Cyclotomic Polynomials

Let m be a positive integer. The m^{th} cyclotomic polynomial is defined to be

$$\Phi_m(x) = \prod_{\substack{1 \le k \le m \\ \gcd(k,m)=1}} (x - e^{\frac{2\pi i k}{m}}) \in \mathbb{C}[x].$$

It is monic with degree $\phi(m)$. Its roots are precisely the primitive m^{th} roots of unity in $\mathbb{C}$ (generators of the group $\{x \in \mathbb{C} : x^m = 1\}$ under multiplication).

1. Write down $\Phi_m(x)$ for $m = 1, 2, \ldots, 8$.
2. Prove that $x^m - 1 = \prod_{d|m} \Phi_d(x)$.
3. Use Galois theory to prove that $\Phi_m(x)$ has rational coefficients for all m.
4. Prove by induction on m that $\Phi_m(x)$ has integer coefficients for all m.
   (Hint: Use Problem 1 and polynomial long division.)

Note: The expression in problem (2) is valid over every commutative ring R with identity, via the unique ring homomorphism from $\mathbb{Z}$ to R.

Theorem (Gauss) (Theorem 8.12 in Howie)
The cyclotomic polynomial $\Phi_m(x)$ is irreducible over $\mathbb{Q}$ for each $m \ge 1$.

Proof. Let f be a monic irreducible polynomial with integer coefficients that divides $\Phi_m(x)$.

Claim: If ϵ is a root of f in $\mathbb{C}$, then ϵ^p is also a root of f for any prime p not dividing m.

(Proof on next page.)

Use the Claim to show that all other primitive m^{th} roots of unity are roots of $f(x)$.

(Hint: other primitive m^{th} roots of unity have the form ϵ^k where k is __________________.

Consider the prime factorization of k.)

Finish the proof.

Claim: Let $f(x) \in \mathbb{Z}(x)$ be a monic irreducible polynomial that divides $\Phi_m(x)$. If ϵ is a root of f in $\mathbb{C}$, then ϵ^p is also a root of f for any prime p not dividing m.

Proof of Claim. Suppose not. Then $f \neq \Phi_m$, and let $g(x) = \Phi_m(x)/f(x)$.

Then $g(x)$ is non-constant, has integer coefficients (why?), and $g(\epsilon^p) =$ ____________.

Let $h(x) = g(x^p) \in \mathbb{Z}[x]$. Then $h(\epsilon) =$ ____________

How are f and h related?

Consider the natural map from $\mathbb{Z}$ to $\mathbb{Z}_p$ and extend it to a map from $\mathbb{Z}[x]$ to $\mathbb{Z}_p[x]$.

Let $\overline{f}, \overline{g}, \overline{h} \in \mathbb{Z}_p[x]$ be the images of f, g, h respectively.

Then $\overline{h} = (\overline{g})^p$ because

Let q be an irreducible factor of $\overline{f}$ in $\mathbb{Z}_p[x]$.

How are q and $\overline{h}$ related?

How are q and $\overline{g}$ related?

Then q^2 divides $\overline{\Phi_m}$ because

This implies that $x^m - 1$ has a repeated root in a splitting field over $\mathbb{Z}_p$, which is a contradiction because