Assignment 2

1. Let $m = p^r$ with p prime and $r \in \mathbb{N}$ and let $n = \varphi(m)$. Let $\zeta = e^{2\pi i/m}$ and $K = \mathbb{Q}(\zeta)$. Show that
$$\Delta(\zeta) = \frac{(-1)^{\binom{n}{2}} m^n}{p^{m/p}}.$$

   The minimal polynomial for ζ over $\mathbb{Q}$ is
$$f(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1}.$$

   Its derivative is
$$f'(x) = \frac{p^r x^{p^r-1}\left(x^{p^{r-1}} - 1\right) - p^{r-1}x^{p^{r-1}-1}\left(x^{p^r} - 1\right)}{\left(x^{p^{r-1}} - 1\right)^2}.$$

   This simplifies considerably when evaluated at $x = \zeta$, since $\zeta^{p^r} = 1$ and $\zeta^{p^r-1} = \zeta^{-1}$:
$$f'(\zeta) = \frac{p^r\left(\zeta^{p^{r-1}-1} - \zeta^{-1}\right)}{\left(\zeta^{p^{r-1}} - 1\right)^2} = \frac{p^r}{\zeta\left(\zeta^{p^{r-1}} - 1\right)}.$$

   Next we compute the norm:
$$N_{\mathbb{Q}}^K(f'(\zeta)) = \frac{(p^r)^n}{N_{\mathbb{Q}}^K(\zeta^{p^{r-1}} - 1)}.$$

   Letting $\omega = \zeta^{p^{r-1}}$, we have $\omega^p = 1$ and (seen in the lectures):
$$N_{\mathbb{Q}}^{\mathbb{Q}(\omega)}(\omega - 1) = p,$$

   therefore
$$N_{\mathbb{Q}}^K(\omega - 1) = \left(N_{\mathbb{Q}}^{\mathbb{Q}(\omega)}(\omega - 1)\right)^{p^{r-1}} = p^{p^{r-1}},$$

   and finally
$$\Delta_K = (-1)^{\binom{n}{2}} N_{\mathbb{Q}}^K(f'(\zeta)) = \frac{(-1)^{\binom{n}{2}} m^n}{p^{m/p}}.$$

2. Let K be a number field and consider its embeddings $\sigma_1, \ldots, \sigma_n \colon K \to \mathbb{C}$. Let r_1 denote the number of embeddings whose image is actually contained in $\mathbb{R}$. The remaining $n - r_1$ embeddings come in pairs $\sigma, \overline{\sigma}$, where $\overline{\sigma}$ is the composition of σ and the complex conjugation automorphism of $\mathbb{C}$. Let r_2 be the number of such pairs, so that $n = r_1 + 2r_2$.

   Prove that the sign of Δ_K is $(-1)^{r_2}$.

   Let $\omega_1, \ldots, \omega_n$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$, then
$$\Delta_K = \det(\sigma_i(\omega_j))^2.$$

   Consider the effect of complex conjugation; it leaves the r_1 rows corresponding to the real embeddings, and interchanges each pair of r_2 rows corresponding to the conjugate pairs of non-real embeddings. Therefore
$$\overline{\det(\sigma_i(\omega_j))} = (-1)^{r_2}\det(\sigma_i(\omega_j)).$$

   If r_2 is even, then $\det(\sigma_i(\omega_j))$ is real, so its square $\Delta_K > 0$.
   If r_2 is odd, then $\det(\sigma_i(\omega_j))$ is purely imaginary, so its square $\Delta_K < 0$.

3. Fix $g, n \in \mathbb{Z}_{>1}$ with n odd such that $d := n^g - 1$ is squarefree. Show that the ideal class group of $K = \mathbb{Q}(\sqrt{-d})$ contains an element of order equal to g.

   As d is even and squarefree, it must be $\equiv 2 \pmod 4$, so $\mathcal{O}_K = \mathbb{Z}[\sqrt{-d}]$. As ideals of $\mathcal{O}_K$ we have
   $$(n)^g = (n^g) = (1+d) = (1+\sqrt{-d})(1-\sqrt{-d}).$$
   Consider the ideal $(1+\sqrt{-d}) + (1-\sqrt{-d})$. It contains $2 = 1+\sqrt{-d}+1-\sqrt{-d}$. It also contains the odd number $n^g = (1+\sqrt{-d})(1-\sqrt{-d})$. Therefore it contains $1 = \gcd(2, n^g)$, so $(1+\sqrt{-d})$ and $(1-\sqrt{-d})$ are coprime ideals. As their product is the g-th power of the ideal (n), each of these ideals must be a g-th power, so there exist ideals I, J such that $I^g = (1+\sqrt{-d})$ and $J^g = (1-\sqrt{-d})$ and $IJ = (n)$.
   Clearly the order of I in the ideal class group divides g.
   Suppose $I^k = (a+b\sqrt{-d})$ for some $k \in \mathbb{N}$, $a, b \in \mathbb{Z}$. We cannot have $b = 0$: otherwise $I^k = (a) = J^k$, but I and J are coprime, so $(a) = \mathcal{O}_K$, therefore $N(I)^k = N(J)^k = 1$, contradicting the fact that $N(IJ) = N(n) > 1$.
   Taking norms in $I^k = (a+b\sqrt{-d})$ we have
   $$n^k = a^2 + b^2 d \geq d = n^g - 1,$$
   which forces $k \geq g$.

4. Find the class number of $K = \mathbb{Q}(\sqrt{-19})$.

   Since $-19 \equiv 1 \pmod 4$, we have $\Delta_K = -19$ and $\mathcal{O}_K = \mathbb{Z}[\theta]$ where $\theta = \frac{1+\sqrt{-19}}{2}$. Note that $\theta^2 - \theta + 5 = 0$. The Hurwitz bound is
   $$B_K = (1+|\theta|)(1+|\bar{\theta}|) \approx 10.472\ldots$$
   It suffices then to consider the decomposition of the primes $2, 3, 5, 7$ to determine the prime ideals with norm ≤ 10.
   The polynomial $x^2 - x + 5$ is irreducible modulo 2 and 3, so these are inert and $2\mathcal{O}_K$, $3\mathcal{O}_K$ are prime ideals.
   The polynomial $x^2 - x + 5 = x(x-1)$ modulo 5, so $5\mathcal{O}_K = (5, \theta)(5, \theta - 1)$. But $\theta(\theta - 1) = -5$ implying that $5 \in (\theta)$ and $5 \in (\theta - 1)$ and hence the two prime ideals $(5, \theta) = (\theta)$ and $(5, \theta - 1) = (\theta - 1)$ of norm 5 are principal.
   Finally, the polynomial $x^2 - x + 5 = x^2 - x - 2 = (x+1)(x-2)$ modulo 7, so $7\mathcal{O}_K = (7, \theta+1)(7, \theta-2)$. Since $(\theta+1)(\theta-2) = -7$, we get that $(7, \theta+1) = (\theta+1)$ and $(7, \theta-2) = (\theta-2)$ are also principal.
   We conclude that the class number is one.

5. Let p be a prime number that is congruent to 13 or 17 modulo 20.

   a) Show that the congruence $x^4 \equiv 25 \pmod p$ has no solutions.

      Since $x^4 - 25 = (x^2 - 5)(x^2 + 5)$ and p is prime, if the congruence has a solution then
      $$1 = \left(\frac{\pm 5}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{\pm 3}{5}\right) = -1,$$
      which is a contradiction. In the process we used the fact that $p \equiv 1 \pmod 4$ in two places (to get that -1 is a quadratic residue mod p, and in applying the Law of Quadratic Reciprocity).

b) Show that the equation $x^4 + py^4 = 25z^4$ has no integer solutions other than $(0, 0, 0)$.
Suppose (x, y, z) is a non-zero integer solution.
Without loss of generality $\gcd(x, y, z) = 1$ (otherwise divide through by the gcd to reduce to this case). Also $\gcd(p, z) = 1$, as otherwise $p \mid x$ and $p \mid y$ and $\gcd(x, y, z) \geq p$.
Reducing the equation modulo p, we get $x^4 \equiv 25z^4 \pmod{p}$, which has no solutions by part (a).

6. Let $K = \mathbb{Q}(\sqrt{-6})$. Determine which prime numbers p split, ramify, respectively remain inert in K, expressing your answer in terms of congruence conditions on p.

Since $-6 \equiv 2 \pmod{4}$ we have $\Delta_K = -24$.
Therefore 2 and 3 are the primes that ramify in $\mathcal{O}_K$.
For $p \neq 2, 3$ we have that p splits in $\mathcal{O}_K$ if and only if

$$1 = \left(\frac{-24}{p}\right) = \left(\frac{-6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-3}{p}\right).$$

We know that (for $p \neq 2, 3$)

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod{8} \\ -1 & \text{if } p \equiv 3, 5 \pmod{8} \end{cases}$$

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{3} \\ -1 & \text{if } p \equiv 2 \pmod{3}, \end{cases}$$

where $\left(\frac{p}{3}\right) = \left(\frac{3^*}{p}\right) = \left(\frac{-3}{p}\right)$ comes from the Quadratic Reciprocity Law.
The conditions can be combined into

- p splits in $\mathcal{O}_K$ if and only if $p \equiv 1, 5, 7, 11 \pmod{24}$;
- p is inert in $\mathcal{O}_K$ if and only if $p \equiv 13, 17, 19, 23 \pmod{24}$;
- p is ramified in $\mathcal{O}_K$ if and only if $p = 2, 3$.