Problem Sheet 3

Problem 1

Let p be an odd prime and q a power of p.

(a) Prove that $x \in \mathbb{F}_q^\times$ is a square if and only if $x^{(q-1)/2} = 1$.

(b) Prove that 2 is a square in $\mathbb{F}_p$ if and only if $p \equiv \pm 1 \mod 8$. Show similarly that -2 is a square in $\mathbb{F}_p$ if and only if $p \equiv 1, 3 \mod 8$.
Hint: Prove and use the identity $(\zeta + \zeta^{-1})^2 = 2$, where $\zeta \in \overline{\mathbb{F}_p}$ is a primitive 8-th root of unity.

Problem 2

For $n \geq 1$ let $r(n) := \sharp\{(x, y) \in \mathbb{Z}^2 \mid x^2 + 2y^2 = n\}$. Show that

$$r(n) = 2 \sum_{m|n} \chi(m)$$

where $\chi : \mathbb{Z}_{\geq 1} \longrightarrow \{-1, 0, 1\}$ is the multiplicative extension of

$$\chi(p) = \begin{cases} 0 & \text{if } p = 2 \\ 1 & \text{if } p \text{ prime} \equiv 1, 3 \mod 8 \\ -1 & \text{if } p \text{ prime} \equiv 5, 7 \mod 8. \end{cases}$$

Problem 3

Let ζ be a primitve N-th root of unity ($N \geq 3$) and set $\theta := \zeta + \zeta^{-1}$.

(a) Show that $\mathbb{Q}(\theta)$ is the fixed field of $\mathbb{Q}(\zeta)$ under the automorphism defined by complex conjugation.

(b) Put $n = \phi(N)/2$. Show that $\{1, \zeta, \theta, \theta\zeta, \theta^2, \theta^2\zeta, \ldots, \theta^{n-1}, \theta^{n-1}\zeta\}$ is a basis for $\mathbb{Z}[\zeta]$.

(c) Show that the ring of integers of $\mathbb{Q}(\theta)$ is $\mathbb{Z}[\theta]$.

(d) Suppose that $N = p$ is an odd prime. Prove that the discriminant of $\mathbb{Q}(\theta)$ is $\Delta_{\mathbb{Q}(\theta)} = p^{(p-3)/2}$.

Problem 4

Let A be a Dedekind ring.

(a) Prove that for any multiplicative subset $S \subseteq A \setminus \{0\}$, the localization $A[S^{-1}]$ is again a Dedekind ring.

(b) Show that for any ideal $0 \neq \mathfrak{a} \subseteq A$, every ideal of $A/\mathfrak{a}$ is principal. Show further that every ideal of A can be generated by two elements.