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

Schinzel's Theorem: If there is an $f(x) \in \mathbb{Z}[x]$ with $f(1) \neq -1$ such that $f(x)x^n + 1$ is reducible for all $n \geq 0$, then there is an odd covering of the integers.

Notation: Let $\zeta_n = e^{2\pi i/n}$ and $\Phi_n(x) = \prod_{1 \leq k \leq n, \gcd(k,n)=1} (x - \zeta_n^k)$.

Lemma 1: $\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)} = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)}$.

Proof: The factor $x - \zeta_n^k$ is a factor of $x^{n/d} - 1$ precisely when n/d is a multiple of $n/\gcd(n,k)$ (i.e., when $d|\gcd(n,k)$. Thus, $x - \zeta_n^k$ appears in the right-most product above with exponent $\sum_{d|\gcd(n,k)} \mu(d)$. The rest is clear.

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

Proof: Use Lemma 1. If $p|n$, then $\Phi_{pn}(x) = \prod_{pd|pn} (x^{pd} - 1)^{\mu(pn/pd)} = \prod_{d|n} (x^{pd} - 1)^{\mu(n/d)} = \Phi_n(x^p)$. If $p \nmid n$, then $\Phi_{pn}(x) = \prod_{pd|pn} (x^{pd} - 1)^{\mu(pn/pd)} \prod_{d|n} (x^d - 1)^{\mu(pn/d)} = \Phi_n(x^p)/\Phi_n(x)$.

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 $w \in \mathbb{Z}[\zeta_n]$.

Proof: Consider three cases: (i) $m = pn$ and $p \nmid n$, (ii) $m = p^r n$ with $r > 1$ and $p \nmid n$, and (iii) $m = p^u t$ and $n = p^v t$ with $u > v > 0$. Let ξ denote an arbitrary primitive nth root of 1 (so $\xi \in \mathbb{Z}[\zeta_n]$). For (i), observe that Lemma 2 implies

$$\Phi_m(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)} = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} \left(\frac{x^p - \xi^{kp}}{x - \xi^k} \right) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} \left(x^{p-1} + \xi^k x^{p-2} + \xi^{2k} x^{p-3} + \cdots + \xi^{(p-1)k} \right).$$

In particular, $\Phi_m(\xi)$ has the factor (take $k = 1$) $p\xi^{p-1}$. For (ii), use Lemma 2 again to obtain $\Phi_m(\zeta_n) = \Phi_{pn}\left(\zeta_n^{p^{r-1}}\right)$ and apply the argument for (i) with $\xi = \zeta_n^{p^{r-1}}$. For (iii), use Lemma 2 as before to obtain $\Phi_m(\zeta_n) = \Phi_{p^{u-v}t}\left(\zeta_n^{p^v}\right) = \Phi_{p^{u-v}t}(\zeta_t)$. Now, cases (i) and (ii) imply $\Phi_m(\zeta_n) = pw$ for some $w \in \mathbb{Z}[\zeta_t] \subseteq \mathbb{Z}[\zeta_n]$ (since $\zeta_t = \zeta_n^{p^v}$).

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 $x \in \mathbb{Q}(\zeta_m)$.

Proof: Let $\zeta = \zeta_m$. The roots of $x^p - \zeta = 0$ are $\zeta_{pm}\zeta_p^k$ where $0 \leq k \leq p-1$. Note that $\zeta_p = \zeta_m^{m/p} \subseteq \mathbb{Q}(\zeta)$. Thus, $x^p = \zeta$ and $x \in \mathbb{Q}(\zeta)$ imply $\zeta_{pm} \in \mathbb{Q}(\zeta)$, a contradiction.

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, $\left(g(\zeta)^u \zeta^v\right)^p = \zeta^{-nu+pv} = \zeta$. Thus, $x^p = \zeta$ has a solution $x \in \mathbb{Q}(\zeta)$, contradicting Lemma 4.