1. (a) That $d$ is a quadratic residue (mod $p$) says, in symbols, $d \equiv x^2 \pmod{p}$ for some $x$. Hence, $p$ divides $x^2 - d \cdot 1^2$. Hence $p$ divides $(x + \sqrt{d})(x - \sqrt{d})$. We don’t necessarily have unique factorization of elements in $R$, but because it’s the ring of integers of a number field, we do have unique factorization of ideals in $R$. That $p$ divides $(x + \sqrt{d})(x - \sqrt{d})$ implies that the (principal) ideal $(p)$ divides the product of the (principal) ideals $(x + \sqrt{d})(x - \sqrt{d})$. If $(p)$ were prime, then it would divide one factor or the other, but at least as long as $p \neq 2$, it’s clear that as elements $p$ doesn’t divide either of those generators. (Do you see why 2 actually could divide one of those generators?)

(b) The idea here is sort of similar to some of the ideas in Problem Set 7, problem 2d. There we calculated that the norm of an element divided $p^2$ and was not 1, and hence must be $p$. We could have concluded from there that the element was prime (as long as we were in a unique factorization domain, which we were). If you do something similar for ideals, using the concept of norm from problem 6 below, you get that the norm of $(x + y\sqrt{d}, p)$ strictly divides the norm of $(p)$, which is $p^2$. Our ideal does not have norm 1 because it is not the whole ring because it contains only elements of norm divisible by $p$. Hence our ideal has norm $p$, and hence is prime. The part which maybe makes this problem too hard is that I don’t think the assertion is obvious that if the ideal $I$ divides the ideal $J$ then the norm of $I$ divides norm of $J$.

(c) Assume to the contrary that $(p)$ is not prime, and say $(x + y\sqrt{d})(z + w\sqrt{d}) \in (p)$ with neither element in $(p)$. Considering the norm on elements (where the first term has norm $x^2 - dy^2$), we have that one of the terms has norm divisible by $p$. Say $p$ divides $x^2 - dy^2$. If $p$ divides $y$ then $p$ also has to divide $x$, which contradicts that our element is not in $(p)$. So $p$ does not divide $y$. We can then find $z$ such that $yz \equiv 1 \pmod{p}$, and then $d \equiv (xz)^2 \pmod{p}$, which contradicts that $d$ is not a quadratic residue.

2. We know that

$$\left( \frac{6}{p} \right) = \left( \frac{2}{p} \right) \left( \frac{3}{p} \right) = (-1)^{(p^2-1)/8} \left( \frac{p}{3} \right) (-1)^{(p-1)(3-1)/4} = (-1)^{(p^2-1)/8} \left( \frac{p}{3} \right) (-1)^{(p-1)/2}$$

So we see that whether 6 is a square mod $p$ depends on the values $p \pmod{8}$ and $p \pmod{3}$ (and $p \pmod{4}$, but that is subsumed by $p$’s value mod 8).
2 SOLUTIONS TO THE EXTRA PROBLEMS (FIRST DRAFT)

\[ p \equiv 1 \pmod{3}, p \equiv 1 \pmod{8} \Rightarrow \left( \frac{6}{p} \right) = 1 \ast 1 \ast 1 = 1 \]

\[ p \equiv 1 \pmod{3}, p \equiv 3 \pmod{8} \Rightarrow \left( \frac{6}{p} \right) = 1 \]

\[ p \equiv 1 \pmod{3}, p \equiv 5 \pmod{8} \Rightarrow \left( \frac{6}{p} \right) = -1 \]

\[ p \equiv 1 \pmod{3}, p \equiv 7 \pmod{8} \Rightarrow \left( \frac{6}{p} \right) = -1 \]

\[ p \equiv 2 \pmod{3}, p \equiv 1 \pmod{8} \Rightarrow \left( \frac{6}{p} \right) = -1 \]

\[ p \equiv 2 \pmod{3}, p \equiv 3 \pmod{8} \Rightarrow \left( \frac{6}{p} \right) = -1 \]

\[ p \equiv 2 \pmod{3}, p \equiv 5 \pmod{8} \Rightarrow \left( \frac{6}{p} \right) = 1 \]

\[ p \equiv 2 \pmod{3}, p \equiv 7 \pmod{8} \Rightarrow \left( \frac{6}{p} \right) = 1. \]

By the Chinese Remainder Theorem, each equivalence mod 3 and mod 8 leads to an equivalence mod 24. The result is that 6 is a quadratic residue mod p for primes p congruent to 1, 19, 5, 23 (mod 24), and 6 is not a quadratic residue mod p for primes p congruent to 13, 7, 17, 11 (mod 24).

3. Let’s first show uniqueness. If an ideal contains \((p)\) and \((q)\), with \(p, q\) distinct, ordinary prime numbers, then it contains 1 also, because by the Euclidean algorithm 1 can be written as a linear combination of them.

The key for existence is to note that we can factor the ideal \((N)\) as \((p_1)^{a_1} \cdots (p_n)^{a_n}\), where \(N = p_1^{a_1} \cdots p_n^{a_n}\). So a prime ideal dividing \((N)\) must divide one of the principal ideals \((p_i)\), and that is the same as to say it must contain one of the principal ideals \((p_i)\).

4. We just saw in problem 3 that every prime ideal divides some ideal \((p)\). So, to find all the prime ideals in \(\mathbb{Z}[(\sqrt{6})]\), it will suffice to factor all of the ideals \((p)\). We know that if 6 is a square modulo \(p\) (for \(p \neq 2, 3\)), then the ideal is not prime, and we even know how to factor it, as

\[ (p) = (x + \sqrt{6}, p)(x - \sqrt{6}, p) \]

, with \(x\) such that \(x^2 \equiv 6 \pmod{p}\). This is a prime factorization by 1b. If 6 is not a square modulo \(p\), then \((p)\) is already prime.

The cases \(p = 2\) and \(p = 3\) remain. The ideal \((2)\) is not prime; it factors as \((2 + \sqrt{6}, 2)(2 - \sqrt{6}, 2)\). Nor is the ideal \((3)\) prime; it factors as \((3 + \sqrt{6}, 3)(3 - \sqrt{6}, 3)\). In both cases, the two given ideals are the same, for instance,

\[ 2 - \sqrt{6} = -1 \ast (2 + \sqrt{6}) + 2 \ast 2. \]
So the ideals (2) and (3) should actually be thought of as squares: 

\[ (2) = (\sqrt{6}, 2)^2 \]

and 

\[ (3) = (\sqrt{6}, 3)^2. \]

In summary, the prime ideals of \( \mathbb{Z}[\sqrt{6}] \) are:

- \((p)\) for prime \( p \equiv 7, 11, 13, 17 \pmod{24} \).
- \((x + \sqrt{6}, p)\) and \((x - \sqrt{6}, p)\) for \( p \equiv 1, 5, 19, 23 \pmod{24} \) and \( x \) such that \( x^2 \equiv 6 \pmod{p} \). (Note that, though each appropriate prime \( p \) yields a different pair of prime ideals, conversely, by unique factorization of \( (p) \), different appropriate choices of \( x \) must yield the same pair of prime ideals.)
- \((\sqrt{6}, 3)\) and \((\sqrt{6}, 2)\).

5. (a) If \( d \equiv 1 \pmod{4} \), we can take \( \alpha_1 = 1 \) and \( \alpha_2 = \frac{1 + \sqrt{d}}{2} \). Otherwise we take 1 and \( \sqrt{d} \).

6. (a) \( \beta_1 = 1 \ast (x + y\sqrt{d}) \) and \( \beta_2 = \sqrt{d}(x + y\sqrt{d}) = yd + x\sqrt{d} \). So we are reduced to calculating the determinant of the matrix

\[
\begin{pmatrix}
 x & yd \\
 y & x
\end{pmatrix}
\]

7. 

\[
\frac{a_0}{\alpha} = (-1)(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1),
\]

and since the right hand side is a linear combination of elements in the ring of algebraic integers, the left hand side is also in the ring of algebraic integers.