Problem A. Let $D > 0$ be a square-free$^1$ integer and consider the set $\mathbb{Z}[(\sqrt{-D})]$ of complex numbers of the form $a + b\sqrt{-D}$ with $a, b \in \mathbb{Z}$. (Note that when we write $\sqrt{-D}$ we mean $i\sqrt{D}$.)

(a) Check that $\mathbb{Z}[(\sqrt{-D})]$ is closed under addition and multiplication.

(b) Justify the formula below for the norm of $a + b\sqrt{-D}$:

$$N(a + b\sqrt{-D}) = |a + b\sqrt{-D}|^2 = a^2 + Db^2.$$  

(c) When $D > 1$ show that the only elements of $\mathbb{Z}[(\sqrt{-D})]$ whose multiplicative inverses lie in $\mathbb{Z}[(\sqrt{-D})]$ are $\{\pm 1\}$.

(d) For $D = 3$ there are two ways to factor 4 in $\mathbb{Z}[(\sqrt{-3})]$ – namely

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Verify that all the factors 2 and $1 \pm \sqrt{-3}$ are irreducible in $\mathbb{Z}[(\sqrt{-3})]$.

(e) Conclude that $\mathbb{Z}[(\sqrt{-3})]$ fails to have unique factorization into irreducibles.

---

$^1$I.e., a product of distinct primes; so no square $> 1$ divides it. We allow $D = 1.$