THE INDEX OF NEGATIVE ONE

THOMAS A. HULSE

Suppose \( g \) is a primitive root \((\mod n)\). As the primitive root theorem states, this occurs exactly when \( n = 2, 4, p^i \) or \( 2p^i \) where \( p \) is an odd prime. Thus a complete set of reduced residues is

\[ 1, g, g^2, \ldots, g^{\phi(n)-1}. \]

One of these must be \(-1\). Suppose \( g^k \equiv -1 \pmod n \) for \( 0 \leq k \leq \phi(n) - 1 \), then \( g^{2k} \equiv (g^k)^2 \equiv (-1)^2 \equiv 1 \pmod n \). Since \( \phi(n) \) is the order of \( g \pmod n \) we have that \( \phi(n)|2k \). But \( 2k < 2\phi(n) \) and it’s obvious \( k \neq 0 \) unless \( n = 2 \), so \( 2k = \phi(n) \) and so \( k = \phi(n)/2 \). Thus we have that for any \( n > 2 \) where primitive roots exist

\[ \text{ind}(-1) = \phi(n)/2 \pmod n \]

regardless of our choice of primitive root.

To better understand why the proof I gave in lecture was incomplete, attempt Problem 1b) in Assignment 3.

\[ \text{Date: October 9, 2014.} \]