Lecture 10: A Curious Connection with the Odd Covering Problem

Definition: A *covering of the integers* is a system of congruences $x \equiv a_j \pmod{m_j}$ such that every integer satisfies at least one of the congruences.

Examples:

$x \equiv 0 \pmod 2$	$x \equiv 0 \pmod 2$	$x \equiv 0 \pmod 2$	$x \equiv 0 \pmod 2$
$x \equiv 1 \pmod 2$	$x \equiv 1 \pmod 4$	$x \equiv 2 \pmod 3$	$x \equiv 0 \pmod 3$
	$x \equiv 3 \pmod 8$	$x \equiv 1 \pmod 4$	$x \equiv 1 \pmod 4$
	$x \equiv 7 \pmod{16}$	$x \equiv 1 \pmod 6$	$x \equiv 3 \pmod 8$
	$\vdots$	$x \equiv 3 \pmod{12}$	$x \equiv 7 \pmod{12}$
			$x \equiv 23 \pmod{24}$

Open Problem 1: For every $c > 0$, does there exist a finite covering with distinct moduli and with the minimum modulus $> c$? (Erdős \$1000)

Open Problem 2 (The "Odd Covering" Problem): Does there exist a finite covering with distinct odd moduli > 1? (Erdős \$25 for "No"; Selfridge \$2000 for construction)

Theorem (Sierpinski): A positive proportion of integers k satisfy $k \cdot 2^n + 1$ is composite for all nonnegative integers n. (Maybe 78557 is the smallest such k.)

The Analogous Polynomial Problem: Find $f(x) \in \mathbb{Z}[x]$ with $f(1) \neq -1$ such that $f(x)x^n + 1$ is reducible for all $n \geq 0$.

Schinzel's Example: If $f(x) = 5x^9 + 6x^8 + 3x^6 + 8x^5 + 9x^3 + 6x^2 + 8x + 3$, then $f(x)x^n + 12$ is reducible for all $n \geq 0$.

Comments: This follows from the third covering example above. If $n \equiv 0 \pmod 2$, then $f(x)x^n + 12 \equiv 0 \pmod{x+1}$; if $n \equiv 2 \pmod 3$, then $f(x)x^n + 12 \equiv 0 \pmod{x^2+x+1}$; if $n \equiv 1 \pmod 4$, then $f(x)x^n + 12 \equiv 0 \pmod{x^2+1}$; and so on. The dual role of 12 here might be misleading. One can find an example of an $f(x) \in \mathbb{Z}^+[x]$ with 12 replaced by 4.

Schinzel's Theorem: If there is an $f(x)$ as in the analogous polynomial problem, then there is an odd covering of the integers.

Lemma 1: 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 ± 1 unless one of the following holds:

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

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

Notation: Let $\Phi_n(x)$ denote the n^{th} cyclotomic polynomial.

Lemma 2 (Apostol): Let n and m be positive integers with $n > m$. The resultant of $\Phi_n(x)$ and $\Phi_m(x)$ is divisible by a prime p if and only if n/m is a power of p.

Main Ideas for Proof of Schinzel's Theorem:

- If a system of congruences "covers" all large integers, it covers all integers.
- 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 $x \in \mathbb{Q}(\zeta_m)$.
- Suppose that $-f(x) = g(x)^p$ for some prime p and $f(x)x^n + 1$ is divisible by $\Phi_m(x)$ where $p|m$. Then $n \equiv 0 \pmod{p}$. (Use integers u and v such that $-nu + pv = 1$ and set $x = \zeta_m$.)
- It suffices to consider $f(0) \neq 0$ (as we will see). Also, $x^{2^t} + 1 = \Phi_{2^{t+1}}(x)$ irreducible for every $t \in \mathbb{Z}^+$ implies $f(x) \not\equiv 1$.
- There is a finite list of irreducible reciprocal factors that can divide $f(x)x^n + 1$ as n varies.
- For $n \geq n_0$ (for some n_0), every reciprocal factor of $F(x)$ is cyclotomic.
- There are $m_1, m_2, \dots, m_r$ such that if $n \geq n_0$ and both (i) and (ii) of Lemma 1 do not hold, then $\Phi_{m_j}(x) \big| \big(f(x)x^n + 1\big)$ for some j. Furthermore, for each $j \in \{1, 2, \dots, r\}$, we may suppose that there is an a_j such that $\Phi_{m_j}(x) \big| \big(f(x)x^{a_j} + 1\big)$.
- The condition (ii) does not hold.
- Let $\mathcal{P}$ denote the set of primes p for which $f(x)$ is minus a pth power. Remove any m_j divisible by a $p \in \mathcal{P}$ (but keep the same subscripts on m_j). The congruences $x \equiv 0 \pmod{p}$ for $p \in \mathcal{P}$ and $x \equiv a_j \pmod{m_j}$ for $j \in \{1, 2, \dots, r\}$ form a covering of the integers.
- We claim: Suppose $m_j = 2^t m_0$ and $m_i = 2^s m_0$, where m_0 is an odd integer > 1, and t and s are integers with $t > s \geq 0$. Then $a_j \equiv a_i \pmod{m_0}$.
- Define $k \in \mathbb{Z}^+ \cup \{0\}$ by $a_i + (k-1)m_i < a_j \leq a_i + km_i$ and $\ell = a_i + km_i - a_j \in [0, m_i)$. Since $\Phi_{m_i}(x)$ divides $f(x)x^{a_i + km_i} + 1$ and $\Phi_{m_j}(x)$ divides $f(x)x^{a_j} + 1$, deduce that there are $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ such that $\Phi_{m_i}(x)u(x) + \Phi_{m_j}(x)v(x) = x^\ell - 1$.
- Since $\Phi_{m_0}(x)$ divides both $\Phi_{m_i}(x)$ and $\Phi_{m_j}(x)$ modulo 2, some divisor $\Phi_{\ell'}(x)$ of $x^\ell - 1$ and $\Phi_{m_0}(x)$ have a factor in common mod 2, and the resultant of $\Phi_{m_0}(x)$ and $\Phi_{\ell'}(x)$ is even.
- Since m_0 is odd, Lemma 2 implies that ℓ'/m_0 is a power of 2. It follows that m_0 divides ℓ' and, hence, ℓ. Since m_0 also divides m_i, the definition of ℓ implies the claim.
- Replace everywhere $x \equiv a_j \pmod{m_j}$ and $x \equiv a_i \pmod{m_i}$ with $x \equiv a_j \pmod{m_0}$. If for some j there is no i as above, we still replace $x \equiv a_j \pmod{m_j}$ with $x \equiv a_j \pmod{m_0}$. Deduce that there is a covering with moduli that are distinct odd numbers together with possibly powers of 2.
- Since $\sum_{j=1}^{\infty} 1/2^j = 1$, 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 $2^k u + v\Big(\prod m'_j\Big) = 1$. 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. Hence, the congruences $x \equiv a'_j \pmod{m'_j}$ form an odd covering of the integers.