1. A loose end from class.

(a) Let $p$ be an odd prime and let $a \in \mathbb{Z}$ such that $\gcd(a,p) = 1$. Show that if $a$ is a quadratic residue mod $p$, then $a$ is a quadratic residue mod $p^n$ for any positive integer $n$. (Note: you already had to show this on the previous homework for §3.1, #24.)

(b) To handle the case when $(a,p) \neq 1$, solve Sec 3.3, #12 in the book.

(c) Using CRT and the first part of this problem, conclude that if $m$ is odd and $\gcd(a,m) = 1$, then $a$ is a quadratic residue mod $m$ if and only if $a$ is a quadratic residue mod $p$ for every prime $p$ dividing $m$.

(d) Using CRT and the first two parts of this problem prove the following. Let $m$ be odd and let $a \in \mathbb{Z}$. Prove that the congruence $x^2 \equiv a \pmod{m}$ has a solution if and only if for each prime $p$ dividing $m$, one of the following conditions holds, where $p^\alpha \mid m$ and $p^\beta \mid a$ (this means that $p^\alpha$ is the largest power of $p$ dividing $m$ and similarly for $p^\beta$ and $a$):

- $\beta \geq \alpha$
- $\beta < \alpha$, $\beta$ is even, and $a/p^\beta$ is a quadratic residue mod $p$.

2. Sec 3.3, #14, #17.

3. Let $d$ be a fundamental discriminant. Over a series of steps, we are going to prove the result stated in class, that $(N(I)) = I\overline{I}$ for an ideal $I$ of $\mathcal{O}_d$.

(a) Let $\mathbb{Q}(\sqrt{d}) = \{ a + b\sqrt{d} : a,b \in \mathbb{Q} \}$. Show that $\mathbb{Q}(\sqrt{d})$ is a field. (Just show that there are multiplicative inverses for nonzero elements; the other field properties are obvious.)

(b) A number $\alpha \in \mathbb{C}$ is called algebraic if it satisfies a nonzero polynomial with rational coefficients. The minimal polynomial $f(x)$ of an algebraic number $\alpha \in \mathbb{C}$ is the monic polynomial of smallest degree, with coefficients in $\mathbb{Q}$, such that $f(\alpha) = 0$. What is the minimal polynomial of $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$? (Note: there are two cases, $b = 0$, and $b \neq 0$.)

(c) Show that if a rational number $a \in \mathbb{Q}$ satisfies a monic polynomial with integer coefficients, then in fact $a \in \mathbb{Z}$.

(d) (Quite difficult and therefore optional.) An element $\alpha \in \mathbb{C}$ is called an algebraic integer if the coefficients of its minimal polynomial $f(x)$ lie in $\mathbb{Z}$. Generalizing part (3c), show that if $\alpha \in \mathbb{C}$ satisfies a monic polynomial with integer coefficients, then in fact $\alpha$ is an algebraic integer. We won’t need this, but it is a very important fact.
(e) Show that the set of algebraic integers in $\mathbb{Q}(\sqrt{d})$ is equal to the ring defined in class,

$$\mathcal{O}_d = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \text{ is even} \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \text{ is odd.} \end{cases}$$

(f) Recall that conjugation is defined by $a + b\sqrt{d} = a - b\sqrt{d}$. Let $I$ be an ideal of $\mathcal{O}_d$. Show that $\overline{I} = \{ \overline{x} : x \in I \}$ is also an ideal of $\mathcal{O}_d$.

(g) Recall that $N(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 \in \mathbb{Z}$. Let $N(I)$ be the greatest common divisor in $\mathbb{Z}$ of $N(x)$ for all $x \in I$. Since $N(x) \in \overline{I}$ for $x \in I$, it is clear that $(N(I)) \subseteq \overline{I}$. Hence to prove that $(N(I)) = \overline{I}$, we have to prove the reverse inclusion. Thus, let $\alpha, \beta \in I$; we will prove that $\alpha \beta \in (N(I))$ as follows. First, prove that the polynomial

$$f(x) = x^2 - (\alpha \overline{\beta} + \overline{\alpha} \beta)x + \alpha \overline{\alpha} \beta \overline{\beta}$$

has coefficients in $\mathbb{Z}$, and that $\alpha \overline{\beta}$ is a root. Second, using the fact that $N(I)$ divides the integers $N(\alpha + \beta)$, $N(\alpha)$, and $N(\beta)$, prove that $N(I)$ divides the coefficient of $x$ in $f(x)$, and that $N(I)^2$ divides the constant coefficient. Conclude that the polynomial

$$g(x) = \frac{1}{N(I)^2} f(x \cdot N(I))$$

is a monic polynomial in $\mathbb{Z}[x]$, and note that the element $\alpha \overline{\beta} / N(I)$ is a root. Now consider two cases: either $\alpha \overline{\beta}$ is a rational number, in which case we can conclude it is an integer by part (3c). Otherwise, $g(x)$ is the minimal polynomial of $\alpha \overline{\beta} / N(I)$, and hence this number is an algebraic integer. Therefore it lies in $\mathcal{O}_d$ by part (3e). In either case, $\alpha \overline{\beta} / N(I) \in \mathcal{O}_d$, so $\alpha \overline{\beta} \in (N(I))$ as desired.