Problem Set 10.

1. The goal of this problem is to show that the maximal order in the cyclotomic field $\mathbf{Q}(e^{2\pi i/n})$ is the ring $\mathbf{Z}[e^{2\pi i/n}]$.

   a) Show that if R is a unique factorization domain with fraction field F and π is an irreducible element of R then any polynomial of the form
   $$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in R[x]$$
   such that $\pi | a_i, \pi^2 \not| a_0$ is irreducible as a polynomial in $F[x]$.

   b) Suppose K is a number field and $R = O_K$ is the maximal order. Show by localizing R by inverting all elements not in a nonzero prime ideal $P \subset R$ to obtain R_P as in problem 6.3 that R_P is a principal ideal domain. Show by applying part a) that if $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathcal{O}_K[x]$ satisfies $a_i \in P, a_0 \notin P^2$ then $f(x)$ is irreducible as a polynomial in $F[x]$. (we say that $f(x)$ satisfies the Eisenstein criterion for P when this occurs).

   c) Suppose that K is a number field and $L = K(\alpha)$ is an extension field such that the minimal polynomial of α is Eisenstein for an unramified prime $P \subset \mathcal{O}_K$ containing the rational prime p. Show that $O_K[\alpha]$ is an order in L and that the index $[\mathcal{O}_L : \mathcal{O}_K[\alpha]]$ is not divisible by p.

   d) Let $\zeta_m = e^{2\pi i/m}$ and let $\Phi_m(x)$ be the minimal monic integer polynomial satisfied ζ_m. Show that if a prime integer p divides the discriminant of the cyclotomic polynomial $\Phi_m(x)$ then $p|m$.

   e) Show by induction on the number of distinct prime factors that the maximal order in the cyclotomic field $\mathbf{Q}(\zeta_n)$ is the ring $\mathbf{Z}[\zeta_n]$. Hint: Show that if p is a prime not dividing m then $1 - \zeta_{p^k}$ satisfies an Eisenstein polynomial over $O_{\mathbf{Q}(\zeta_m)}$.

2. Show that $y^2 = x^3 - 26$ has a solution with $y = 1$ which does not appear in the list of solutions in Problem 9.1e so that $t = 26$ cannot satisfy the hypothesis of the theorem proved there. Show this implies that the class number of the field $K = Q(\sqrt{-26})$ is divisible by 3. Compute the class group $Pic(\mathcal{O}_K)$ of this field.

3. Compute the class group of the real quadratic field $\mathbf{Q}(\sqrt{473})$.

4. Let p be a prime number and let a be an integer prime to p. Show that the sequence $a, a^p, a^{p^2}, \ldots$ is a Cauchy sequence and so converges to an element ζ in the completion $\mathbf{Q}_p$ of the rationals with respect to the p-adic absolute value. Show that $\zeta^p = \zeta$, so that $\mathbf{Q}_p$ contains the $(p-1)$-th roots of 1.