1. (This question is not terribly important for our purposes, but you should be aware of its assertions.) Let $K/k$ be a finitely generated extension of fields.
    (i) Prove that every intermediate extension is finitely generated over $k$.
    (ii) Give a finitely generated $k$-algebra containing a $k$-subalgebra that is not finitely generated.
    (iii) Prove that if $K/k$ admits a separating transcendence basis, then $K \otimes_k k'$ is a domain (and hence a field) for any purely inseparable algebraic extension $k'/k$. Deduce that if $k = \mathbf{F}_p(X,Y)$ and $K$ is the fraction field of $k[U,V]/(U^p - XV^p - Y)$ (why is this a domain?), then $K/k$ does not admit a separating transcendence basis (extra credit: Show that $k$ is algebraically closed in $K$ in this example, so the example is “geometric.”)

2. Let $p$ be a positive prime in $\mathbf{Z}$.
    (i) Prove that if $p \equiv 3 \mod 4$ then $p$ remains prime in $\mathbf{Z}[i]$.
    (ii) Assume $p \equiv 1 \mod 4$. Using cyclicity of $\mathbf{F}_p^\times$, deduce that $-1$ is a square in $\mathbf{F}_p^\times$ and hence $p|(x^2 + 1)$ in $\mathbf{Z}$ for some $x \in \mathbf{Z}$.
    (iii) For any nonzero $n \in \mathbf{Z}$, show that the elements $n + i, n - i \in \mathbf{Z}[i]$ are not divisible (in $\mathbf{Z}[i]$) by an element of $\mathbf{O}$ not in $\mathbf{O}^\times$. Conclude via (ii) and the UFD property of $\mathbf{Z}[i]$ that if $p \equiv 1 \mod 4$ then $p$ cannot be irreducible in $\mathbf{Z}[i]$.
    (iv) Assume $p \equiv 1 \mod 4$. Use norms and (iii) to prove that $p = \pi \overline{\pi}$ for an irreducible $\pi \in \mathbf{Z}[i]$ (with $\pi \not\in \mathbf{Z}$) that must have norm $p$, and infer that $p = a^2 + b^2$ for nonzero integers $a, b \in \mathbf{Z}$ that are unique up to ordering and signs.
    (v) Extra credit: Prove that $\mathbf{Z}[[1 + \sqrt{-3}]/2]$ is Euclidean, and use arithmetic in this ring to study representability of primes in the form $a^2 - ab + b^2$, including uniqueness aspects.

3. Let $d \in \mathbf{Z}$ be a nonzero squarefree integer with $d > 1$. Let $K = \mathbf{Q}(\sqrt{d})$ and let $\mathcal{O}$ be its ring of integers. Let us grant Dirichlet’s unit theorem, so $\mathcal{O}^\times/\{\pm 1\}$ is infinite cyclic. A fundamental unit of $K$ is a unit $\varepsilon \in \mathcal{O}^\times$ such that it reduces to a generator in $\mathcal{O}^\times/\{\pm 1\}$ (so the fundamental units are $\pm \varepsilon$ and $\pm 1/\varepsilon$). If an embedding $K \hookrightarrow \mathbf{R}$ is chosen, then the unique fundamental unit $> 1$ is often called “the” fundamental unit (relative to the chosen embedding). There is a close relationship between Pell’s equation and fundamental units, as you will work out below, but some care is required because a fundamental unit may have norm $-1$ and (if $d \equiv 1 \mod 4$) may not even lie in $\mathbf{Z}[\sqrt{d}]$.
    (i) Find a quadratic field for which the ring of integers is $\mathbf{Z}[\sqrt{d}]$ and there is a unit with norm $-1$ (so the fundamental unit has norm $-1$, whatever it may be). Note that no such example is possible if $d \equiv 3 \mod 4$, or more generally if $d$ is not a square modulo $4$. Explain the relationship between fundamental units and Pell’s equation when $d \equiv 2, 3 \mod 4$; in particular, derive the classical structure of the solution set to Pell’s equation by using the unit theorem. Upon embedding $K$ into $\mathbf{R}$, prove that “the” fundamental unit (or its square when the fundamental unit has norm $-1$) corresponds to the solution $(x, y)$ to Pell’s equation with small $y$-coordinate. (As best I can tell, for $d \equiv 2 \mod 4$ the only way to determine if there exists a fundamental unit with norm $-1$ is to grind out the continued fraction of $\sqrt{d}$ in accordance with (iii) below.)
    (ii) Find $d \equiv 1 \mod 4$ such that the fundamental unit in $\mathcal{O}_K = \mathbf{Z}[(1 + \sqrt{d})/2]$ does not lie in $\mathbf{Z}[\sqrt{d}]$, and prove in general that if $\alpha \in \mathcal{O}_K$ does not lie in $\mathbf{Z}[\sqrt{d}]$ then $\alpha^2 \not\in \mathbf{Z}[\sqrt{d}]$! However, this is about as bad as it gets. Construct an isomorphism
    $$\mathcal{O}_K \simeq \mathbf{Z}[X]/(X^2 - X + (1 - d)/4)$$
    and use this to infer that $\mathcal{O}_K/2\mathcal{O}_K \simeq \mathbf{F}_4$ (resp. $\mathcal{O}_K/2\mathcal{O}_K \simeq \mathbf{F}_2 \times \mathbf{F}_2$) when $d \equiv 5 \mod 8$ (resp. $d \equiv 1 \mod 8$).
    Since $\mathbf{Z}[\sqrt{d}] = \mathbf{Z} + 2\mathcal{O}_K$, conclude via inspecting the structure of $(\mathcal{O}_K/2\mathcal{O}_K)^\times$ that if $d \equiv 1 \mod 8$ then a fundamental unit of $\mathcal{O}_K$ must lie in $\mathbf{Z}[\sqrt{d}]$, and that if $d \equiv 5 \mod 8$ then the cube of any unit must lie in $\mathbf{Z}[\sqrt{d}]$. Upon embedding $K$ into $\mathbf{R}$, use the unit theorem to deduce the classical structure of the solution set to Pell’s equation for $d \equiv 1 \mod 4$, and relate “the” fundamental unit (or its square or cube or sixth power) to the “minimal” solution to Pell’s equation.
(iii) Formulate variants of Pell’s equation (of the form $x^2 - dy^2 = k$) whose solvability in $\mathbb{Z}$ (with $y \neq 0$) is equivalent to the fundamental unit having norm $-1$, or not lying in $\mathbb{Z}[\sqrt{d}]$ (for $d \equiv 1 \pmod{4}$), or both.

4. A number field $K$ is **totally real** if all embeddings of $K$ into $\mathbb{C}$ have image contained in $\mathbb{R}$, and $K$ is **totally imaginary** if $K$ has no embeddings into $\mathbb{R}$. The field $K$ is a **CM field** if it is a totally imaginary extension of a totally real subfield $K_0$ with $[K : K_0] = 2$. (CM fields first arose in the study of abelian varieties with “complex multiplication,” hence the terminology.)

(i) Give necessary and sufficient conditions for $K$ to be totally real (resp. totally imaginary) in terms of the structure of the $\mathbb{R}$-algebra $K \otimes_{\mathbb{Q}} \mathbb{R}$.

(ii) If $K$ is a CM field, prove that for all embeddings $\iota : K \hookrightarrow \mathbb{C}$, the action of complex conjugation preserves $\iota(K)$ and hence induces an involution on $K$. Prove that this involution is independent of $\iota$, and so $K$ admits an *intrinsic* “complex conjugation”.

(iii) Conversely, let $K$ be a number field such that for all embeddings $\iota : K \hookrightarrow \mathbb{C}$, the subfield $\iota(K)$ is stable under complex conjugation and the automorphism $x \mapsto \iota^{-1}(\overline{\iota(x)})$ of $K$ with order $\leq 2$ is independent of $\iota$ and is non-trivial. Prove that $K$ is a CM field.

(iv) Prove that any finite abelian extension of $\mathbb{Q}$ is either totally real or CM, and that a compositum of CM fields is CM. Also prove that if $f \in \mathbb{Q}[X]$ is an irreducible cubic that is not split over $\mathbb{R}$ then a splitting field for $f$ over $\mathbb{Q}$ is an even-degree extension of $\mathbb{Q}$ that is neither totally real nor CM.

5. Let $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ be a splitting field for $(X^2 - 3)(X^2 - 5)$ over $\mathbb{Q}$. Prove that $\alpha = \sqrt{3} + \sqrt{5}$ is a primitive element, and compute the discriminant of the order $\mathcal{O} = \mathbb{Z}[\alpha]$ over $\mathbb{Z}$ in two different ways: use the definition as a determinant of traces, and alternatively (since it is easy to “write down” the conjugates of $\alpha$ over $\mathbb{Q}$) use the formula $(-1)^{n(n-1)/2} \prod_{\sigma \neq \tau} (\sigma(\alpha) - \tau(\alpha))$ (with $n = [K : \mathbb{Q}] = 4$ here). Do you get the same answer by both methods? I hope so!