Two nontraditional approaches to the fundamental theorem of arithmetic

Paul Pollack

The fundamental theorem of arithmetic states that every natural number factors uniquely as a product of prime numbers. Perhaps the most familiar proof involves showing (implicitly or explicitly) that every ideal of the ring $\mathbf{Z}$ of integers is principal (see, e.g., Hardy and Wright §§2.9–2.10).

The purpose of this mininote is to highlight two nonstandard approaches approaches to the fundamental theorem where the division algorithm takes a backseat to elementary group and ring theory. (One might say that the division algrorithm is thus hidden in plain sight.) We use only the simplest concepts and results from these subjects, such as the order of an element in a finite group dividing the size of the group.

Actually we do not prove the fundamental theorem in its entirety. Instead, we concentrate our efforts on the following result, which might be called the fundamental lemma for the fundamental theorem. The proof of unique factorization can then be completed as in the usual treatments (see, e.g., §2.10 of Hardy and Wright)

Lemma 1. *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 $p \mid b$.*

First proof of Lemma 1. 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 $p \mid b$. □

Another non-traditional approach to Lemma 1 goes through the following result.

Lemma 2. *Let p be a prime number. If G is a group whose order is divisible by p, then the number of elements of G of order dividing p is a multiple of p.*

Proof. The proof is well-known to those who know it well, but we include it to dispel any fears that Lemma 1 is being smuggled in. Since we do not assume G is abelian, we write G multiplicatively. Consider the set S of all p-tuples $(g_1, g_2, \dots, g_p)$ of elements of G whose product $g_1 g_2 \cdots g_p$ is the identity. Then $|S| = |G|^{p-1}$, since $g_1, \dots, g_{p-1}$ can be chosen arbitrarily if we set $g_p = (g_1 \cdots g_{p-1})^{-1}$.

Next, observe that S is closed under cyclic permutations. Calling two elements of S equivalent if they differ by a cyclic permutation, the equivalence classes all have size 1 or

p. (Here is where we use that p is prime.) The equivalence classes of size 1 are in one-to-one correspondence with elements of S of the form $(g, \dots, g)$, i.e., elements $g \in G$ of order dividing p. Thus, the number of elements of order dividing p is congruent, modulo p, to $|G|^{p-1}$. Since $p \mid |G|$ by hypothesis, the result follows. □

Second proof of Lemma 1. Apply Lemma 2 to the symmetric group on p letters, which has order $p!$. The elements of order dividing p are precisely the identity and the p-cycles, the latter of which number $(p-1)!$. Hence, $p \mid 1 + (p-1)!$, or

$$[(p-1)!] = [-1] \quad \text{in } \mathbf{Z}_p. \tag{1}$$

This last result is known in number-theoretic circles as Wilson's Theorem. (The usual proofs of this result rely on Lemma 1, but the above proof – found by F. Gerrish in 1972 – avoids this!) Viewing (1) now as taking place in the *ring* $\mathbf{Z}_p$, we have that

$$\prod_{\substack{\beta \neq 0 \\ \beta \in \mathbf{Z}_p}} \beta = [(p-1)!] = [-1].$$

Since $[-1]$ is a unit in $\mathbf{Z}_p$, it follows that each nonzero $\beta \in \mathbf{Z}_p$ is a unit. That is, $\mathbf{Z}_p$ is a field. Thus, $\mathbf{Z}_p$ is an integral domain; but that is just another way of phrasing Lemma 1. □

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

E-mail address: pppollac@illinois.edu