LIBERTAS MATHEMATICA, VOL. 13, 1993

Classroom Notes

FINITE CYCLIC GROUPS WITH TWO OR MORE GENERATORS

Marion E. Moore

ABSTRACT. An implementation of Bertrand's conjecture is used to prove that every finite cyclic group of order greater than six has more than two generators.

The manner by which the number of generators of a finite cyclic group is usually calculated is via the Euler phi-function $\phi(n)$. One always has the trivial upper bound for $\phi(n)$, namely $\phi(n) \leq n-1$, $n>1$, with equality holding of course when n is prime. However, a lower bound for $\phi(n)$ is not so immediate ([1], p. 114).

In 1845, Bertrand showed (empirically) that there is a prime between n and $2n$ for $1<n<6{,}000{,}000$, and thusly conjectured this to be the case for all natural numbers n larger than 1. In 1850, Chebyshev settled Bertrand's Conjecture in the affirmative, and in fact, showed that for every $a>1/5$ there is a b such that for each $x>b$ there is a prime between x and $(1+a)x$. This last theorem has since been proved for every $a>0$ (again, see [1], p. 108).

In this note we furnish an alternative proof to the fact that every finite cyclic group of order greater than six has more than two generators. Our proof, which is devoid of the Euler ϕ-function, relies instead on Bertrand's Conjecture.

To prove the result, it clearly suffices to consider $\mathbf{Z}_m$, $m>6$. In any case, $\overline{1}$ and $\overline{m-1}$ are generators of $\mathbf{Z}_m$. If m is prime or twice a prime, then the result follows by noting that $\pm\overline{1}$ and $\pm\overline{3}$ are generators. If m is not

of this form, then let q be the largest prime divisor of m. Then $2q < m$ and by Bertrand's Conjecture there is a prime p with $q < p < 2q < m$. Since $p \nmid m$, $\mathbb{Z}_m = \langle \overline{p} \rangle$, and the proof is complete.

Clearly, it follows that a cyclic group G has exactly two generators if and only if G is isomorphic to one of $\mathbb{Z}, \mathbb{Z}_3, \mathbb{Z}_4$ or $\mathbb{Z}_6$.

Acknowledgement. The author wishes to acknowledge Wynne Johnson for initially stimulating the author's interest in this problem and to an unknown referee.

Reference.

[1] W. J. Leveque, Topics in Number Theory, Vol. 1, Addison-Wesley, 1956.