PROBLEM SET 1

Below, $d(\neq 0,1)$ is always squarefree.

(1) (a) Show that for $p \neq 2$, $\left(\frac{a}{p}\right) = 1 \iff a^{\frac{p-1}{2}} \underset{(p)}{\equiv} 1$. [Hint: the multiplicative group of a finite field is . . .] (b) Show $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. (c) Let p be a prime of the form $4m+1$, $m \in \mathbb{Z}$. Show $\left(\frac{-1}{p}\right) = 1$, hence that p is not prime in $\mathbb{Z}[i]$, hence that $p = a^2 + b^2$ $(a, b \in \mathbb{Z})$.

(2) Recall that we know $R = \mathbb{Z}[i]$ is a UFD, so that the primes and irreducibles in R are the same. Find all of them. [Hint: any element r divides its norm $\mathcal{N}(r) = r\bar{r}$. Factor this into integer primes and then factor those in $\mathbb{Z}[i]$.]

(3) [Jacobson p. 147 #8] Let p be a prime of the form $4n+1$ and let q be a prime such that the Legendre symbol $(\frac{q}{p}) = -1$ (cf. [**Algebra I**. III.J.16]). Show that $\mathbb{Z}[\sqrt{pq}]$ is not a UFD. (In particular, this applies to $\mathbb{Z}[\sqrt{10}]$.) [Hint: by [**Algebra I**, Thm. III.I.12], it suffices to show that the "Primeness Condition" fails for some element of $\mathbb{Z}[\sqrt{pq}]$. One way to do this uses Exercise (1) parts (b) and (c).]

(4) Let $K = \mathbb{Q}[\sqrt{-29}]$. From [**Algebra I**, III.L.26] we know that $[\wp_5] \in Cl(K)$ has order 3, and we also note that $(2) = (2, 1+\sqrt{-29})^2 =: \wp_2^2$. Show that $\mathcal{O}_K$ has ideals of norm 3 and 11 of order 6 in $Cl(K)$. [Hint: start by looking for principal ideals of norm 30 and 33.]

(5) We explained how odd primes p decompose in number rings. What about the even prime? Let $K = \mathbb{Q}[\sqrt{d}]$, and show that (in $\mathcal{O}_K$)

$$d \underset{(4)}{\equiv} 2 \implies (2) = (2, \sqrt{d})^2$$

$$d \underset{(4)}{\equiv} 3 \implies (2) = (2, 1+\sqrt{d})^2$$

$$d \underset{(8)}{\equiv} 1 \implies (2) = (2, \tfrac{1+\sqrt{d}}{2})(2, \tfrac{1-\sqrt{d}}{2})$$

$$d \underset{(8)}{\equiv} 5 \implies (2) \text{ prime}$$

(6) Let $K = \mathbb{Q}[\sqrt{-26}]$. Find all non-principal ideals of norm 30 in $\mathcal{O}_K$. [Hint: here are some of your tools: [**Algebra I**, Prop. III.L.25], Pell's equation (i.e. using solutions of $x^2 + 26y^2 = m$ to test whether there exists a principal ideal of norm m), uniqueness of ideal factorization, and Caesar.]

(7) Show that $X^2 = Y^3 - 14$ has no solution with $X, Y \in \mathbb{Z}$. You may assume that $h_{\mathbb{Q}(\sqrt{-14})} = 4$. [Hint: if (X, Y) is a solution, put $\alpha := X + \sqrt{-14}$ (not $X + Y\sqrt{-14}$!!). Turn the equation into an equation of ideals, decompose both sides into prime factors, and use uniqueness of ideal factorization to deduce that α is a cube in $\mathbb{Z}[\sqrt{-14}]$.]

(8) Let $K = \mathbb{Q}[\sqrt{d}]$, $d \underset{(4)}{\equiv} 2$ or 3, and $I \subset \mathcal{O}_K$ an ideal. Show that $\mathfrak{N}(I) = |\mathcal{O}_K/I|$, where $\mathfrak{N}(I)$ is defined via Hurwitz. [Hint: first compute $|\mathcal{O}_K/I|$ as a determinant.]