The arithmetic of cyclic subgroups

Zebediah Engberg

Abstract

In this thesis, we consider several problems relating to cyclic subgroups of the unit group $(\mathbb{Z}/n\mathbb{Z})^\times$. For $n > 2$, every element of $(\mathbb{Z}/n\mathbb{Z})^\times$ has a unique representative in one of the two intervals $(0, n/2)$ and $(n/2, n)$. A subgroup H of $(\mathbb{Z}/n\mathbb{Z})^\times$ is *balanced* if every coset of H intersects these two intervals equally. For a fixed integer g, how often is the cyclic subgroup $\langle g \bmod n\rangle$ balanced? We prove a conjecture of Pomerance and Ulmer that this distribution is essentially determined by two special families of balanced subgroups.

The behavior of the cyclic subgroup $\langle 2 \bmod p\rangle$ as p ranges over odd primes is closely connected to the arithmetic of the Mersenne numbers $2^n - 1$. Let $f(n) = \sum_{p|2^n-1} 1/p$, the reciprocal sum of the primes dividing the nth Mersenne number. Erdős showed that $f(n) < \log\log\log n + C$ for some constant C. Apart from the exact value of C, this inequality is tight. Assuming the truth of a well-believed conjecture in number theory, we answer Erdős's question on the correct value of C. We also show that Erdős's theorem is still true when the Mersenne number $2^n - 1$ is replaced with the nth Fibonacci number.