Math 319NT Fall 2024 **Name: Aby Soumare**
Lab 2: Exploring the Gaussian Integers
Collaborators:

Introduction

For this lab, we were tasked by Professor Tori Day to explore the Gaussian integers, $\mathbb{Z}[i]$, by completing various exercises given by her. There were two questions that Professor Day wanted us to be able to answer by the end of the lab:

- How can you work with the Gaussian integers?
- What numbers that are prime in $\mathbb{Z}$ are also prime in $\mathbb{Z}[i]$?

Resources used in this lab are as follows; Magma, Overleaf, Professor Tori Day, and the textbook Number Theory and Cryptography by Tori Day and Tom Weston.

Background

Before we start to get into the rest of the lab, here are some terms you must be familiar with:

Definition 0.1 ***Gaussian integers*** *are the numbers with a number within $\mathbb{Z}$ and an imaginary part. Often denoted as $\mathbb{Z}[i]$.*

Example 0.2 *Gaussian Integers:*

$$5i,$$
$$-2i.$$

Note the i that is being multiplied onto the normal integers, this is the imaginary part of the Gaussian integer. The i being multiplied on is a tell-tale sign that the number you have is within the Gaussian integers.

Definition 0.3 *The **norm** of a Gaussian integer $a + bi$ will be the real number associated with a Gaussian integer. The equation for this would be $a^2 + b^2$. We denote the norm as $N()$.*

Example 0.4 *See the Gaussian integer $2+2i$, the norm of this would be $N(2+2i) = 2^2+2^2 = 8$. For the Gaussian integer $4 + 2i$, $N(4 + 2i) = 4^2 + 2^2 = 20$.*

Definition 0.5 *The **conjugate** of a Gaussian integer is best described with an example: $(4 - i)(4 + i)$. The $(4 + i)$ would be the conjugate of $(4 - i)$.*

Definition 0.6 *A **divisor** is a number that evenly divides a number with no remainder. If we want to know if $a|b$ (said "a divides b") then there exists an $m \in \mathbb{Z}$ or $\mathbb{Z}[i]$ such that $b = am$.*

Example 0.7 *$4 = 2 * 2$, so $2|4$ in $\mathbb{Z}$.*
$2 = (1-i)(1+i)$ so $(1-i)|2$ and $(1+i)|2$ in $\mathbb{Z}[i]$.
Also note that there does not exist an m such that
$0 = am$.
If a number does not divide another, we use the notation $a \nmid b$.

Definition 0.8 *A prime in the Gaussian integers is a number that only has divisors ± 1, $\pm i$ and itself.*

In the rest of this lab, we will use this knowledge and resources stated above to dive deeper into understanding the Gaussian integers.

Analysis

At the beginning of the lab, we were tasked to play around with magma a little bit. This would allow us to more clearly understand the code we are given, as well as give us the tools to try and tackle larger tasks. Our first exercise is as follows:

Exercise 0.1 *Do the following:*

- *Create two different Gaussian integers: $g := R!5; c := R!6$*
- *Add the two integers: $g + c; ... = 11$*
- *Multiply the two integers: $g * c; ... = 30$*

As one can see, the integers produced act as they normally would in $\mathbb{Z}$. We need to tell the computer that we are working in the Gaussian integers, and this next exercise will help us realize the differences:

Exercise 0.2 *Do the following:*

- *Use IsSquare() to check if -1 is a square: False*
- *Use IsSquare() to check if $-1 + 0 * i$ is a square: True, $-i$*
- *Why did you get two different numbers here?: Within $\mathbb{Z}$, -1 is not square because a square will never be negative, but $-1 = i^2$ in the Gaussian.*

Now that we understand how the computer works with Gaussian and non-Gaussian integers, let's play with the Gaussian a little more by doing the following:

Exercise 0.3 *Do the following:*

- *Create your favorite Gaussian integer in Magma:* $m := R!8;$
- *Use Magma to find its conjugate:* $conjugate(m); ...8$
- *Use Magma to find its norm:* $Norm(m); ...64$

Now that we understand all that the computer can do for us, we will move on to the second question asked at the beginning of the lab.

A clean way to do this is to first understand the divisors of numbers within $\mathbb{Z}$ and $\mathbb{Z}[i]$.

Exercise 0.4 *Use Divisors to compute the divisors of the following Gaussian integers:*

- *5:* $1, i+2, -i+2, 5$
- *3:* $1, 3$
- *Divisors(R!8):* $1, -i+1, -2*i, -2*i, -2, -4, 4*i-4, 8$

Now, what does this mean for the lab? For our question, it is important to note what makes a number prime in $\mathbb{Z}$ and what makes a number prime in $\mathbb{Z}[i]$. So, in order to make sure we know exactly what is happening in our computer, we need to ask ourselves a very important question:

Exercise 0.5 *How many elements should be in divisors for an integer that is prime and remains prime in* $\mathbb{Z}[i]$*?: While using magma, the only thing that should be returned for the divisors of a prime number in both* $\mathbb{Z}$ *and* $\mathbb{Z}[i]$ *is* 1*, so there are* 2 *elements in the list.*

Let us expand our understanding of the topic. We were tasked to write some code to figure out which of the first 100 primes in $\mathbb{Z}$ remain prime in $\mathbb{Z}[i]$. The code for this is written within Code 0.6.

Conjecture 0.9 *Notice what primes become not-prime within the Gaussian integers:*
$2, 5, 13, 17, ...$ *etc.*
These numbers in the Gaussian integers have more than 2 *divisors. The property that all of these numbers have in the Gaussian integers is that they can be expressed as a sum of two squares. For example:*

$$\begin{aligned} 2 &= 1^2 + 1^2, \\ 5 &= 2^2 + 1^1, \\ 13 &= 3^2 + 2^2, \end{aligned}$$

and so on. Remember our definition of Norm: "The real number associated with a Gaussian integer, the equation being $a^2 + b^2$*." Because of this we know if our prime number can be expressed as a sum of two squares, it is not prime in the Gaussian integers.*

Exercise 0.6 *Recall our conjecture from the first lab. In the first lab, our conjecture was talking about the quantity of primes in primes of $\mathbb{Z}$ and this lab is now talking about the primes within $\mathbb{Z}[i]$. Within the primes up to 100 in $\mathbb{Z}$, the number of primes that can be expressed as a sum of two squares was the floor() of the number of primes, and this held for primes up to 200 as well. For this lab, the same pattern is also present, however the number of primes in both $\mathbb{Z}$ and $\mathbb{Z}[i]$ will be half of the number of primes from 1-100 rounded UP to the nearest whole number.*

Future Directions

There were many topics undiscovered in this lab. A couple questions to ask yourself are as follows:

- How would modular arithmetic fit into this lab?
- How would one complete this lab purely via proof writing? Is magma needed to solve these questions?

Appendix

Code 0.10 *Define the Gaussian Integers:*

```
R<i>:=MaximalOrder(QuadraticField(-1))
```

Code 0.11 *Coercing Elements into R:*

```
R!(1+i);
R!5;
a:=R!10;
```

Code 0.12 *Writing Elements:*

```
1+2*i;
5+0*i;
b:=3-4*i;
```

Code 0.13 *Remain Prime in $\boldsymbol{Z}[i]$*

```
S:={};
for n in PrimesUpTo(200) do
    a:=R!n;
    b:=#Divisors(a);
    if b le 2 then
        S join {b,a};
```

```
        end if;
    end for;
    print(S);
```