition 1.3. *If a number $\pi = a + b\omega \in D$ can not be stated as the product of two non-unit elements $c + d\omega$, $e + f\omega$ in D then π is called a complex prime.*

We call ordinary primes in $\mathbb{Z}$ rational primes.

Theorem 1.3. *Let $p \equiv 1(3)$ be a prime. Then $\omega = \frac{-1+\sqrt{-3}}{2}$ is an element of $\mathbb{Z}_p$.*

Proof. First we show that $\sqrt{-3} \in \mathbb{Z}_p$. . For this we need show the existence of a positive number k such that $-3 \equiv k^2(p)$. Equivalently we need show that $\left(\frac{-3}{p}\right) = \pm 1$. Here $\left(\frac{\cdot}{\cdot}\right)$ denotes the Legendre symbol.

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$$

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}\frac{3-1}{2}}$$

$$\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}$$

$$\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)$$

Here as $p > 2$ is prime, p-1 is even and also as $p \equiv 1(3)$ $\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = +1$.

Hence $\left(\frac{-3}{p}\right) = 1$.

Secondly, we know that $(2, p) = 1$ and therefore, in this case, 2 has a multiplicative inverse t in mod p. Then, as $\sqrt{-3} \in \mathbb{Z}_p$, $-1 + \sqrt{-3} \in \mathbb{Z}_p$ and therefore $\frac{1}{2}(-1 + \sqrt{-3}) = t(1 + \sqrt{-3})(p)$. ∎

Corollary 1.4. *If $p \equiv 1(3)$ then $\omega^2 \in \mathbb{Z}$.*

Example 1.1. *For $p = 7$, $\omega = \frac{(-1+\sqrt{-3})}{2} \equiv \frac{-1+\sqrt{4}}{2} = \frac{1}{2} \equiv \frac{8}{2} \equiv 4$ (7) . As $\omega^2 = -1 - \omega$, we find $\omega^2 \equiv -5 \equiv 2$ (7). That is ω and ω^2 are in $\mathbb{Z}_7$.*

If $p = 3$, similarly $\omega \equiv 9$ (13) and $\omega^2 \equiv 3$ (13) are elements of $\mathbb{Z}_{13}$.

Remark 1.1. *If p is a prime not congruent to 1 modulo 3, then ω and ω^2 can't be elements of $\mathbb{Z}_p$. Because $-3 + 5k$ ends, with 2 or 7 and no square number ends with 2 or 7.*

In fact there is no complex prime congruent to 2 modulo 3 as we shall soon show.

2. **Primes in D**

In this section we classify all primes in D.

Theorem 2.1. *If p is rational $Np = p^2$.*

Proof. Obvious from the definition of norm. ∎

Theorem 2.2. *If a rational prime p is not prime in D, then it has exactly two non-unitfactors, each having norm p.*

Proof. Let p be a rational prime and be a non-prime in D. Then it has at least two factors. Let us call these $a_1, a_2, ..., a_n$. Then

$$Np = Na_1.Na_2...Na_n$$

And as $Np = p^2$ by Theorem 2.1, we find,

$$p^2 = Na_1.Na_2...Na_n$$

This means that just one of the numbers on the right hand side is p^2 and the others are 1. In the first case, as there is only one factor with norm different from 1 (that is non-unit), p must be prime in D, giving a contradiction. Therefore there must be two factors, each with norm p. ∎

Theorem 2.3. *If $p \equiv 1(3)$ is a rational prime, then p can not be prime in D.*

Proof. As p is a prime congruent to 1 modulo 3, we can take $p \equiv 1(6)$. But we know that every rational prime number with this property can be written in the for $p = a^2 - ab + b^2$, for $a, b \in \mathbb{Z}$. Therefore we can write

$$p = a^2 - ab + b^2$$

$$p = a^2 - ab + b^2(-\omega + \omega + 1)$$

$$p = a^2 - ab - \omega b^2 + \omega b^2 + b^2$$

$$p = a^2 - ab - \omega b^2 + b^2(1 + \omega)$$

$$p = a^2 - ab - \omega b^2 - b^2\omega^2$$

$$p = a^2 - ab - \omega b^2 - b^2\omega^2 + ab\omega - ab\omega$$

$$p = (a + b\omega).(a - b - b\omega).$$

f we write $c = a - b$ and $d = -b$, then

$$p = (a + b\omega).(c + d\omega).$$

Then

$$N(a + b\omega).N(c + d\omega) = a^2 - ab + b^2 = p.$$

Therefore $a + b\omega$ and $c + d\omega$ are non-units, giving that p is not a prime in D. ∎

Finally if $p = 3$, then as

$$3 = (2 + \omega)(1 - \omega)$$

3 is not prime in D. As a result of all this we have the following.

Theorem 2.4. *Let p be a rational prime. Then p is prime in D iff $p \equiv 2(3)$.*

Proof. Let the rational prime p be prime in D as well and p be not congruent to 2 modulo 3. Then either $p \equiv 1(3)$ or $p = 3$. In both cases we know that p is not prime in D. This contradicts with primality of p in D .Therefore $p \equiv 2(3)$.

Let now $p \equiv 2(3)$. Then $p \equiv 2, 5(6)$. In the contrary, we assume that p is not prime in D. Then there are two non-unit elements

$$a + b\omega, c + d\omega$$

in D such that

$$p = (a + b\omega)(c + d\omega)$$

.

Then as

$$p^2 = Np = N(a + b\omega).N(c + d\omega)$$

we find

$$N(a + b\omega) = N(c + d\omega) = p.$$

That means that

$$a^2 - ab + b^2 = c^2 - cd + d^2 = p.$$

But p is prime and all primes that can be stated in the form $a^2 - ab + b^2$ are congruent to 1 modulo 6, this contradicts with $p \equiv 2(3)$. Therefore p is prime in D. ∎

This concludes the study of rational primes in D. We now look for the complex primes.

Let $\pi = a + b\omega \in D$ and $b \neq 0$. First suppose that $N\pi = 3$. That is $a^2 - ab + b^2 = 3$. Then all integer solutions (a, b) of the equation

$$(2a-b)^2+3b^2=12$$

give all possible $\pi=a+b\omega$ as $1-\omega$, $-1+\omega$, $1+2\omega$, $-1-2\omega$,$2+\omega$ and $-2-\omega$. These are, in fact, associates of $1-\omega$ (or of anyone).Hence

Theorem 2.5. *All elements with norm* 3 *are prime in D.*

Proof. If we show that $1-\omega$ is prime in D, the other 5 elements, being associates of $1-\omega$, are also shown to be prime.

Suppose, on the contrary, that $1-\omega$ is not prime in D. Then $1-\omega$ can be written as a product of two non-unit elements $a+b\omega$ and $c+d\omega$. Then

$$N(1-\omega)=N(a+b\omega).N(c+d\omega)$$

And hence

$$3=N(a+b\omega).N(c+d\omega).$$

But as the numbers on the right hand side are positive integers, one of them must be 1. The corresponding element is a unit. This contradicts with the fact $a+b\omega$ and $c+d\omega$ are non-units. Therefore $1-\omega$ is prime in D. That is all elements with norm 3 in D are primes. ∎

We now consider the primality of elements with norm congruent to 2 modulo 3.

Theorem 2.6. *There is no prime* $\pi=a+b\omega$ *in D with norm* $N\pi\equiv 2(3)$.

Proof. In the cases $a\equiv 0(3)$ and $b\equiv 1(3)$; $a\equiv 1(3)$ and $b\equiv 0(3)$;$a\equiv b\equiv 1(3)$; $a\equiv b\equiv 2(3)$; $a\equiv 2(3)$ and $b\equiv 0(3)$; $a\equiv 0(3)$ and $b\equiv 2(3)$, $N\pi\equiv 1(3)$. Further in the cases $a\equiv b\equiv 0(3)$; $a\equiv 2(3)$ and $b\equiv 1(3)$, $a\equiv 1(3)$ and $b\equiv 2(3)$, $N\pi\equiv 0(3)$. Therefore in any case, we can not have $N\pi\equiv 2(3)$. ∎

Theorem 2.7. *Let* $k>1$. *There is no prime number in D with norm* $3k$.

Proof. By Theorem 2.6, if the norm of $\pi=a+b\omega$ is congruent to zero modulo 3, then there are three cases:

i) $a\equiv 0\equiv b(3)$: In this case, as $\pi=a+b\omega$ is a multiple of 3, it can not be prime.

ii) $a\equiv 2(3), b\equiv 1(3)$: Here we can take $a=3k+2, b=3m+1$, where $k,m\in\mathbb{Z}$. Then

$$N(a+b\omega)=3[3k^2+3k-3km+3m^2+1]$$

We know the existence of elements in D with norm 3. Therefore the only thing that needs to be shown is the existence of an element of D with norm $3k^2+3k-3km+3m^2+1$.It is known that, in D, there are elements conguent to 1 modulo 6. Then if we show that $k^2+k-km+m^2$ is even, then we can write $a+b\omega$ as a product of two elements each congruent to 1 modulo 6.This shows that $a+b\omega$ is not prime.

We have the following possibilities:

a) If k and m are odd

b) If k and m are even

c) If k is odd and m is even, it is straightforward to show that $k^2+k-km+m^2$ is even.

d) If k is even and m is odd, then $a=3k+2$ and $b=3m+1$ are even and hence $2 \mid \pi$. This implies that π can not be prime.

iii) The case $a \equiv 1(3), b \equiv 2(3)$ can be proven similarly to the case ii).

As a result there is no element having norm a proper multiple of 3. ∎

Theorem 2.8. *If p is a rational prime and $N\pi = p \equiv 1(3)$, then p is prime in D.*

Proof. Conversely, suppose that π is not prime in D. Then

$$\pi = (a+b\omega)(c+d\omega)$$

where $a+b\omega$ and $c+d\omega$ are non-units in D. Hence

$$p = N\pi = N(a+b\omega).N(c+d\omega)$$

and therefore $N(a+b\omega)=1$ or $N(c+d\omega)=1$. That is, $a+b\omega$ or $c+d\omega$ must be unit. This contradicts the primality of π. Suppose that $a+b\omega$ is a unit. Then

$$p = N\pi = N(c+d\omega)$$

and as $p \equiv 1(3)$, we have $N(c+d\omega) \equiv 1(3)$. That is $N(c+d\omega)$ can not have a norm congruent to 2 modulo 3. Therefore only the primes $p \equiv 1(3)$ satisfy this property. ∎

Therefore there are three types of primes in D:

1) All elements $\pi = a+b\omega \in D$with norm $N\pi = p$ where $p \equiv 1(3)$ is a rational prime,

2) All rational primes $\pi = q \equiv 2(3)$,

3) All six associates of $\pi = 1-\omega$.

Definition 2.1. *a) The primes in 1) with* $a \equiv 2(3)$, $b \equiv 0(3)$ *appear often in the study of cubic residues. Also in the special case of* $b = 0$, *we have the primes in 2). These two types of primes are called primary primes.*

b) The ones in 1) which are not primary are obtained for

$$a \equiv 1(3),\ b \equiv 0(3)$$

$$a \equiv 1(3),\ b \equiv 1(3)$$

$$a \equiv 0(3),\ b \equiv 1(3)$$

$$a \equiv 2(3),\ b \equiv 2(3)$$

$$a \equiv 0(3),\ b \equiv 2(3)$$

These primes are called secondary primes.

c) The associates of $1 - \omega$ *are called the primes of the third type.*

Remark 2.1. *Note that some primes in* $\mathbb{Z}$ *are not prime in D. For example*

$$7 = (3 + \omega)(2 - \omega)$$

and

$$19 = (5 + 3\omega)(2 - 3\omega)$$

These are rational primes congruent to 1 *modulo* 3.

Example 2.1. *a)* $2 + 3\omega$ *with norm* $7, -1 + 3\omega$ *with norm* 13 *and* $5 + 3\omega$ *with norm* 19 *are primary primes. Also, the rational primes* $2, 5, 11, 17, ...$ *are primary.*

b) $1 + 3\omega, 3 + 4\omega$ *and* $2 + 5\omega$ *having norm* $7, 13$ *and* 19, *respectively, are secondary primes.*

c) All the primes of the third type are $1 - \omega, -1 + \omega, 1 + 2\omega, -1 - 2\omega, 2 + \omega$ *and* $-2 - \omega$.

It is known that every non-zero and non-unit element in D can be stated uniquely as a product of primes in D. Therefore D is a unique factorization domain.

Theorem 2.9. *If* π *is primary in D, then* $N\pi = p$ *or* $N\pi = p^2$ *where* p *is a rational prime. [1]*

Corollary 2.10. *1) If π is primary, then there exists a rational prime p such that $N\pi = p \equiv 1(3)$ when π is complex, and $N\pi = p2 \equiv 1(3)$ when p is rational.*

2) If π is secondary, then there exists a rational prime p such that $N\pi = p \equiv 1(3)$.

3) If π is a prime of the third type, then π is a prime in D as $N\pi = 3$.

Theorem 2.11. *Let p be a rational prime and $\pi \in D$. If $N\pi = p$, then π is prime in D. That is, every element with norm a rational prime is a prime in D. [1]*

Theorem 2.12. *If $\pi \in D$ is prime, then all its associates are also prime. Further, if $N\pi = p$, then the norm of associates of π is also p.*

Proof. Let π be a prime. By definition all of its associates are also prime. Now each associate of π can be written as $\alpha = u.\pi$, where u is a unit in D. Then

$$N\alpha = N(u.\pi) = N(u).N(\pi) = N(\pi)$$

∎

References

[1] Cangül, İ. N., Sayılar Teorisi Problemleri, Paradigma Akademi Yayınları, Bursa, 2002.
[2] Ireland, K. and Rosen, M., A Classical Introduction to Modern Number Theory, Springer, New York,1982.

Received: December 31, 2005