2. Problem 2 Solution

2.3 Part 3.

Consider a prime number p of the form $4n+1$, p is prime in $\mathbb{Z}$.

Lemma 4. *p is not prime in $\mathbb{Z}[i]$ if p is of the form $4n+1$.*

Proof. Since p is of the form $4n+1$, by (2.5) we have some x such that $(x^2+1)mod\,p = 0$, or we can say that $x^2+1 = kp, k \in \mathbb{N}$.
Now assume p is a prime number in $\mathbb{Z}[i]$.
We can write $x^2+1 = (x+i)(x-i)$ and since $p \mid x^2+1$, by definition of prime in $\mathbb{Z}[i]$, $p \mid x+i$ or $p \mid x-i$.
Case 1. $p \mid x+i$
Since $p \mid x+i$, $\frac{x}{p} + \frac{i}{p} \in \mathbb{Z}[i]$ but since we know that i is a unit in $\mathbb{Z}[i]$, $\frac{i}{p} \notin \mathbb{Z}[i]$, thus our statement is a **Contradiction**.
Case 2. $p \mid x-i$
Same argument as that of **Case 1**.
By above 2 cases, our lemma is proved. □

Now we will prove that there exists integers x, y and c such that $x^2+y^2 = cp$ and $gcd(c,p) = 1$.

Proof. Since we have proved that p is not a prime in $\mathbb{Z}[i]$, we consider that it is product of 2 numbers from $\mathbb{Z}[i]$.
Let $p = (x+iy)(a+ib)$, doing computations on it and equating imaginary part to 0, we get:

$$p = (ax - by) + i(ay + bx) \tag{2.6}$$

$$ay + bx = 0 \tag{2.7}$$

$$\frac{a}{b} = -\frac{x}{y} \tag{2.8}$$

$$kp = x^2 + y^2, k = \frac{x}{a} \tag{2.9}$$

Putting $k = 1$ in the above equation, we get $p * 1 = x^2 + y^2, x, y \in \mathbb{Z}$ and $gcd(1,p) = 1$ and so the proof is complete □

2.4 Part 4.

We are given that p is prime number such that $x^2 + y^2 = cp$, where x, y and c are integers and $gcd(c,p) = 1$.
I have to prove that p is not a prime in $\mathbb{Z}[i]$.

Proof. Assume that p is a prime in $\mathbb{Z}[i]$.
Since $cp = x^2 + y^2$, we can write it as $cp = (x+iy)(x-iy)$, since $p \mid (x+iy)(x-iy)$, by definition of prime in $\mathbb{Z}[i]$, either $p \mid (x+iy)$ or $p \mid (x-iy)$.
Considering either of the both cases we get that $\frac{x}{p}, \frac{y}{p} \in \mathbb{Z}[i]$ and since $x, y \in \mathbb{Z}$, also units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$, and $p \mid x$ and $p \mid y$.
Using above result, $x = ap$ and $y = bp$, $a, b \in \mathbb{Z}$, putting these values in our original equation we get:

$$cp = b^2p^2 + a^2p^2 \tag{2.10}$$

$$c = p(b^2 + a^2) \tag{2.11}$$

Since equation (2.11) is a **Contradiction** to the fact that $gcd(c,p) = 1$, thus p is not a prime in $\mathbb{Z}[i]$. □

2.5 Part 5.

We are given a prime number p which is prime in $\mathbb{Z}$ but not in $\mathbb{Z}[i]$.
I have to prove that $p = a^2 + b^2$ and $a, b \in \mathbb{Z}$.

Proof. Since p is not a prime in $\mathbb{Z}[i]$, we can write p as $p = (a + ib)(x + iy)$, where a, b, x, y are integers.
Now doing the same computations done in (2.6),(2.7),(2.8) and (2.9), putting $k = 1$, we get:

$$p = x^2 + y^2, \quad x, y \in \mathbb{Z}$$

The above equation is the one which I had to prove and so my proof is complete. □

2.6 Part 6.

We are given that p is a prime number in $\mathbb{Z}$ and is of the form $4n + 1$.
I have to prove that $p = a^2 + b^2$, where $a, b \in \mathbb{Z}$.

Proof. Using **Lemma 4**, we can say that since p is of the form $4n + 1$, p will not be a prime in $\mathbb{Z}[i]$.
Since p is not a prime in $\mathbb{Z}[i]$, from the proof of **2.5 Part 5.** we can say that $p = a^2 + b^2$ for some integers a and b, which concludes our proof. □