MA 638 - Section 8.3 Homework

1. Let $R = \mathbb{Z}[\sqrt{-n}]$ where n is a squarefree integer greater than 3.

(a) Prove that $2, \sqrt{-n}$, and $1+\sqrt{-n}$ are irreducibles in R.

(b) Prove that R is not a UFD. Conclude that the quadratic integer ring $\mathcal{O}$ is not a UFD for $D \equiv 2, 3 \pmod 4$, $D < -3$ (so also not an ED and not a PID). [Hint: Show that either $\sqrt{-n}$ or $1+\sqrt{-n}$ is not prime].

(c) Give an explicit ideal in R that is not principal.

(a) *Proof:* Suppose $2 = ab$ then $N(2) = 4 = N(a)N(b)$. Then $N(a)$ can only be 1, 2, or 4. If $N(a) = 1$ then a is a unit, and therefore there is nothing to prove. If $N(a) = 4$ then $N(b) = 1$ so b is a unit, and there is nothing to prove. So consider $N(a) = 2$. If $a = x + y\sqrt{-n} \in \mathbb{Z}[\sqrt{-n}]$ then $2 = x^2 + ny^2$. Now if $y \neq 0$ then $x^2 + ny^2 \geq n > 3$ and therefore this case is impossible, so $y = 0$. But then $x^2 = 2$ which has no solution in the integers, so this also is impossible. Hence $N(a) \neq 2$ and so 2 is irreducible.

Next suppose $\sqrt{-n} = ab$ so that $N(\sqrt{-n}) = n = N(a)N(b)$. If $a = x + y\sqrt{-n}$ and $b = w + z\sqrt{-n}$ then

$$N(a)N(b) = (x^2 + ny^2)(w^2 + nz^2)$$

$$= n$$

$$= (xw)^2 + n([xz]^2 + [yw]^2) + n^2(yz)^2.$$

Now if $yz > 0$ then $N(a)N(b) \geq n^2 > n$ which is impossible, so either y or z is zero. Without loss of generality suppose $y = 0$. But then $a = x$ is just an integer, and then $ab = x(w + z\sqrt{-n}) = \sqrt{-n}$. Therefore $xw = 0$ and $xz = 1$. The latter requires $x = \pm 1$ since no other number can divide 1 in $\mathbb{Z}$ and therefore a is a unit. So $\sqrt{-n}$ is irreducible.

(b) *Proof:* Suppose that $D = -n$ is congruent to 2 mod 4. We will show that $\sqrt{-n}$ is not prime in $\mathbb{Z}[\sqrt{-n}]$. First note that in this case n is even, since $-n = 2 + 4k = 2(1 + 2k)$ for some integer k. So let $n = 2m$.

We will use the fact that an element is prime if and only if it generates a prime ideal. So it suffices to show that $(\sqrt{-n})$ is not prime. First note that $n = (-\sqrt{-n})\sqrt{-n}$ so that $2m = n \in (\sqrt{-n})$. However, $2 \notin (\sqrt{-n})$ since if it were, $2 = a\sqrt{-n}$ for some a but then $N(2) = 4 = N(\sqrt{-n})N(a) = nN(a)$. However, $n > 3$ would entail that $N(a) = 1$ and then $\sqrt{-n} = \pm 2$ which is impossible. Also we have that $m \notin (\sqrt{-n})$ for if $m = a\sqrt{-n}$ then $2m = n = 2a\sqrt{-n}$. From this it would follow that $n^2 = 2an$ and so $n^2 - 2an = 0$ so that

$$n(n - 2a) = 0 \quad \Rightarrow$$

$$n = 2a = 2m \quad \Rightarrow$$

$$a = m$$

But then $a = a\sqrt{-n}$ so that $n = 1$ which contradicts $n > 3$. Hence $(\sqrt{-n})$ is not a prime ideal and therefore $\sqrt{-n}$ is not prime. Since $\mathcal{O}$ then has some irreducible element that is not prime, it must not be a UFD.

Next consider $D = -n$ is congruent to 3 mod 4 so that $-n = 3 + 4k$ for some k. Then we show that $1 + \sqrt{-n}$ is not prime. First note that because $(1 + \sqrt{-n})(1 - \sqrt{-n}) = 1 - n \in (1 + \sqrt{-n})$ then therefore $1 + 3 + 4k = 4(k + 1) \in (1 + \sqrt{-n})$. However $4 \notin (1 + \sqrt{-n})$ because if it were and $4 = a(1 + \sqrt{-n})$ then we would have $N(4) = 16 = N(a)(1 + n)$. Now since $n > 3$ and since n is squarefree, then also $n \neq 4$ so that in fact $n \geq 5$. For $N(a)(1 + n)$ to have exactly 4 factors of 2, we must have $1 + n$ equal to either 8 or 16. If $1 + n = 8$ so that $n = 7$ then $4 = a(1 + \sqrt{-7})$. If we call $a = x + y\sqrt{-7}$ then

$$4 = (x + y\sqrt{-7})(1 + \sqrt{-7}) = (x - 7y) + (x + y)\sqrt{-7} \quad \Rightarrow$$

$$\begin{aligned} 4 &= x - 7y \quad \text{and} \\ 0 &= x + y \end{aligned}$$

But this implies $x = -y$ and therefore $4 = -y - 7y = -8y$ which is not true for any integer y.

On the other hand we also have $k + 1 \notin (1 + \sqrt{-n})$ since then $4(k + 1) = 1 - n = 4a(1 + \sqrt{-n})$ so that