8.3.3. We factor $N$ into elements of $\mathbb{Z}[i]$ by factoring each of the prime factors: $N = (4 + 1)^2(4 - 1)^2(8 + 3i)(8 - 3i)(10 + i)(10 - i)$. Note that writing $N$ in the form $a^2 + b^2$ is equivalent to writing $N$ as the norm of some $a + bi \in \mathbb{Z}[i]$. Therefore we obtain the following possibilities: $N = (4 + 1)^x(4 - 1)^x(8 + 3i)^y(8 - 3i)^y(10 + i)^z(10 - i)^z$ where $(x, x') \in \{(1, 0), (1, 1), (0, 1)\}$, $(y, y') \in \{(1, 0), (0, 1)\}$, $(z, z') \in \{(1, 0), (0, 1)\}$. (Note that these give exactly 48 possibilities, and by a corollary in the book, $N$ has $4 \times 2 \times 2 = 8$ representations as all its prime factors equal 1 modulo 4. Thus these indeed cover all possible cases.) Direct computations yield the following (not ordered) pairs: $(851, 1186)$, $(994, 1069)$, $(334, 1421)$, $(46, 1459)$, $(646, 1309)$, $(374, 1411)$.

8.3.6. (a) By computing the norm we know $1+i$ is irreducible in $\mathbb{Z}[i]$, so $\mathbb{Z}[i]/(1+i)$ is indeed a field. Any element in $\mathbb{Z}[i]$ has the form $a+bi$ for some $a, b \in \mathbb{Z}$. If $a \equiv b \mod 2$, then $(1+i)(a+bi) = a+bi$, so $a+bi = \overline{0}$ in the quotient field. If $a \not\equiv b \mod 2$, then $a - b \equiv b \mod 2$, in which case by a similar computation we have $(a+bi) - 1 = \overline{0}$ in the quotient field. Thus the only elements in the quotient field is $\overline{0}$ and $\overline{1}$, so we obtain a finite field of order 2.

(b) Since $q \equiv 3 \mod 4$, it is irreducible in $\mathbb{Z}[i]$ and hence the quotient is a field. It remains to show that $\mathbb{Z}[i]/(q) = \{a+bi \mid 0 \leq a, b \leq q-1\}$. For any $x + yi \in \mathbb{Z}[i]/(q)$, there exist $a, b \in \{0, 1, \ldots, q-1\}$ and $x', y' \in \mathbb{Z}$ such that $x = x' + a, y = y' + b$, then $x + yi = q(x' + yi') + a + bi = a + bi$. Clearly, for any $a, b \in \{0, 1, \ldots, q-1\}$, $\overline{a+bi} \in \mathbb{Z}[i]/(q)$, so $\mathbb{Z}[i]/(q)$ is a field of order $q^2$.

(c) Note that $\pi$ and $\overline{\pi}$ are both irreducible, so $\mathbb{Z}[i]/(\pi)$ and $\mathbb{Z}[i]/(\overline{\pi})$ are fields. I claim that $(\pi, \overline{\pi}) = 1$. Let $d = \gcd(\pi, \overline{\pi})$ then we can write $\pi = da, \overline{\pi} = db$ for some $a, b \in \mathbb{Z}[i]$. If $d$ is not a unit, then $x$ and $y$ are both units since $\pi, \overline{\pi}$ are not associates. Thus $\pi = ab^{-1}\overline{\pi}$, a contradiction. Thus $d$ is a unit and $(\pi, \overline{\pi}) = 1$. By the CRT, we get $\mathbb{Z}[i]/(p) \cong \mathbb{Z}[i]/(\pi) \times \mathbb{Z}[i]/(\overline{\pi})$.

Now, by a similar argument to part (b), we know that $\mathbb{Z}[i]/(p)$ as a set has $p^2$ elements. Since $\pi$ and $\overline{\pi}$ are proper ideals, the corresponding quotients are nontrivial fields, so each of them must have exactly $p$ elements.

9.4.11. If $x^2 + y^2 - 1$ is reducible in $\mathbb{Q}[x, y]$, then in particular it would be reducible over $\mathbb{Q}[y]$. We show that it is in fact irreducible over $\mathbb{Q}[y]$. Note that $\mathbb{Q}[y]$ is a UFD since $\mathbb{Q}$ is. Clearly, $(1 + y)$ is a prime ideal in $\mathbb{Q}[y]$. Then $x^2 + y^2 - 1 = x^2 + (y + 1)(y - 1)$ is irreducible by the Eisenstein criterion applies w.r.t. $p = (y + 1)$.

9.4.13. By the rational root theorem, the only possible rational roots of $p(x)$ are $\pm 1$ and $\pm 2$. 

February 6, 2017

Luciena Xiao
Computation shows that $p(1) = 0 \Rightarrow n = -3$, $p(-1) = 0 \Rightarrow n = -1$, $p(2) = 0 \Rightarrow n = -5$, $p(-2) = 0 \Rightarrow n = -3$. Since $p(x)$ has no other integral roots, we conclude $p(x)$ is irreducible for $n \neq 1, -3, -5$.

9.5.1. Since $F$ is a field, $F[x]$ is a UFD, so we can write $f(x) = \prod_{i=1}^{n} f_i(x)^{k_i}$ for irreducible polynomials $f_i \in F[x]$. Claim: $N = \mathcal{N}(F[x]/(f(x))) = (\prod_{i=1}^{n} f_i(x))/(f(x))$.

Proof of claim: Let $g \in N$, then $g$ is of the form $h(x) + (f(x))$ for some $h(x) \in F[x]$. Then $h^m(x) \in (f(x))$ for some $n$ since $g$ is nilpotent, $f|h$. In particular, $f_i|h$ for any $f_i$, so $h \in \prod_{i=1}^{n} f_i(x)$, i.e. $g \in (\prod_{i=1}^{n} f_i(x))/(f(x))$. On the other hand, for any $g \in \prod_{i=1}^{n} f_i(x)$, we have $g^m \in (f(x))$ where $m = \max\{k_1, \cdots, k_n\}$, so $g$ becomes nilpotent in $F[x]/(f(x))$. Thus we conclude equality.

9.5.3. Note that $\mathbb{Z}[i]$ is a UFD. If $p \equiv 3 \mod 4$ then $p$ is irreducible in $\mathbb{Z}[i]$, so by Eisenstein’s criterion $x^n - p$ is irreducible. If $p \equiv 1 \mod 4$, then $p = (a + bi)(a - bi) \in \mathbb{Z}[i]$ for some irreducibles $a + bi$ and $a - bi$; then by the same reason $x^n - p$ is irreducible.

**Additional Problem.** Let $f \in \mathbb{R}[x]$ be a polynomial. By the fundamental theorem of algebra, complex roots of $f$ must appear in conjugate pairs. If $f$ has odd degree, then it must have at least one real root, which implies $f$ has a linear factor in $\mathbb{R}[x]$; hence $f$ is irreducible if and only if $\deg(f) = 1$. If $f$ has even degree, then each pair of linear factors over $\mathbb{C}[x]$ corresponding to a conjugate pair of root will multiply to an element in $\mathbb{R}[x]$, so $f$ has a factor of degree 2 in $\mathbb{R}[x]$; thus $f$ is irreducible if and only if $\deg(f) = 2$. In conclusion, irreducible polynomials over $\mathbb{R}$ are either linear or quadratic.