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

Lemma 6: Suppose \( f(x)x^n+1 \) is divisible by \( \Phi_m(x) \) for some positive integer \( m \). Then \( f(x)x^n+1 \) is divisible by \( \Phi_m(x) \) if and only if \( n \equiv a \pmod{m} \).

Proof: Let \( F(x) = f(x)x^n+1 \). If \( n \equiv a \pmod{m} \), then clearly \( F(\zeta_m) = 0 \) so that \( F(x) \) is divisible by \( \Phi_m(x) \). If \( F(x) \) is divisible by \( \Phi_m(x) \), the equality

\[
0 = \zeta_m^{-a}(f(\zeta_m)\zeta_m^a + 1) - F(\zeta_m) = \zeta_m^{-a} - 1
\]

implies \( n \equiv a \pmod{m} \).

Comment: Note that if \( f(x)x^n+1 \) is divisible by \( g(x) \) for some irreducible \( g(x) \in \mathbb{Z}[x] \) and for at least two different nonnegative integers \( n \), then \( g(x) = \Phi_m(x) \) for some \( m \).

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 \( \Phi_m(1) = \Phi_p(1)^r \Phi_k(1) \). The lemma follows if \( k = 1 \). If \( k > 1 \), then applying Lemma 2 again we obtain \( \Phi_m(1) = \Phi_p(1) = \Phi_k(1)^r/\Phi_k(1) = 1 \).

Lemma 8: Let \( m \) and \( \ell \) 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 \( \alpha \). Then \( N(\zeta_m^\ell - 1) \) 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 \( N(\zeta_m^\ell - 1) = \pm \Phi_{m/\gcd(\ell, m)}(1)^{\phi(m/\gcd(\ell, m))} \).

Comment: We only need the “only if” part of Lemma 8 which follows from \( N(\zeta_m^\ell - 1) \) dividing a power of \( \Phi_{m/\gcd(\ell, m)}(1) \).

Main Lemma: Let \( f(x) \in \mathbb{Z}[x] \), and suppose \( n \) is sufficiently large (depending on \( f \)). Then the non-reciprocal part of \( f(x)x^n+1 \) is irreducible or identically \( \pm 1 \) unless one of the following holds:

(i) \( -f(x) \) is a \( p \)th power for some prime \( p \) dividing \( n \).

(ii) \( f(x) \) is 4 times a 4th power and \( n \) is divisible by 4.

Proof of Theorem Assuming Main Lemma: We suppose (as we may) that \( f(0) \neq 0 \). Since \( x^{2^t} + 1 = \Phi_{2^t+1}(x) \) is irreducible for every \( t \in \mathbb{Z}^+ \), we deduce \( f(x) \neq 1 \). Let \( \tilde{f}(x) = x^{\deg f}f(1/x) \). Then each reciprocal factor \( g(x) \) of \( F(x) = f(x)x^n+1 \) divides

\[
f(x)\tilde{F}(x) - x^{\deg f} F(x) = f(x)(x^{n+\deg f} + \tilde{f}(x)) - x^{\deg f}f(x)x^n + 1 = f(x)\tilde{f}(x) - x^{\deg f}f.
\]

In particular, there is a finite list of irreducible reciprocal factors that can divide \( f(x)x^n+1 \) as \( n \) varies. Each reciprocal non-cyclotomic irreducible factor divides at most one polynomial of the form \( f(x)x^n+1 \). By the Main Lemma, we deduce that there are \( \Phi_{m_1}(x), \ldots, \Phi_{m_s}(x) \) such that if \( n \) is sufficiently large and both (i) and (ii) do not hold, then \( \Phi_{m_j}(x)(f(x)x^n+1) \) for some \( j \). Note that (ii) does not hold since otherwise \( f(x)x^n+1 \) could not be divisible by a cyclotomic polynomial (if \( \Phi_m(x) \) were a factor, then \( f(\zeta_m)\zeta_m^a = -1 \), contradicting that the left side has even norm and the right side has odd norm) so that \( f(x)x^n+1 \) is irreducible whenever \( 4 \nmid n \) and \( n \) is sufficiently
large. We may suppose that there is an \( a_j \) such that \( \Phi_{m_j}(x) | (f(x)x^{a_j} + 1) \). Let \( \mathcal{P} \) denote the set of primes \( p \) for which \( f(x) \) is minus a \( p \)th power. We remove from consideration any \( m_j \) divisible by a \( p \in \mathcal{P} \) (but abusing notation we keep the range of subscripts). Then Lemmas 5 and 6 imply that the congruences
\[
x \equiv 0 \pmod{p} \quad \text{for } p \in \mathcal{P} \quad \text{and} \quad x \equiv a_j \pmod{m_j} \quad \text{for } j \in \{1, 2, \ldots, r\}
\]
cover the integers.

**Claim:** Suppose \( m_{j_t} = p^t m_0 \) 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 \( a_j \equiv a_i \pmod{m_0} \).

Take \( p = 2 \) in the Claim. We replace \( x \equiv a_j \pmod{m_j} \) and \( x \equiv a_i \pmod{m_i} \) with \( x \equiv a_i \pmod{m_0} \). If for some \( j \) there is no \( i \) as above, we still replace \( x \equiv a_j \pmod{m_j} \) with \( x \equiv a_j \pmod{m_0} \). Then we are left with a covering with moduli that are distinct odd numbers together with possibly powers of 2. Observe that \( \sum_{j=1}^{\infty} 1/2^j = 1 \) implies that there is an \( a \in \mathbb{Z} \) and a \( k \in \mathbb{Z}^+ \) such that no integer satisfying \( x \equiv a \pmod{2^k} \) satisfies one of the congruences in our covering with moduli a power of 2.

Denote by \( x \equiv a_j' \pmod{m_j'} \) the congruences with \( m_j' \) odd. Let \( u \) and \( v \) be integers such that
\[
2^k u + v \left( \prod m_j' \right) = 1.
\]
For any \( n \in \mathbb{Z} \), consider the number \( m = a + 2^k u (n - a) \). Then \( m \equiv n \pmod{m_j'} \) for every \( m_j' \) and \( m \equiv a \pmod{2^k} \). It follows that \( n \equiv m \equiv a_j' \pmod{m_j'} \) for some \( m_j' \). Therefore, every \( n \in \mathbb{Z} \) satisfies one of the congruences \( x \equiv a_j' \pmod{m_j'} \). So these congruences form an odd covering of the integers.