Assignment 26

Cyclotomic extensions.

In the following, $\varphi : \mathbb{Z}_{\geqslant 1} \longrightarrow \mathbb{Z}_{\geqslant 0}$ is the Euler function $\varphi(n) = \operatorname{card}((\mathbb{Z}/n\mathbb{Z})^\times)$. For each integer $n \geqslant 1$, we consider the n-th cyclotomic polynomial

$$\Phi_n := \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} (T - e^{\frac{2\pi i}{n} a}) \in \mathbb{Z}[T].$$

1. Prove the following properties of the cyclotomic polynomials $\varphi_n \in \mathbb{Z}[T]$
   (a) $\Phi_n(T) = T^{\varphi(n)} \Phi_n\left(\frac{1}{T}\right)$ for every integer $n \geqslant 2$.
   (b) $\Phi_p(T) = T^{p-1} + \cdots + 1$ for every prime number p.
   (c) $\Phi_{p^r}(T) = \Phi_p(T^{p^{r-1}})$ for every prime number p and integer $r \geqslant 1$.
   (d) $\Phi_{2n}(T) = \Phi_n(-T)$ for every **odd** integer $n \geqslant 1$.

2. Let p be an odd prime number and $r \geqslant 2$ an integer. We want to prove that there is an isomorphism of abelian groups
$$(\mathbb{Z}/p^r\mathbb{Z})^\times = \mathbb{Z}/p^{r-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}.$$
   (a) Explain why the statement is equivalent to proving that $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is cyclic.
   (b) Prove that there exists $g \in \mathbb{Z}$ which generates $(\mathbb{Z}/p\mathbb{Z})^\times$ and such that $g^{p-1} \not\equiv 1 \mod p^2$ [*Hint:* Let g be a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. Look at $(g+p)^{p-1}$ modulo p^2 and eventually replace g with $g+p$]
   (c) Prove inductively that there are integers $k_1, k_2, \ldots, k_{r-1} \in \mathbb{Z}$ for which
$$g^{p^{j-1}(p-1)} = 1 + k_j p^j,\ p \nmid k_j$$
   (d) Deduce that $g^{p^{r-2}(p-1)} \not\equiv 1 \mod p^r$. Moreover, prove that $\operatorname{ord}_{(\mathbb{Z}/p^r\mathbb{Z})^\times}(g)$ divides $p^{r-1}(p-1)$.
   (e) Suppose that $g^{p^\varepsilon d} \equiv 1 \mod p^r$ for some integer $\varepsilon \geqslant 1$ and a proper divisor d of $p-1$. Deduce that $g^d \equiv 1 \mod p$ and derive a contradiction.
   (f) Conclude that g is a generator of $(\mathbb{Z}/p^r\mathbb{Z})^\times$.

3. Prove that for every integer $r \geqslant 2$ there is an isomorphism of abelian groups
$$(\mathbb{Z}/2^r\mathbb{Z})^\times = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}.$$
   More specifically, show for $r \geqslant 3$ that
$$(\mathbb{Z}/2^r\mathbb{Z})^\times \cong \{\pm 1\} \times \{1, 5, 5^2 \ldots, 5^{2^{r-2}-1}\}.$$

4. Let n be a positive integer and $p \nmid n$ a prime number. Prove that the irreducible factors of $\Phi_n \in \mathbb{F}_p[X]$ are all distinct and their degree is equal to the order of $p + n\mathbb{Z}$ in $(\mathbb{Z}/n\mathbb{Z})^\times$. [*Hint:* You may want to prove the following claim: if α is a root of Φ_n, then α is a primitive root of 1.]

5. Let n be a positive integer. Prove that there are infinitely many primes p such that $p \equiv 1 \bmod n$. [*Hint:* If one such prime p exists for every n, then one can find a bigger one p' satisfying $p' \equiv 1 \bmod (n \cdot p)$]