# Unique factorization via cyclic groups

Paul Pollack

The fundamental theorem of arithmetic states that every natural number factors uniquely as a product of prime numbers. Since the time of Euclid, it has been usual to base the proof of this result on the following key property of prime numbers:

Euclid's Lemma. *Suppose that $a$ and $b$ are natural numbers and that $p$ is a prime number. If $p \mid ab$, then either $p \mid a$ or $p \mid b$.*

The purpose of this note is to advertise a proof of Euclid's Lemma which relies only on the most basic properties of finite cyclic groups. Let $\mathbf{Z}_n$ denote the integers modulo $n$, considered as an additive group, and let $[m]$ denote the equivalence class of $m$ modulo $n$.

Proof of Euclid's Lemma. Suppose that $p \mid ab$ but that $p \nmid a$; we show that $p \mid b$. Since $p \mid ab$, one has that $m := ab/p \in \mathbf{Z}$. Since $a \mid ab = pm$, it follows that the order of $[m]$ in the group $\mathbf{Z}_a$ divides $p$. Hence, this order is 1 or $p$. The order cannot be $p$, since $p \nmid |\mathbf{Z}_a|$. Thus, $[m]$ is the identity element of $\mathbf{Z}_a$, i.e., $[m] = [0]$. Hence $a \mid m = ab/p$. But then $\frac{ab/p}{a} = \frac{b}{p} \in \mathbf{Z}$, so that $p \mid b$. $\square$

This proof eschews developing the theory of the greatest common divisor. Of course, we have not entirely avoided the division algorithm, which is needed to establish the few group-theoretic results employed above. Nevertheless, it seems of some interest that the so much can be hidden in plain sight!

University of British Columbia, Department of Mathematics, Room 121, 1984 Mathematics Road, Vancouver, BC Canada V6T 1Z2

Simon Fraser University, Mathematics Department, Burnaby, BC Canada V5A 1S6

*E-mail address*: pollack@math.ubc.ca