1. Let $\Phi_n(x) \in \mathbb{Z}[x]$ be the n-th cyclotomic polynomial and for an odd prime p which does not divide n, let $\Phi_{n,p}(x) \in \mathbb{F}_p[x]$ be $\Phi_n(x)$ modulo p. Let $E \subseteq \overline{\mathbb{F}}_p$ be a splitting field of $\Phi_{n,p}(x)$ over $\mathbb{F}_p$ where $\overline{\mathbb{F}}_p$ is an algebraic closure of $\mathbb{F}_p$.

   (a) Prove that $\zeta \in \overline{\mathbb{F}}_p$ is a zero of $\Phi_{n,p}$ if and only if the multiplicative order of ζ is n.

   (b) Prove that $\Phi_{n,p}(x) = \prod_{1\leq i\leq n, \gcd(i,n)=1}(x-\zeta^i)$ where $\zeta \in \overline{\mathbb{F}}_p^{\times}$ is a zero of $\Phi_{n,p}(x)$, and deduce that the restriction gives us an embedding

$$\mathrm{Gal}(E/\mathbb{F}_p) \hookrightarrow \mathrm{Aut}(\langle\zeta\rangle) \simeq (\mathbb{Z}/n\mathbb{Z})^{\times}.$$

   (c) Prove that $\mathrm{Gal}(E/\mathbb{F}_p) \simeq \langle p + n\mathbb{Z}\rangle \subseteq (\mathbb{Z}/n\mathbb{Z})^{\times}$.

   (**Hint**. Notice that $x^n - 1 = \prod_{d|n} \Phi_d(x)$ in $\mathbb{Z}[x]$, and so in

$$x^n - 1 = \prod_{d|n} \Phi_{n,p}(x)$$

   in $\mathbb{F}_p[x]$. Hence, if ζ is a zero of $\Phi_{n,p}(x)$, then $\zeta^n = 1$. If $\zeta^d = 1$ for $d < n$, then ζ is a zero of $\Phi_{d,p}(x)$; this implies that ζ is a multiple-zero of $x^n - 1$. Argue why this is a contradiction.

   For part (c), use the fact that the Galois group of a finite field is generated by the Frobenius map.)

2. Prove that there are infinitely many primes in the arithmetic progression $\{nk+1\}_{k=1}^{\infty}$.

   (**Hint**. Use the previous problem and show that if $\Phi_{n,p}$ has a zero in $\mathbb{F}_p$, then $n|p-1$. Next, suppose to the contrary there are only finitely many such primes $p_1, \ldots, p_{k_0}$ (k_0 might be zero). Consider the non-constant polynomial

$$f(x) := \Phi_n(2n\prod_{i=1}^{k_0} p_i x) \in \mathbb{Z}[x].$$

   For large enough $a \in \mathbb{Z}$, $f(a) \notin \{0, \pm 1\}$, and so there exists a prime p which divides $f(a)$. Argue why $p|(2n\prod_{i=1}^{k_0} p_i a)^n - 1$, and so p is odd, $p \nmid n$, and $p \neq p_i$ for every i. Argue why $n|p-1$.)

3. Suppose p is an odd prime which does not divide n, and $\Phi_n(x)$ is the n-th cyclotomic polynomial. Prove that $\Phi_n(x)$ modulo p is irreducible in $\mathbb{F}_p[x]$ if and only if p generates $(\mathbb{Z}/n\mathbb{Z})^\times$.

   (**Hint**. Use part (c) of problem 1.)

4. Suppose $q = p^n$ where p is prime and n is a positive integer. Prove that every irreducible factor of $x^q - x + 1$ in $\mathbb{F}_q[x]$ is of degree p.

   (**Hint**. Let E be a splitting field of $x^q - x + 1$ over $\mathbb{F}_q$. For every $\alpha \in E$, which is a zero of $x^q - x + 1$,

$$\deg m_{\alpha,\mathbb{F}_q} = [\mathbb{F}_q[\alpha] : \mathbb{F}_q] = |\mathrm{Gal}(\mathbb{F}_q[\alpha]/\mathbb{F}_q)|.$$

   Argue why the restriction gives us a surjective map

$$\mathrm{Gal}(E/\mathbb{F}_q) \to \mathrm{Gal}(\mathbb{F}_q[\alpha]/\mathbb{F}_q).$$

   Argue why $\mathrm{Gal}(E/\mathbb{F}_q) = \langle \sigma \rangle$, where $\sigma(x) = x^q$. Show that $\sigma(\alpha) = \alpha - 1$, and deduce that for every integer i, $\sigma^i(\alpha) = \alpha - i$. Hence $\sigma^p(\alpha) = \alpha$ and $\sigma^i(\alpha) \neq \alpha$ for every $i \in [1, p)$. Deduce that $|\mathrm{Gal}(\mathbb{F}_q[\alpha]/\mathbb{F}_q)| = p$.)

5. Suppose F is a field, $f \in F[x]$ is irreducible, and E is a splitting field of f over F. Suppose there exists $\alpha \in E$ such that

$$f(\alpha) = f(\alpha + 1) = 0.$$

   (a) Prove that the characteristic of F is $p > 0$.

   (b) Prove that there exists $K \in \mathrm{Int}(E/F)$ such that E/K is Galois and $[E : K] = p$.

   (**Hint.** Argue why there exists $\theta \in \mathrm{Aut}_F(E)$ such that $\theta(\alpha) = \alpha + 1$. Deduce that for every $k \in \mathbb{Z}^+$, $\theta^k(\alpha) = \alpha + k$. Because $\mathrm{Aut}_F(E)$ is a finite group, deduce that F is of positive characteristic. Moreover, $\theta(F[\alpha]) = F[\alpha]$ and the order of the restriction of θ to $F[\alpha]$ is p. This implies that the order of θ is a multiple of p. Therefore, p divides the order of $\mathrm{Aut}_F(E)$. Hence, there exists an element $\sigma \in \mathrm{Aut}_F(E)$ that has order p. Let $K := \mathrm{Fix}(\sigma)$. Argue why E/K is Galois and $\mathrm{Gal}(E/K) = \langle \sigma \rangle$; deduce that $[E : K] = p$.)

6. Suppose p is an odd prime and $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$ for every positive integer n.

(a) Prove that $[\mathbb{Q}[\zeta_{4p}] : \mathbb{Q}[\sin(2\pi/p)]] = 2$.

(b) Prove that $\mathbb{Q}[\sin(2\pi/p)] = \mathrm{Fix}(1, \tau)$ where τ is the restriction of the complex conjugation to $\mathbb{Q}[\zeta_{4p}]$.

(c) Prove that $\mathbb{Q}[\sin(2\pi/p)]/\mathbb{Q}$ is a Galois extension and

$$\mathrm{Gal}(\mathbb{Q}[\sin(2\pi/p)]/\mathbb{Q}) \simeq \frac{(\mathbb{Z}/4p\mathbb{Z})^{\times}}{\{\pm 1\}};$$

in particular, $[\mathbb{Q}[\sin(2\pi/p)] : \mathbb{Q}] = p - 1$.

(**Hint**. For the first part, notice that $\zeta_p i$ has multiplicative order $4p$, and its real part is $\sin(2\pi/p)$.)

7. Suppose n are positive integers.

(a) Prove that there exists a prime p such that $\mathbb{Z}/n\mathbb{Z}$ is a quotient of $(\mathbb{Z}/p\mathbb{Z})^{\times}$.

(b) Suppose A is a finite abelian group. Prove that there exists a square-free integer m such that A is a quotient of $(\mathbb{Z}/m\mathbb{Z})^{\times}$.

(c) Suppose A is a finite abelian group. Prove that there exists a finite Galois extension $E/\mathbb{Q}$ such that

$$\mathrm{Gal}(E/\mathbb{Q}) \simeq A.$$

(**Hint.** For part (a), use problem 2. For part (c), use part (b), and $\mathrm{Gal}(\mathbb{Q}[\zeta_m]/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^{\times}$.)