**Assignment-1**

**$\mathbb{Z}[i]$ : The ring of Gaussian integers**

( Concepts covered: Norm function, Units, Prime elements of $\mathbb{Z}[i]$)

Notation: $p$ will always denote a prime number in $\mathbb{Z}$ and $R$ will denote the ring $\mathbb{Z}[i]$.

**(1)**Revise basic concepts and results from Ring theory related to: Euclidean domain, P.I.D, U.F.D.

**(2)** Show that there are infinitely many integer solutions to the the equation

$$a^n + b^n = c^n, \quad n = 1, 2$$

**(3)** Let $F$ be a finite field.
(a) Show that the multiplicative group $F^\times$ is a cyclic group.
(b) Use (a) to show that if $p \equiv 1 (\text{mod } 4)$ then there exists a square root of $-1$ in $(\mathbb{Z}/p\mathbb{Z})^\times$

There is another way of proving the fact in 3(b) :
(**3′**) Prove Wilson's theorem: For any prime no. $p$,

$$(p-1)! \equiv -1 (\text{mod } p)$$

and prove the above fact as an application of Wilson's theorem.

**(4)** Prove the following properties for $R$.
(a) $R$ is a domain and a Euclidean domain w.r.t. the norm $N : R \to \mathbb{Z}$ where for any element $\alpha = a + ib \in R$, $N(\alpha) = a^2 + b^2$.
(b) Show that the norm function is multiplicative, i.e. $N(\alpha\beta) = N(\alpha)N(\beta)$.
(c) $N(\alpha) = 1$ if and only if $\alpha$ is a unit.
(d) Calculate the group $\mathbb{Z}[i]^\times$.
(f) Show that if $\alpha \in R$ is such that $N(\alpha)$ is a prime no. Then show that $\alpha$ is a prime element of $R$.

In next exercises we will compute $Spec(R)$ := the set of all prime ideals of $R$.

**(5)** Show that if $\pi$ is a prime element of $R$ then $\pi$ divides some prime no. in $\mathbb{Z}$.

**(6)** Prove that $p \equiv 1 (\text{mod } 4)$ if and only if $p = a^2 + b^2$ where $a, b \in \mathbb{Z}$:
**Hint:** you can use following steps and some of the previous exercises:

Step 1: Use (2) to show that if $p \equiv 1(\text{mod } 4)$ then $p|(X^2+1)$.
Step 2: Considering the fact $p|(X^2+1)$ in $R$, conclude that $p$ is not a prime element in $R$. Thus by using 4(a) conclude that $p$ is not a irreducible element.
Step 3: Write $p = \alpha\beta$ for some $\alpha, \beta \in R$. Use norm function and 4(b)and 4(c) to conclude that $p = a^2 + b^2$.

**(7)** Prove that if $\pi$ is a prime element in $R$, then
(a) $\pi = 1 + i$ or
(b) $\pi = a + bi$ where $a^2 + b^2 = p, p \equiv 1(\text{mod } 4)$ or
(c) $\pi = p \equiv 3(\text{mod } 4)$.

The next exercise is the summary of how a prime no. in $\mathbb{Z}$ behaves when considered as an element of $R$.

**(8)** If $p$ is a prime no. in $\mathbb{Z}$, then
(a) $p = 2 = (1+i)(1-i)$. i.e. it is a product of two conjugate prime elements.
(b) $p \equiv 1(\text{mod } 4)$ then (6) tells us that $p = (a+bi)(a-bi)$ where $(a+bi)$ is a prime element by 7(b). Thus it is again a product of conjugate prime elements.
In the cases (a) , (b) we say that '$p$ **ramifies** in $R$'.
(c) $p \equiv 3(\text{mod } 4)$ then $p$ stays a prime element in $R$ by 7(c). In such a case we rephrase this by saying '$p$ stays **inert** in $R$'.