Notes for Seminar:
The Odd Covering Problem and Its Relatives, Part IV

(Cut-and-Paste from Previous Notes)

Lemma 2: $\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) & \text{if } p|n \\ \Phi_n(x^p)/\Phi_n(x) & \text{if } p \nmid n \end{cases}.$

Lemma 3: Suppose m and n are integers with $m/n = p^r$ for some prime p and some positive integer r. Then $\Phi_m(\zeta_n) = pw$ for some $w \in \mathbb{Z}[\zeta_n]$.

Lemma 4: Let p be a prime, and let m be a positive integer such that p divides m. Then $x^p = \zeta_m$ has no solutions $x \in \mathbb{Q}(\zeta_m)$.

Lemma 5: Suppose $f(x) = -g(x)^p$ for some prime p and $f(x)x^n + 1$ is divisible by $\Phi_m(x)$ where $p|m$. Then $n \equiv 0 \pmod{p}$.

Proof: Assume $p \nmid n$. Then there are integers u and v such that $-nu + pv = 1$. Since also $f(\zeta)\zeta^n + 1 = 0$, we deduce that $-f(\zeta) = \zeta^{-n}$. Hence, $\big(g(\zeta)^u \zeta^v\big)^p = \zeta^{-nu+pv} = \zeta$. Thus, $x^p = \zeta$ has a solution $x \in \mathbb{Q}(\zeta)$, contradicting Lemma 4.

Lemma 7: Let m be an integer > 1. Then $\Phi_m(1) = \begin{cases} p & \text{if } m = p^r \text{ for some } r \in \mathbb{Z}^+ \\ 1 & \text{otherwise} \end{cases}.$

Proof: Clearly, $\Phi_p(1) = p$. If $m = p^r k$ with k and r positive integers such that $p \nmid k$, then Lemma 2 implies $\Phi_m(1) = \Phi_{pk}(1^{p^{r-1}}) = \Phi_{pk}(1)$. The lemma follows if $k = 1$. If $k > 1$, then applying Lemma 2 again we obtain $\Phi_m(1) = \Phi_{pk}(1) = \Phi_k(1^p)/\Phi_k(1) = 1$.

Lemma 8: Let m and ℓ be integers with $m \geq 1$ and $\ell \geq 0$. For $\alpha \in \mathbb{Q}(\zeta_m)$, let $N(\alpha) = N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\alpha)$ denote the norm of α. Then $N\big(\zeta_m^\ell - 1\big)$ is divisible by a prime p if and only if $m/\gcd(\ell, m)$ is a power of p.

Proof: Apply Lemma 7 and use that $N\big(\zeta_m^\ell - 1\big) = \pm\Phi_{m/\gcd(\ell,m)}(1)^{\phi(m)/\phi(m/\gcd(\ell,m))}$.

Claim: Suppose $m_j = p^t m_0$ and $m_i = p^s m_0$, where p is prime, m_0 is an integer > 1 such that $p \nmid m_0$, and t and s are integers with $t > s \geq 0$. Then $a_j \equiv a_i \pmod{m_0}$.

Recall: $\Phi_{m_j}(x)$ divides $f(x)x^n + 1$ if and only if $n \equiv a_j \pmod{m_j}$, $0 \leq a_j < m_j$

Proof of Claim: Let $k \in \mathbb{Z}^+ \cup \{0\}$ such that

$$a_i + (k-1)m_i < a_j \leq a_i + km_i.$$

Let $\ell = a_i + km_i - a_j$. Then $\ell \in [0, m_i)$. Since $\Phi_{m_i}(x)$ divides $f(x)x^{a_i+km_i} + 1$ and $\Phi_{m_j}(x)$ divides $f(x)x^{a_j} + 1$, we deduce that there are $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ such that

$$f(x)x^{a_i+km_i} + 1 = -\Phi_{m_i}(x)u(x) \quad \text{and} \quad f(x)x^{a_i+km_i} = f(x)x^{\ell+a_j} = -x^\ell + \Phi_{m_j}(x)v(x).$$

Hence,

$$\Phi_{m_i}(x)u(x) + \Phi_{m_j}(x)v(x) = x^\ell - 1.$$

Letting $x = \zeta_{m_i}$ above and applying Lemma 3, we obtain $pw = \zeta_{m_i}^\ell - 1$ for some $w \in \mathbb{Z}[\zeta_{m_i}]$. Applying Lemma 8, we deduce that m_0 divides ℓ. The definition of ℓ and the fact that m_0 divides both ℓ and m_i imply the claim.