$\mathbb{Z}_n[i]$ Rings

Rings of the form $\{a+bi|a,b \in \mathbb{Z}_n\}$

Reem Mahmoud

Supervised by: Dr. Ayman Badawi

Department of Mathematics and Statistics
American University of Sharjah
12 May 2019

Abstract

This paper studies the Gaussian ring of integers modulo n, $\mathbb{Z}_n[i]$. The motivation for this paper comes from analogizing the ring of real numbers $\mathbb{R}$ to the ring of integers modulo n, $\mathbb{Z}_n$. When appending $[i]$ to the field $\mathbb{R}$, defining $\mathbb{R}[i] := \{a+bi|a,b \in \mathbb{R}\}$, we get the field of complex numbers, $\mathbb{C}$. This paper investigates the possibility of a similar outcome when accounting for $\mathbb{Z}_n$. Does appending $[i]$ to the ring of integers modulo n, $\mathbb{Z}_n$, defining $\mathbb{Z}_n[i] := \{a+bi|a,b \in \mathbb{Z}_n\}$, make it a field? Seeing as $\mathbb{Z}_p^*$ is a field for prime p, our assumption was that $\mathbb{Z}_p[i]$ would be a field for prime p. However, in this paper we examine $\mathbb{Z}_n[i]$ for all $n \in \mathbb{Z}^+$, and find that $\mathbb{Z}_n[i]$ is a field only for values $n = p$ where p is a prime of the form $4k+3$. Additionally, we give a necessary and sufficient condition for an element to be a unit and zero divisor in $\mathbb{Z}_n[i]$. Examples are added to further illustrate the use of our findings. To conclude, we verify our results with algorithms and MATLAB code designed to compute the inverse for any unit and the set of units of $\mathbb{Z}_n[i]$.

Contents

1 Introduction

1.1 Terminology and Notation

- A ring R is a set with operations $(+, .)$ which satisfies the following properties:
  - An abelian group under addition
  - A semigroup under multiplication
  - Distribution: $a(b+c) = ab + ac \, \forall a, b, c \in R$
- A ring with identity is a ring which has an identity under multiplication i.e. $\exists e \in R$ such that $ea = ae = a \, \forall a \in R$
- Let R be a ring, $a \in R$. The inverse of a under addition will be denoted $-a$. The inverse of a under multiplication will be denoted a^{-1}
- Let R be a ring with identity, R is called a commutative ring if and only if it is abelian under multiplication i.e. $ab = ba \, \forall a, b \in R$
- Let R be a commutative ring with identity, R is called a field if and only if it is a group under multiplication i.e. $\exists c \in R$ such that $ca = ac =$ identity of R under multiplication $\forall a \in R$
- Let R be a ring, an element $a \in R$, is called a unit if and only if a is invertible. $U(R)$ will be used to denote the set of units of R.
- Let R be a ring, an element $a \in R, a \neq 0$, is called a nonzero zero divisor if and only if $\exists b \in R, b \neq 0$, such that $ab = 0$. $Z(R)$ will be used to denote the set of zero divisors of R.
- A ring is called an integral domain if and only if the only zero divisor is zero.
- The ring $\mathbb{Z}_n$, the set of integers modulo n, is a field if and only if $n = p$ where p is a prime
- $\mathbb{C}$, which denotes the set of complex numbers, $\mathbb{C} := \{a + bi | a, b \in \mathbb{R}\}$, is a field.
- Addition and multiplication of complex numbers are defined as follows:
  - $(a + bi) + (c + di) = (a + c) + i(b + d)$
  - $(a + bi)(c + di) = (ac - bd) + i(ad + bc)$

2 Fields

Define a set $\mathbb{Z}_n[i] := \{a + bi | a, b \in \mathbb{Z}_n\}$.

Theorem 1. *$\mathbb{Z}_n[i]$ is a commutative ring with identity.*

Proof. First, we show that $\mathbb{Z}_n[i]$ is an abelian group under addition $\forall n$.

- Closure: Let $x = a+bi, y = c+di$. Then $x+y = (a+c)+i(b+d)$. $(a+c), (b+d) \in \mathbb{Z}_n$ so, $x + y \in \mathbb{Z}_n[i]$.
- Associativity: Let $x = a + bi, y = c + di, z = e + fi$. Then $x + (y + z) = (a + bi) + ((c + e) + i(d + f)) = ((a + c) + i(b + d)) + (e + fi) = (x + y) + z$.
- Abelian: Let $x = a+bi, y = c+di$. Then $x+y = (a+c)+i(b+d) = (c+a)+i(d+b) = y + x$.
- Identity: $0 + 0i$. Let $x = a + bi$, then $(0 + 0i) + x = (0 + a) + i(0 + b) = a + bi = x$.
- Inverse: Let $x = a+bi$, then $-x = -(a+bi) = -a-bi$. Now $x-x = (a-a)+i(b-b) = 0 + 0i$.

Now, we show that $\mathbb{Z}_n[i]$ is closed, associative, and has an identity under multiplication $\forall n$.

- Closure: Let $x = a+bi, y = c+di$. Then $xy = (ac-bd)+i(ad+bc)$. $ac, bd, ad, bc, (ac-bd), (ad + bc) \in \mathbb{Z}_n$ so, $xy \in \mathbb{Z}_n[i]$.
- Associativity: Let $x = a + bi, y = c + di, z = e + fi$. Then $x(yz) = (a + bi)((ce - df) + i(cf + de)) = ((ac - bd) + i(ad + bc)) + (e + fi) = (xy)z$.
- Commutativity: Let $x = a + bi, y = c + di$. Then $xy = (ac - bd) + i(ad + bc) = (ca - db) + i(da + cb) = yx$.
- Distribution: Let $x = a+bi, y = c+di, z = e+fi$. Then $x(y+z) = (a+bi)((c+e)+i(d+f)) = (a(c+e)-b(d+f))+i(a(d+f)+b(c+e)) = ac+ae-bd-bf+i(ad+af+bc+be) = ((ac - bd) + i(ad + bc)) + ((ae - bf) + i(af + be)) = xy + xz$.
- Identity: $1 + 0i$. Let $x = a + bi$, then $(1 + 0i)x = (a - 0) + i(b + 0) = a + bi = x$.

■

Theorem 2. *If n is composite or $n = 2$, $\mathbb{Z}_n[i]$ is not a field.*

Proof. For $n = 2$:
$\mathbb{Z}_2[i] = \{0 + 0i, 0 + 1i, 1 + 0i, 1 + 1i\}$. We have $(1 + 1i)^2 = 0 + 0i$. Thus $1 + 1i$ doesn't have a multiplicative inverse in $\mathbb{Z}_2[i]$. $\mathbb{Z}_2[i]$ is not a field.
For composite n:
Since $\mathbb{Z}_n$ is not a field for composite n, and $\mathbb{Z}_n \subset \mathbb{Z}_n[i]$, $\mathbb{Z}_n[i]$ is not a field. ■

Now, it is clear from *Theorem*2 that for $\mathbb{Z}_n[i]$ to be a field the only 2 possible values left for n are: $n = p$, where p is an odd prime of the form $4k + 3$, or $n = p$, where p is an odd prime of the form $4k + 1$.

Theorem 3. *$\mathbb{Z}_n[i]$ is a field if and only if $n = p$ for some odd prime p of the form $4k + 3$, $k \in \mathbb{Z}$.*

Proof. Let $a + bi \in \mathbb{Z}_p[i]$, $a + bi \neq 0$, we are trying to find an element, say $c + di \in \mathbb{Z}_p[i]$, $c + di \neq 0$, such that $(a + bi)(c + di) = 1$ i.e. such that:

- $ac - bd \equiv 1$
- $ad + bc \equiv 0$

Using Cramer's Rule, this system has a unique solution if and only if

$$\begin{vmatrix} a & -b \\ b & a \end{vmatrix} \neq 0 \tag{1}$$

$$a^2 + b^2 \neq 0 \tag{2}$$

multiplying by a^{-2} assuming, without loss of generality, that $a \neq 0$, and since $\mathbb{Z}_p^*$ is a field

$$1 + a^{-2}b^2 \neq 0 \tag{3}$$

$$(a^{-1}b)^2 \neq -1 \tag{4}$$

let $x = a^{-1}b$

$$x^2 = -1 \tag{5}$$

is not solvable in $\mathbb{Z}_p^*$

$$x^4 = 1 \tag{6}$$

is not solvable in $\mathbb{Z}_p^*$ i.e. if and only if $\nexists x \in \mathbb{Z}_p^*$ with order 4.

Now, we know $\mathbb{Z}_p^*$ is a cyclic group under multiplication and $|\mathbb{Z}_p^*| = p-1$. So, if $p = 4k+1$, $p - 1 = 4k$, so $4 \mid p - 1$. Hence, $\exists!$ cyclic subgroup of order 4 and thus, $\exists$ an element $x \in \mathbb{Z}_p^*$ of order 4. Therefore, $x^4 = 1$ is solvable in $\mathbb{Z}_p^*$. However, if $p = 4k + 3$, $p - 1 = 4k + 2$, so $4 \nmid p - 1$. Hence, $\nexists$ a cyclic subgroup of order 4 and thus, $\nexists$ an element $x \in \mathbb{Z}_p^*$ of order 4. Therefore, $x^4 = 1$ is not solvable in $\mathbb{Z}_p^*$.
So, $\mathbb{Z}_p[i]$ is a field if and only if $p = 4k + 3$. ■

Corollary 1. *Since $\mathbb{Z}_n[i]$ is finite, it is an integral domain if and only if it is a field. Hence, $\mathbb{Z}_n[i]$ is an integral domain if and only if $n = p$ for some odd prime p of the form $4k + 3$, $k \in \mathbb{Z}$.*

Theorem 4. *Let F be a finite field, define $F[i] := \{a + bi | a, b \in F\}$. $F[i]$ is a field if and only if $|F| = p^n$, where p is a prime of the form $4k + 3$, $k \in \mathbb{Z}$ with $n \in \mathbb{Z}^+$.*

Proof. Let F be a finite field, we know $|F| = p^n$, where p is a prime, $n \in \mathbb{Z}^+$. Additionally, F is a field extension of $\mathbb{Z}p$ i.e. $\mathbb{Z}_p \subset F$. Thus, if $|F| = p^n$ where $p = 2$ or p is of the form $4k+1$, then $\mathbb{Z}_p[i] \subset F[i]$, and $F[i]$ is not a field. On the other hand, if p is of the form $4k+3$, $|F| = (4k + 3)^n$. Using the binomial expansion theorem, $|F| = (4k + 3)^n = \sum_{m=0}^{n} \binom{n}{m} (4k)^{n-m} 3^m$. Clearly, each term in this summation has 4 as a factor expect for the last term which is 3^n. Thus, $4 \nmid |F|$, and since every finite field is cyclic under multiplication, by the same approach presented in *Theorem*3, and given that equations $(1 - 6)$ are applicable still, $F[i]$ is a field. ■

Examples.

The following are examples of fields: $\mathbb{Z}_3[i]$, $\mathbb{Z}_7[i]$, $\mathbb{Z}_{11}[i]$, $\mathbb{Z}_{19}[i]$, $F[i]$ where $|F| = p^n$ and p is a prime of the form $4k+3$, etc.

On the other hand, the following are not fields: $\mathbb{Z}_2[i]$, $\mathbb{Z}_4[i]$, $\mathbb{Z}_5[i]$, $\mathbb{Z}_{13}[i]$, etc.

Ultimately, what makes these findings even more interesting is the fact that we can now construct fields of specific orders using an unconventional method. Normally, fields are constructed using irreducible polynomials. Taking an irreducible polynomial $f(x)$ of degree n, which is guaranteed to exist, and forming $\mathbb{Z}_p[x]/f(x)$ gives us a field of order p^n. However, we have found a new way involving complex numbers which allows us to form fields of order p^n, $n \in 2\mathbb{Z}^+$, where p is a prime of the form $4k+3$. Notice that $n \in 2\mathbb{Z}^+$, that is because depending on the order of the field we use for construction, say F, the resulting field $F + Fi$ will have $|F + Fi| = |F|^2$. So, if $|F| = p^m$, $m \in \mathbb{Z}^+$, $|F + Fi| = p^{2m} = p^n$, where $n = 2m \in 2Z^+$.

Consider constructing a field of order p^2. By taking a field F of order p you can form the field $F_1 = F + Fi$ which has p^2 elements. Similarly, consider constructing a field of order p^4. One can either construct $G_1 = G + Gi$ where G is a field of order p^2, or they can construct $F_2 = F_1 + F_1 j$ where, similar to i, $j^2 = -1$. The reason for a variable change is to ensure the formation of p^4 distinct elements, because if we were to construct F_2 as $F_2 = F_1 + F_1 i$, then taking any 2 elements $a + bi$ and $c + di \in F_1$ leads to constructing the following element in F_2, $(a + bi) + (c + di)i = (a - d) + (b + c)i$ which is also $\in F_1$. In other words, we end up always constructing elements from F_1, so, we'd construct only p^2 elements since half of the elements will be duplicates of the others.

Accordingly, consider constructing a field of order p^6. One can construct the field $H_1 = H + Hi$ where H is a field of order p^3. However, since we can't construct a field of the form $F_3 = M + Mi$, where F_3 is a field of order p^3 and M is a finite field, seeing as $3 \notin 2Z^+$, we can't use the trick we used for p^2 and construct H_1 as $H_1 = F_3 + F_3 j$.

As a result, we can clearly see that in order to construct a field F of order p^n, where $F = F_1 + F_1 i_1$, $i_1^2 = -1$, and $F_1 = F_2 + F_2 i_2$, $i_2^2 = -1$, and $F_2 = F_3 + F_3 i_3$, $i_3^2 = -1$, ..., and $F_{m-1} = F_m + F_m$, $i_m^2 = -1$, where $|F_m| = p^k$, $k \in \mathbb{Z}^+$, $gcd(k, 2) = 1$, it must be that $n = 2^m k$.

Based on that, consider constructing finite fields of the following orders (assume p is a prime of the form $4k+3$):

- $p^{24} = p^{3(2)^3}$
  - Method 1: Let F_1 be a finite field, $|F_1| = p^{12}$, we construct $F = F_1 + F_1 i_1 \rightarrow |F| = p^{24}$
  - Method 2: Let F_2 be a finite field, $|F_2| = p^6$, we construct $F_1 = F_2 + F_2 i_2 \rightarrow |F_1| = p^{12}$, then we construct $F = F_1 + F_1 i_1 \rightarrow |F| = p^{24}$
  - Method 3: Let F_3 be a finite field, $|F_3| = p^3$, we construct $F_2 = F_3 + F_3 i_3 \rightarrow |F_2| = p^6$, then we construct $F_1 = F_2 + F_2 i_2 \rightarrow |F_1| = p^{12}$, then we construct $F = F_1 + F_1 i_1 \rightarrow |F| = p^{24}$
- $p^{16} = p^{2^4}$

- Method 1: Let F_1 be a finite field, $|F_1| = p^8$, we construct $F = F_1 + F_1 i_1 \to |F| = p^{16}$
- Method 2: Let F_2 be a finite field, $|F_2| = p^4$, we construct $F_1 = F_2 + F_2 i_2 \to |F_1| = p^8$, then we construct $F = F_1 + F_1 i_1 \to |F| = p^{16}$
- Method 3: Let F_3 be a finite field, $|F_3| = p^2$, we construct $F_2 = F_3 + F_3 i_3 \to |F_2| = p^4$, then we construct $F_1 = F_2 + F_2 i_2 \to |F_1| = p^8$, then we construct $F = F_1 + F_1 i_1 \to |F| = p^{16}$
- Method 4: Let F_4 be a finite field, $|F_4| = p$, we construct $F_3 = F_4 + F_4 i_4 \to |F_3| = p^2$, then we construct $F_2 = F_3 + F_3 i_3 \to |F_2| = p^4$, then we construct $F_1 = F_2 + F_2 i_2 \to |F_1| = p^8$, then we construct $F = F_1 + F_1 i_1 \to |F| = p^{16}$

- $p^{30} = p^{3(5)(2)}$
  - Method 1: Let F_1 be a finite field, $|F_1| = p^{15}$, we construct $F = F_1 + F_1 i \to |F| = p^{30}$
- $p^{35} = p^{7(5)}$
  - Not possible

3 Set of Units and Zero Divisors

Now, using the proof for *Theorem*3, we give a necessary and sufficient condition so that an element $a + bi \in \mathbb{Z}_n[i]$ is invertible:

Theorem 5. *Let $n \geq 1$ be a positive integer and $a + bi \in \mathbb{Z}_n[i]$, then $a + bi$ is invertible if and only if $a^2 + b^2 \in U(\mathbb{Z}_n)$. Furthermore, suppose $(a+b)^{-1} = c + di$, then $c = a(a^2 + b^2)^{-1}$ and $d = -b(a^2 + b^2)^{-1}$.*

Proof. If $(a + b)^{-1} = c + di$, then $(a + bi)(c + di) = 1$. Now, using Cramer's Rule from *Theorem*3, the unique solution to the equations

- $ac - bd \equiv 1$ in $\mathbb{Z}_n$
- $ad + bc \equiv 0$ in $\mathbb{Z}_n$

is $c = \dfrac{\begin{vmatrix} 1 & -b \\ 0 & a \end{vmatrix}}{\begin{vmatrix} a & -b \\ b & a \end{vmatrix}} = \frac{a}{a^2+b^2} = a(a^2 + b^2)^{-1}$ and $d = \dfrac{\begin{vmatrix} a & 1 \\ b & 0 \end{vmatrix}}{\begin{vmatrix} a & -b \\ b & a \end{vmatrix}} = \frac{-b}{a^2+b^2} = -b(a^2 + b^2)^{-1}$. However, $(a^2 + b^2)^{-1}$ exists if and only if $a^2 + b^2 \in U(\mathbb{Z}_n)$. ■

Corollary 2. *Consequently, since both $\mathbb{Z}_n$ and $\mathbb{Z}_n[i]$ are finite, meaning every non-unit is a zero divisor, let $n \geq 1$ be a positive integer and $a + bi \in \mathbb{Z}_n[i]$, then $a + bi$ is a zero divisor if and only if $a^2 + b^2 \in Z(\mathbb{Z}_n)$. The set of zero divisors thereby is as follows: $Z(\mathbb{Z}_n[i]) := \mathbb{Z}_n[i] - U(\mathbb{Z}_n[i])$.*

Examples.

Consider for starters $\mathbb{Z}_2[i]$, the set of units $U(\mathbb{Z}_2[i]) = \{1+0i, 0+1i\}$ since $0^2+1^2 = 1 \in U(\mathbb{Z}_2)$ and consequently, the set of zero divisors $Z(\mathbb{Z}_2[i]) = \{0+0i, 1+1i\}$ since $0 \notin U(\mathbb{Z}_2)$ and $1^2+1^2 = 2 \equiv 0$ in $\mathbb{Z}_2$. If we wish to compute the inverse of the unit $0+1i$, we will have $(0+1i)^{-1} = c+di$ where $c = 0$ and $d = -1(1^{-1}) = -1 \equiv 1$, thus $(0+1i)^{-1} = 0+1i$.

We consider the following elements in each given ring and test whether this element is a unit. If yes, we compute the inverse:

1. $4+4i \in \mathbb{Z}_5[i] \to 4^2+4^2 = 32 \equiv 2 \in U(\mathbb{Z}_5) \to 4+4i \in U(\mathbb{Z}_5[i]) \to c = 4(2^{-1}) = 4(3) = 12 \equiv 2$ and $d = -4(2^{-1}) = -2 \equiv 3 \to (4+4i)^{-1} = 2+3i$

2. $11+8i \in \mathbb{Z}_{13}[i] \to 11^2+8^2 = 185 \equiv 3 \in U(\mathbb{Z}_{13}) \to 11+8i \in U(\mathbb{Z}_{13}[i]) \to c = 11(3^{-1}) = 11(9) = 99 \equiv 8$ and $d = -8(3^{-1}) = 5(9) = 45 \equiv 6 \to (11+8i)^{-1} = 8+6i$

3. $16+4i \in \mathbb{Z}_{17}[i] \to 16^2+4^2 = 272 \equiv 0 \in Z(\mathbb{Z}_{17}) \to 16+4i \in Z(\mathbb{Z}_{17}[i])$

4. $3+2i \in \mathbb{Z}_4[i] \to 3^2+2^2 = 13 \equiv 1 \in U(\mathbb{Z}_4) \to 3+2i \in U(\mathbb{Z}_4[i]) \to c = 3(1^{-1}) = 3$ and $d = -2(1^{-1}) = -2 \equiv 2 \to (3+2i)^{-1} = 3+2i$

5. $8+7i \in \mathbb{Z}_{15}[i] \to 8^2+7^2 = 113 \equiv 8 \in U(\mathbb{Z}_{15}) \to 8+7i \in U(\mathbb{Z}_{15}[i]) \to c = 8(8^{-1}) = 8(2) = 16 \equiv 1$ and $d = -7(8^{-1}) = 8(2) = 16 \equiv 1 \to (8+7i)^{-1} = 1+1i$

6. $18+6i \in \mathbb{Z}_{21}[i] \to 18^2+6^2 = 360 \equiv 3 \in Z(\mathbb{Z}_{21}) \to 18+6i \in Z(\mathbb{Z}_{21}[i])$

4 Conclusion

In conclusion, this paper considers complex numbers of the form $\mathbb{Z}_n+\mathbb{Z}_n i$ where the imaginary and real parts are taken from $\mathbb{Z}_n$. The primary aim was to find conditions on n such that $\mathbb{Z}_n + \mathbb{Z}_n i$ is a field. Most importantly, we were able to construct fields of cardinalities p^n, $n \in 2\mathbb{Z}^+$, $p = 4k+3$, $k \in \mathbb{Z}$, contrary to common methods which use irreducible polynomials. A set of algorithms and MATLAB code are provided in the appendix for computation of the inverse of any unit and the set of units of $\mathbb{Z}_n + \mathbb{Z}_n i$.

For future work, we would like to study ideals of the ring of Gaussian integers modulo n, $\mathbb{Z}_n[i]$. We wish to investigate theorems pertaining to the order of the ring, or the value of n and its relation with regards to the possibility of the ring being a principle ideal domain, Euclidian domain, and unique factorization domain.

References

[1] A. Badawi, *Abstract Algebra Manual: Problems and Solutions*, Nova Science Publishers, 2004.

Appendices

A Algorithms

In this section we propose algorithms for the construction of the ring of Gaussian integers $\mathbb{Z}_n[i]$, as well as, finding the inverse of any unit and the set of units of $\mathbb{Z}_n[i]$.

A.1 Algorithm to Construct $\mathbb{Z}_n[i]$

input : n
output: 2D array A

```
1 x ← zn(n);
2 for i = 1 to n do
3 |   for j = 1 to n do
4 |   |   A(i,j)← x(i)+x(j)i;
5 |   end
6 end
```

Algorithm 1: Algorithm to Construct $\mathbb{Z}_n[i]$

Commentary: Create a 2D array, A, and give each cell the value of a complex number created using values from $\mathbb{Z}_n$, by calling the function zn which takes n as an input and outputs an array with elements of $\mathbb{Z}_n$, as follows:

input : n
output: 1D array A

```
1 for i = 1 to n do
2 |   A(i)← i − 1;
3 end
```

Algorithm 2: Algorithm to Construct $\mathbb{Z}_n$

MATLAB code:

```
function [A] = zni(n)
y=zn(n);
A=zeros(length(y),length(y));
for i=1:length(y)
    for j=1:length(y)
        A(i,j)=complex(y(i),y(j));
    end
end
end
```

```
function [y] = zn(n)
y=zeros(1,n);
for i=1:n
    y(i)=i-1;
end
end
```

A.2 Algorithm to Check for Unit and Find Inverse for an Element in $\mathbb{Z}_n[i]$

input : a+bi,n
output: inverse

1 **if** unitzn(a^2+b^2,n)$= 0$ **then**
2 | inverse $= 0$;
3 **else**
4 | inverse $\leftarrow a$(unitzn(a^2+b^2,n))$-b$(unitzn(a^2+b^2,n))i;
5 **end**

Algorithm 3: Algorithm to Check for Unit and Find Inverse for an Element in $\mathbb{Z}_n[i]$

Commentary: Verify whether a^2+b^2 is a unit of $\mathbb{Z}_n$, which can be done by calling the function *unitzn* which takes an element from $\mathbb{Z}_n$ and n as inputs and either outputs the inverse of the element in $\mathbb{Z}_n$, or, if the inverse does not exist, outputs zero as the inverse as follows:

input : n
output: inverse

1 **if** *gcd(a,n)=1* **then**
2 | inverse $= c$;
3 | (// c can be calculated using Euclid's Division Algorithm)
4 **else**
5 | inverse $\leftarrow 0$;
6 **end**

Algorithm 4: Algorithm to Check for Unit and Find Inverse for an Element in $\mathbb{Z}_n$

MATLAB code:

```
function [result] = is_unit_zni(x,n)
if is_unit_zn(mod(real(x)^2+imag(x)^2,n),n)==0
    result=0;
else
    result=complex(mod(real(x)*is_unit_zn(real(x)^2+imag(x)^2,n),n),...
    mod(-imag(x)*is_unit_zn(real(x)^2+imag(x)^2,n),n));
end
```

```
function [result] = is_unit_zn(a,n)
[g, c, ~] = gcd(a,n);
if g==1
    result = mod(c,n);
else
    result=0;
end
end
```

A.3 Algorithm to Find Set of Units for $\mathbb{Z}_n[i]$

```
   input  : n
   output: set
 1 A ← zni(n);
 2 k ← 1;
 3 for i = 1 to n do
 4 |   for j = 1 to n do
 5 |   |   if unitzni(A(i,j),n) ≠ 0 then
 6 |   |   |   set(i) ← A(i,j);
 7 |   |   |   k = k + 1;
 8 |   |   end
 9 |   end
10 end
```

Algorithm 5: Algorithm to Find Set of Units for $\mathbb{Z}_n[i]$

Commentary: Create a 2D array, A, with the elements of $\mathbb{Z}_n[i]$ calling the function from the first algorithm. Then, check whether each element in the 2D array is a unit calling the function from the second algorithm. If an element is a unit, add it to the resulting array, *set*.

MATLAB code:

```
1  function [y] = units_zni(n)
2  r=zni(n);
3  k=1;
4  for i=1:n
5      for j=1:n
6          if is_unit_zni(r(i,j),n)~=0
7              y(k)=r(i,j);
8              k=k+1;
9          end
10     end
11 end
```