31.1. Basics: Let $d \in \mathbb{Z}$ be a square-free integer (i.e., $p^2 \nmid d$ for all primes p). Then $F = \mathbb{Q}(\sqrt{d})$ is a *quadratic field*.
The *discriminant* of F is

$$\Delta = \begin{cases} d & \text{if } d \equiv 1 \mod 4 \\ 4d & \text{otherwise} \end{cases}$$

The *ring of integers* of F is

$$D = \mathbb{Z}[\theta] \text{ where } \theta = \begin{cases} (1+\sqrt{d})/2 & \text{if } d \equiv 1 \mod 4 \\ \sqrt{d} & \text{otherwise} \end{cases}$$

Write $\overline{\theta} = -\sqrt{d}$ or $(1-\sqrt{d})/2$.
The minimal polynomial of θ is

$$f_d(x) = (x-\theta)(x-\overline{\theta})$$

which is $x^2 - x + (1-d)/4$ if $d \equiv 1 \mod 4$ or $x^2 - d$.

Definition 31.2. For $\alpha, \beta \in D$ write $(\alpha, \beta) = (\alpha) + (\beta) = \{\alpha\gamma_1 + \beta\gamma_2 : \gamma_1, \gamma_2 \in D\}$.

Lemma 31.3. Every prime ideal $I \neq D$ in D can be written as $(p, b + c\theta)$ where $p \in \mathbb{N}$ is prime, $b, c \in \mathbb{Z}$, $c \mid p$, $0 \leq |b| < p$.

Proof: $I \cap \mathbb{Z}$ is an ideal of $\mathbb{Z}$, so is equal to (p) for some $p \in \mathbb{N}$, and I prime implies p is prime.
We have $(p) \subseteq I$. If $I = (p)$ then $I = (p, 0 + p\theta)$, so suppose $(p) \subsetneq I \subsetneq D$.
Note that $D/(p) \cong \{u + v\theta : 0 \leq u, v < p\} \cong (\mathbb{Z}/p\mathbb{Z})^2$ as additive groups. The quotient $I/(p)$ is isomorphic as a group to a proper non-trivial subgroup of $(\mathbb{Z}/p\mathbb{Z})^2$. Such a subgroup is isomorphic to $(\mathbb{Z}/p\mathbb{Z})$ and so generated by some $u + v\theta$. Multiplying by $v^{-1} \mod p$ we can assume it is generated by $b + \theta$ for some $0 \leq b < p$. Hence $I = (p, b + \theta)$. □

Definition 31.4. An ideal $I = (a, b + c\theta)$ is in *standard form* if $a, b, c \in \mathbb{Z}$, $I \cap \mathbb{Z} = (a)$, $0 < a, c$, $c \mid a$, $0 \leq |b| < a$.

Exercise 31.5. Let p be a prime. Then $I = (p, b + c\theta)$ is a prime ideal in standard form if and only if $p \mid N_F(b + c\theta)$.
If I is in standard form show that $p^a \mid c$ implies $p^a \mid b$. Hence, show that $c \mid b$. Hence, $I = (c)(a/c, b/c + \theta)$.

Definition 31.6. Let I and J be ideals of D. Write $I \mid J$ if $J \subseteq I$.

Theorem 31.7. (Dedekind) Let $p \in \mathbb{N}$ be a prime. Then the proper ideals $I \mid (p)$ are as follows.

- If $f_d(x)$ is irreducible modulo p then $I = (p)$.
- If $f_d(x) \equiv (x+u)(x+v) \mod p$ then $I = (p, u + \theta)$ or $(p, v + \theta)$.

These are prime ideals.

Definition 31.8. The *norm* of an ideal I is $\#(D/I)$.

Lemma 31.9.

(1) If $I = (a, b + c\theta)$ is in standard form then $N(I) = ac$.
(2) If I and J are ideals such that $I \subseteq J$ and $N(I) = N(J)$ then $I = J$.
(3) For $\alpha \in D$ we have $N((\alpha)) = |N_F(\alpha)|$ (see Corollary 5.10 of Stewart and Tall).

Example 31.10. We show that $I = (111, 5 + 7i)$ is principal and equal to $(6 + i)$, which gives a complete answer to Question 1 of Assignment 3.
First, $I \cap \mathbb{Z}$ contains $\gcd(111, N_F(5 + 7i)) = 37$ which is prime, so either $I \cap \mathbb{Z}$ is (1) or (37). In any case $(37) \subseteq I$. Also, $5 + 7i \notin (37)$ as it is not of the form $37u + i37v$. Hence, $I \neq (37)$. and so $N(I) = 1$ or 37.
Now $111 = (6 + i)3(6 - i)$ and $5 + 7i = (6 + i)(1 + i)$. Hence $I \subseteq (6 + i)$ and so $I \neq (1)$. Finally, $N_F(6 + i) = 37$ so $N(I) = N((6 + i))$ and so $I = (6 + i)$.