1. Let $K$ be a number field, and fix a finite set of non-archimedean places $v_1, \ldots, v_r$ and integers $e_1, \ldots, e_r \geq 1$. Show that there is a maximal finite abelian extension $K'/K$ unramified away from $\infty$ and the $v_i$’s with inertia group at $v_i$ of exponent $e_i$ (which includes the case of ramification degree equal to $e_i$). Describe the corresponding subgroup of $A_K^\times/K^\times$. Hint: $(\mathcal{O}_K^\times)^e$ is open in $\mathcal{O}_K^\times$.

2. (i) Using class field theory, prove that $\mathbb{Q}(\zeta_3)/\mathbb{Q}(\sqrt{-3})$ is the maximal finite abelian extension of $\mathbb{Q}(\sqrt{-3})$ that is unramified away from $5\infty$ and has degree prime to $5$. What if we omit the degree condition?

(ii) Use local class field theory and the structure of $\mathbb{Q}_p^\times$ to show that $\mathbb{Q}_p$ has exactly $p$ totally ramified degree-$p$ abelian extensions when $p > 2$.

(iii) Let $K$ be a local field with residue field of size $q$. Use local class field theory to prove that any tamely ramified abelian finite extension of $K$ has ramification degree dividing $q-1$ (regardless of the degree of the total extension, so most of the extension is unramified).

3. Let $K$ be an imaginary quadratic field. In HW8 you saw that its $\mathbb{Z}_p$-rank is 2. Let $L/K$ be the field generated by the $\mathbb{Z}_p$-extensions of $K$, so $\text{Gal}(L/K) \simeq \mathbb{Z}_p^2$.

(i) Prove $L/\mathbb{Q}$ is Galois, and construct a $\mathbb{Z}_p$-linear action of $\text{Gal}(K/\mathbb{Q})$ on $\text{Gal}(L/K)$ (using $\text{Gal}(L/\mathbb{Q})$).

(ii) Using that $\mathbb{Q}$ has $\mathbb{Z}_p$-rank 1 (and not 2), prove that the action by $\text{Gal}(K/\mathbb{Q})$ on $\Gamma \simeq \mathbb{Z}_p^2$ has its nontrivial element acting with eigenvalues $\{-1, 1\}$. Deduce that for each sign $\epsilon = \pm 1$ there is a unique quotient $\Gamma^\epsilon \simeq \mathbb{Z}_p$ of $\Gamma$ on which the non-trivial element of $\text{Gal}(K/\mathbb{Q})$ acts by $\epsilon$. Show that the corresponding field $K^1/K$ is the cyclotomic $\mathbb{Z}_p$-extension; the field $K^1/K$ is called the anti-cyclotomic $\mathbb{Z}_p$-extension.

4. This exercise encapsulates most of the arithmetic content of the book “Primes of the form $x^2 + ny^2$”, up to the issue of using elliptic functions to explicitly compute class fields of imaginary quadratic fields.

(i) Fix a squarefree $n > 1$ with $n \equiv 2, 3 \mod 4$, so $K = \mathbb{Q}(\sqrt{-n})$ has $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$ and the discriminant is $-4n$. Consider primes $p \nmid 2n$, (i.e., primes unramified in $K$). Prove that $p = x^2 + ny^2$ with $x, y \in \mathbb{Z}$ if and only if $p$ is a square mod $n$ (i.e., $p$ splits in $K$) and the two primes over $p$ in $\mathcal{O}_K$ are principal.

(ii) Continuing with (i), given that $p$ is a square mod $n$, so $p\mathcal{O}_K = pp'$, how can we tell when $p$ (or equivalently $p' = \overline{p}$) is principal? By the Hilbert/Artin principal ideal theorem, it is equivalent to say that $p$ splits completely in the Hilbert class field $H$ of $K$! But given that $p$ is already split in $K$ (as $p$ is a square mod $n$), this condition on $p$ says exactly that $p$ is totally split in the Galois (generally not abelian) extension $H/\mathbb{Q}$! Since $p$ is unramified in $H$ (as $H/K$ is unramified everywhere), being totally split amounts to having its common residual degree at all primes over $p$ in $H$ equal to 1.

Fix a lift of complex conjugation from $K$ to $H$ and let $H^+$ be its fixed field, so $H = K \otimes_{\mathbb{Q}} H^+$. (Beware that $H^+$ may not be Galois over $\mathbb{Q}$.) Prove that $H/\mathbb{Q}$ is totally split at a prime $p$ if and only if $K/\mathbb{Q}$ is split at $p$ and $H^+$ is unramified at $p$ with a place of residual degree 1 at $p$. Deduce that if $\alpha \in \mathcal{O}_{H^+}$ is a primitive element for $H^+$ over $\mathbb{Q}$ with minimal polynomial $f \in \mathbb{Z}[X]$, so the inclusion $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_{H^+}$ is an equality locally at all primes away from $f/d(f)$ (why?), then for $p \nmid 2n \cdot \text{disc}(f)$,

$$p = x^2 + ny^2 \text{ for some } x, y \in \mathbb{Z} \iff p \text{ is a square mod } n \text{ and } f(t) \equiv 0 \pmod{p} \text{ has a solution}. $$

(iii) Prove that for $p \neq 2, 23$, $p = x^2 + 23y^2$ for some $x, y \in \mathbb{Z}$ if and only if $p$ is a square mod 23 and $t^3 - t - 1 \equiv 0 \pmod{p}$ has a solution. (Hint: Exercise 4 in HW2.)

Remark The preceding technique required $n$ to be squarefree and $\equiv 2, 3 \mod 4$ so that $\mathbb{Z}[\sqrt{-n}]$ is integrally closed. To allow general non-square $n > 1$, there is a similar argument to be made except that one has to replace the Hilbert class field of $\mathbb{Q}(\sqrt{-n})$ with another class field of $\mathbb{Q}(\sqrt{-n})$ attached to the order $\mathbb{Z}[\sqrt{-n}]$ in its ring of integers.

In general, if $K$ is a number field then for any order $\mathcal{O} \subseteq \mathcal{O}_K$ (say with conductor $c$) the group $\text{Pic}(\mathcal{O})$ (which we saw is always finite in Math 248A) admits an adelic description as quotient of $A_K^\times/K^\times$ modulo an open subgroup (generalizing the case $\mathcal{O} = \mathcal{O}_K$ that we already know and love). Thus, by class field theory we get a finite abelian extension $K_\mathcal{O}/K$ equipped with a canonical isomorphism $\text{Gal}(K_\mathcal{O}/K) \simeq \text{Pic}(\mathcal{O})$ (and it is unramified away from $\mathcal{O}$ but is generally not a ray class field!). This is called the ring class field over $K$ attached to $\mathcal{O}$; in case $\mathcal{O} = \mathcal{O}_K$ it is the Hilbert class field of $K$. 
