Cissy Chen

*Prime Numbers and the Cyclicity of Groups of Units*

Cyclic groups, an integral part of group theory, can be generated by some element a (called a generator) by raising a to different powers. The group of units of Z(n) (the set of congruence classes modulo n) contains all positive integers that are relatively prime to n modulo n. This project determines which n produce cyclic groups of units of Z(n). First, I generated the first 100 groups of units using Mathematica. Then, I tested for cyclicity by raising each of the elements to different powers and comparing them to the original group of units. The results of these tests led to several conjectures characterizing the n that produce cyclic groups of units. In sum, the group of units is cyclic if and only if n is 2, 4, a power of an odd prime (pox), or twice the power of an odd prime (2pox). This theorem was proved in two parts: one, to show the groups of units under the given criteria are cyclic, and two, to show the groups of units of n not under those criteria (in which case n must be a multiple of 8 or have at least two distinct odd prime factors) are not cyclic. These results have applications in cryptography, primality testing, and molecular symmetry. Specifically, the characterization of cyclic groups is especially significant in cryptography. Many encryption systems, such as the Diffie-Hellman Key protocol, are based on the properties of cyclic groups.