Solution to Sheet 3.

Exercise 1 & 2

Multiplicative groups mod n. Given some $n = p_1^{e_1} \cdots p_r^{e_r} \in \mathbb{N}$, we want to investigate the structure of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. By the chinese remainder theorem we find

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \left(\prod_{i=1}^{n} (\mathbb{Z}/p_i^{e_i}\mathbb{Z})\right)^\times \cong \prod_{i=1}^{n} (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times,$$

so we really only care about the structure of $(\mathbb{Z}/p^e\mathbb{Z})^\times$. There, the structure is given by

$$(\mathbb{Z}/p^e\mathbb{Z})^\times \cong \begin{cases} \text{a cyclic subgroup of order } \varphi(p^e) & \text{if } p \text{ is odd} \\ \langle 3 \rangle & \text{if } p = 2 \text{ and } e \leq 2 \\ \langle \pm 5 \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{e-2}\mathbb{Z} & \text{if } p = 2 \text{ and } e \geq 3. \end{cases}$$

A generator of $\mathbb{F}_p^\times$, or more generally, a generator of $(\mathbb{Z}/p^e\mathbb{Z})^\times$ is called a *root of unity*. We have the *Legendre Symbol*, which for $a \in \mathbb{Z}$ and p prime is given by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ (-1) & \text{if there is no solution mod } p \text{ to } x^2 = a \\ 1 & \text{otherwise.} \end{cases}$$

It is multiplicative in a, hence it yields a character $(\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$. The subgroup of *Quadratic residues mod p* is given by $\operatorname{Ker}\left(\left(\frac{-}{p}\right)\right) = \langle \varpi^2 \rangle$ for ϖ a root of unity.

1. Note that the real characters are exactly those $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$ with $\chi^2 = 1$. Note also that given a cyclic group $G \cong \mathbb{Z}/n\mathbb{Z}$, there is an isomorphism $G \cong \hat{G}$ given by $a \mapsto (1 \mapsto \zeta_n^a)$, where ζ_n is an n-th root of unity. As p is odd, there are exactly two solutions to $x^2 = 1$, hence there are exactly 2 real characters mod p, one of which is the trivial one (induced by the principle character mod 1), and the other is given by the legendre symbol. The same reasoning goes through mod p^e for $e \geq 2$, but now the characters are induced from characters mod p.

2.

Notes after correcting.