Problem 16.2 Let r be a Gaussian integer that is a non-zero non-unit. Then r is irreducible in $\mathbb{Z}[i]$ if and only if its conjugate $\bar{r}$ is also irreducible.

Suppose that r is irreducible in $\mathbb{Z}[i]$. Since r is a non-zero non-unit, its only factorizations are trivial. In other words, if $r = xy$, either x or y is a unit. Recall that the units of $\mathbb{Z}[i]$ are ± 1 and $\pm i$ and the conjugate of r is given by $\bar{r} = \bar{x}\bar{y}$. Suppose that $r = xy$ and x is a unit. If $x = \pm 1$, then $\bar{x} = \pm 1$. If $x = i$, its conjugate is $\bar{x} = -i$, and if $x = -i$, its conjuagte is $\bar{x} = i$. In each case, $\bar{r} = \bar{x}\bar{y}$ only has trivial factorizations because $\bar{x}$ is always a unit. Therefore, $\bar{r}$ only has trivial factorzations and is thus irreducible in $\mathbb{Z}[i]$.

Suppose that $\bar{r}$ is irreducible in $\mathbb{Z}[i]$. Then the only factorizations of $\bar{r} = \bar{x}\bar{y}$ are trivial. Let $\bar{x}$ be a unit. Then $\bar{x} = \pm 1$ or $\pm i$. If $\bar{x} = \pm 1$, then its conjugate is $x = \pm 1$. If $\bar{x} = i$, then its conjugate is $x = -i$, and if $\bar{x} = -i$, then its conjugate is $x = i$. In each case, x is a unit, so the conjugate of $\bar{r}$, $r = xy$, only has trivial factorizations because x is always a unit. Therefore, r is irreducible in $\mathbb{Z}[i]$. $\square$

Exercise 16.6 Examine two rings in $\mathbb{Z}_m[i]$

First we will look at $\mathbb{Z}_2[i] = \{a + bi | a, b \in \mathbb{F}_2\}$. Observe that because there are only two elements of $\mathbb{F}_2$, and in the ring $\mathbb{F}_2$ $-1 = 1$, there are only four elements of $\mathbb{Z}_2[i]$: $0, 1, i, 1 + i$. Below are their addition and multiplication tables:

+	0	1	i	1+i
0	0	1	i	i+1
1	1	0	1+i	i
i	i	1+i	0	1
1+i	1+i	i	1	0

×	0	1	i	1+i
0	0	0	0	0
1	0	1	i	1+i
i	0	i	1	1+i
1+i	0	1+i	1+1	0

These tables show that $\mathbb{Z}_2[i]$ is a ring, but not a field because there is a zero divisor: $(1 + i)(1 + i) = 1 + 2i + i^2 = 1 - 1 = 0$. Notice also that $1 + i$ has no multiplicative inverse. Therefore, $\mathbb{Z}_2[i]$ is not a field.

Now, let's take a look at $\mathbb{Z}_3[i] = \{a + bi | a, b \in \mathbb{F}_3\}$. Since $\mathbb{F}_2$ has three elements, $\mathbb{Z}_3[i] = \{a+bi | a, b \in \mathbb{F}_3\}$ will have 9 elements: $0, 1, 2, i, 2i, 1+i, 1+2i, 2+i, 2+2i$. Below is their multiplication table:

×	0	1	2	i	2i	1+i	1+2i	2+i	2+2i
0	0	0	0	0	0	0	0	0	0
1	0	$\boxed{1}$	2	i	2i	1+i	1+2i	2+i	2+2i
2	0	2	$\boxed{1}$	2i	i	2+2i	2+i	1+2i	1+i
i	0	i	2i	2	$\boxed{1}$	2+i	1+i	2+2i	1+2i
2i	0	2i	i	$\boxed{1}$	2	1+i	2+2i	1+i	2+i
1+i	0	1+i	2+2i	2+i	1+i	2i	2	$\boxed{1}$	i
1+2i	0	1+2i	2+i	1+i	2+2i	2	i	2i	$\boxed{1}$
2+i	0	2+i	1+2i	2+2i	1+i	$\boxed{1}$	2i	i	2
2+2i	0	2+2i	1+i	1+2i	2+i	i	$\boxed{1}$	2	2i

Notice that there are no zero-divisors and each element has a multiplicative inverse. Therefore $\mathbb{Z}_3[i] = \{a + bi | a, b \in \mathbb{F}_3\}$ is a field.

Exercise 16.10 A prime number p is irreducible in $\mathbb{Z}[i]$ if and only if the polynomial $x^2 + 1$ is irreducible in $\mathbb{F}_p[x]$.

Suppose that a prime number p is irreducible in $\mathbb{Z}[i]$. By theorem 16.8, the ring $\mathbb{Z}_p[i]$ is a field if and only if p is irreducible in $\mathbb{Z}[i]$, therefore, $\mathbb{Z}_p[i]$ is a field. Using the same notation as the book, we will write $\mathbb{F}_p[i]$ for $\mathbb{Z}_p[i]$. Using theorem 16.10 in the textbook which states that $\mathbb{F}_p[x]_{x^2+1}$ is a field if and only if $\mathbb{F}_p[i]$ is a field, we may conclude that $\mathbb{F}_p[x]_{x^2+1}$ is also a field. By theorem 14.11, we may finally conclude that x^2+1 is irreducible in $\mathbb{F}_p[x]$ since $\mathbb{F}_p[x]_{x^2+1}$ is a field. Therefore, if p is irreducible in $\mathbb{Z}[i]$, $x^2 + 1$ is irreducible in $\mathbb{F}_p[x]$.

Now, suppose that $x^2 + 1$ is irreducible in $\mathbb{F}_p[x]$. Using the same logic as above, we can show that p is irreducible in $\mathbb{Z}[i]$. Because $x^2 + 1$ is irreducible in $\mathbb{F}_p[x]$, this makes $\mathbb{F}_p[x]_{x^2+1}$ a field. Theorem 16.10 states that if $\mathbb{F}_p[x]_{x^2+1}$ is a field, then so is $\mathbb{F}_p[x]$. Thus, we may conclude that $\mathbb{F}_p[x]$ is also a field. Similarly, theorem 16.8 states that if $\mathbb{F}_p[x] = \mathbb{Z}_p[x]$ is a field, then p must be irreducible in $\mathbb{Z}[i]$. Therefore, we have shown that if $x^2 + 1$ is irreducible in $\mathbb{F}_p[x]$, then p is irreducible in $\mathbb{Z}[i]$. $\square$

Exercise 2 Theorem 15.9 in the textbook states a version of the divison theorem for two Gaussian Integers a and b, where if we divide a into b, we find that $b = aq + r$ for Gaussian Integers q and r such that $N(r) < N(a)$. However, it does not state that q and r need be unique. We will show that the division theorem can be true for two different quotients and remainders in the Gaussian Integers.

Let $a = 2 - 4i$ and $b = 1 + 8i$. If $1 + 8i = (2 - 4i)(q) + r$ then we can compute $(1 + 8i)(2 - 4i)^{-1}$ to find q. Recall that the inverse of a Gaussian Integer is given by $\frac{\bar{\alpha}+\bar{\beta}}{\alpha^2+\beta^2}$. So $(2 - 4i)^{-1} = \frac{2+4i}{2^2+4^2}$.

$$\begin{aligned}(1 + 8i)(2 - 4i)^{-1} &= \tfrac{(1+8i)(2+4i)}{20} \\ \tfrac{-30}{20} + \tfrac{20i}{20}\end{aligned}$$

If $q = \alpha + \beta i$, we can pick $\alpha = -1$ and $\beta = 1$. Thus, $q = -1 + i$. To find r, we compute $1 + 8i - (2 - 4i)(-1 + i) = 1 + 8i - 2 - 6i$, therefore, $r = -1 + 2i$. One can compute and verify then that

$$1 + 8i = (-1 + i)(2 - 4i) + (-1 + 2i)$$

where $N(r) = 1^2 + 2^2 = 5 < N(a)$. While this is certainly true, we can also choose $q_1 = -2 + i$ and $r_1 = 1 - 2i$ and see that

$$1 + 8i = (-2 + i)(2 - 4i) + (1 - 2i)$$

where $N(r_1) = 1^2 + 2^2 = 5 < N(a)$ is true as well. Hence, the division theorem works for Gaussian Integers, but the quotient and remainder do not necessarily have to be unique. $\Box$.