Problem 3. (Lang) Show that the ring $\mathbb{Z}[i] = \{a + ib \colon a, b \in \mathbb{Z}\} \subset \mathbb{C}$ is a PID and hence a UFD. What are the units of that ring?

It will be shown that $\mathbb{Z}[i]$ is a Euclidean domain and from that it will immediately follow that $\mathbb{Z}[i]$ os a PIC because all Euclidean domains are also PIDs. Define the measure d to be $d(a + bi) = a^2 + b^2$.

Claim: For any $m, n \in \mathbb{Z}[i]$, $d(mn) = d(m)d(n)$.

Proof: Let $m = p + qi$ and $n = r + si$ for some $p, q, r, s \in \mathbb{Z}$.

$$\begin{aligned} d(mn) &= d((p + qi)(r + si)) \\ &= d(pr - qs + (ps + qr)i) \\ &= (pr - qs)^2 + (ps + qr)^2 \\ &= p^2r^2 - 2prqs + q^2s^2 + p^2s^2 + 2psqr + q^2r^2 \\ &= p^2r^2 + p^2s^2 + q^2r^2 + q^2s^2 \\ &= p^2(r^2 + s^2) + q^2(r^2 + s^2) \\ &= (p^2 + q^2)(r^2 + s^2) = d(m)d(n) \end{aligned}$$

Claim: For any $m, n \in \mathbb{Z}[i]$ where $n \neq 0$ there exist $e, f \in \mathbb{Z}[i]$ such that $m = ne + f$ where $f \geq 0$ and $d(f) < d(n)$.

Proof: If $n|m$ then $m = ne$ for some $e \in \mathbb{Z}[i]$ and the claim obviously holds. So we will only consider cases where $n \nmid y$.

Consider $\frac{m}{n} = \frac{p+qi}{r+si} = \frac{(p+qi)(r-si)}{(r+si)(r-si)} = \frac{1}{r^2+s^2}(pr - psi + qri + qs) = \frac{pr+qs}{r^2+s^2} + \frac{qr-ps}{r^2+s^2}i$. Let $u = \frac{pr+qs}{r^2+s^2}$ and $w = \frac{qr-ps}{r^2+s^2}$. It is clear that $u, w \in \mathbb{Q}$ and therefore $\frac{m}{n} = u + wi \in \mathbb{Q}[i]$.

Now let y be the nearest integer to u and z be the nearest integer to w. This means that $|z - w| \leq \frac{1}{2}$ and $|y - u| \leq \frac{1}{2}$ and it follows that:

$\frac{m}{n} = u + wi = (y - y + u) + (z - z + w)i = (y + zi) + ((u - y) + (w - z)i)$
$m = (y + zi)n + ((u - y) + (w - z)i)n$

Now since $y, z \in \mathbb{Z}$ it is clear that $y + zi \in \mathbb{Z}[i]$ and we can set $e = y + zi$. The term $((u - y) + (w - z)i)n$ also belongs to $\mathbb{Z}[i]$ because $((u - y) + (w - z)i)n = (u + wi)n + (-y - zi)n = \frac{m}{n}n + (-y - zi)n = m - en$. If we set $f = ((u - y) + (w - z)i)n$ then we can see that:

$d(f) = d((((u - y) + (w - z)i)n)) = d((u - y) + (w - z)i)d(n) = ((u - y)^2 + (w - z)^2)d(n) \leq (\frac{1}{2}^2 + \frac{1}{2}^2)d(n) = \frac{1}{2}d(n) < d(n)$ (since $d(n) > 0$)

Therefore $\mathbb{Z}[i]$ satisfies all the conditions of a Euclidean domain and is also a PID.$\square$

The units of the ring must satisfy $1 = aa^{-1} \Rightarrow d(1) = d(a)d(a^{-1}) \Rightarrow 1^2 = d(a)d(a^{-1}) \Rightarrow 1 = d(a)d(a^{-1})$. Since $d(a), d(a^{-1}) \in \mathbb{N}$, this means that the only possible value that $d(a)$ and $d(a^{-1})$ can have is 1. The only such $a \in \mathbb{Z}[i]$ that satisfy this are the pairs $\{1, 1\}$, $\{-1, -1\}$, and $\{i, -i\}$. Therefore the units of the ring $\mathbb{Z}[i]$ are $\{1, -1, i, -i\}$.