A dynamical systems proof of an elementary number theory result

Ulises Morales-Fuentes (ulises.morales@uaem.mx) and Rogelio Valdez (valdez@uaem.mx), Universidad Autónoma del Estado de Morelos, and Enrique Treviño (trevino@lakeforest.edu), Lake Forest College

For two positive integers n, m, the identity $nm = \gcd(n, m)\text{lcm}(n, m)$ is a classic elementary number theory exercise usually proved using the Fundamental Theorem of Arithmetic. In this capsule, our aim is to prove the statement using ideas from dynamical systems.

Before we get to our proof, we need to recall a few definitions from dynamical systems.

Definition. For a function $f : A \to B$, $z \in A$ is a periodic point of period k for the function f if $f^k(z) = z$ and $f^j(z) \neq z$ for all $j < k$, where f^k denotes the composition of f with itself k times.

Given $z \in A$, the set $\mathcal{O}_f(z) = \{w \in A \,:\, w = f^k(z) \text{ for } k \text{ a nonnegative integer}\}$ is the *orbit* of z under f. In the case that z is periodic, this set is finite and it is called the periodic orbit of z.

We are now ready for our proof.

Theorem 1. *Let n, m be positive integers, then $nm = \gcd(n, m)\text{lcm}(n, m)$.*

Proof. Consider $f : \mathbb{C} \to \mathbb{C}$ defined by $f(z) = z^2$. Note that $f^n(z) = z^{2^n}$. Take ζ to be a $(2^n - 1)$-th primitive root of unity, then $\zeta^{2^n} = \zeta$ and so $z_0 = \zeta$ is a periodic point of period n for f (the orbit is $\{\zeta, \zeta^2, \zeta^4, \zeta^8, \ldots, \zeta^{2^{n-1}}\}$). Similarly, if ω is a $(2^m - 1)$-th primitive root of unity, then $w_0 = \omega$ is a periodic point of period m for f.

Let $A = \{z_0, z_1, \ldots, z_{n-1}\}$ be the orbit of z_0 and $B = \{w_0, w_1, \ldots, w_{m-1}\}$ be the orbit of w_0, where $z_i = \zeta^{2^i}$ and $w_j = \omega^{2^j}$. Let $F : A \times B \to A \times B$ be defined as $F(a, b) = (f(a), f(b))$. We will show that F has $\gcd(n, m)$ periodic orbits generated by A and B, all of period $\text{lcm}(n, m)$. Note that this will imply our theorem.

Given $z_i \in A$ and $w_j \in B$, then as the periods of z_i and w_j under f are n and m, respectively, the orbit of (z_i, w_j) under F has period $M = \text{lcm}(n, m)$. To see this, observe first that $F^M(z_i, w_j) = (f^M(z_i), f^M(w_j)) = (f^{nk_1}(z_i), f^{mk_2}(w_j)) = (z_i, w_j)$ as z_i has period n and w_j has period m, where $M = nk_1 = mk_2$. Now, in order to see that M is the minimal integer with the previous property, suppose that there is a positive integer $t < M$ so that $F^t(z_i, w_j) = (f^t(z_i), f^t(w_j)) = (z_i, w_j)$. As z_i has period n and w_j has period m, then t is a multiple of n and m, which contradicts the minimality of M.

Let $d = \gcd(n, m)$. Let O_k be the orbit of the point (z_0, w_k). We will show $(z_i, w_j) \in O_k$ if and only if $j - i \equiv k \bmod d$.

Suppose $(z_i, w_j) \in O_k$. Then there exists an integer ℓ such that $F^\ell(z_0, w_k) = (z_i, w_j)$. But then $\ell \equiv i \bmod n$ and $\ell + k \equiv j \bmod m$. Therefore, there exist integers r, s such that

$$rn + i = \ell = (j - k) + sm. \tag{1}$$

We can write n and m as dn' and dm', respectively, with $\gcd(n', m') = 1$. Then (1) implies

$$d(n'r - m's) = j - k - i. \tag{2}$$

It follows that $d|(j-k-i)$, so $j - i \equiv k \bmod d$.

Now suppose $j - i \equiv k \bmod d$, then $j - i - k = du$ for some integer u. By Bézout's identity ([**2**, Theorem 25]), there exists integers x, y such that $n'x + m'y = 1$, so let $r = xu$ and $s = -yu$, and we have that (2) is satisfied, so $F^{\ell}(z_0, w_k) = (z_i, w_j)$. Therefore, (z_i, w_k) is in the orbit of O_k.

Then the orbits $O_0, O_1, \ldots, O_{d-1}$ partition $A \times B$. It follows that there are exactly d orbits, each of which has M elements, so $Md = nm$ as we wanted to show. ■

Remark. Our proof required Bezout's identity, a key ingredient in the standard proof that factorization of integers greater than 1 into prime factors is unique up to ordering (the uniqueness component of the Fundamental Theorem of Arithmetic).

References

1. Alan F. Beardon, *Iteration of rational functions*, Graduate Texts in Mathematics, vol. 132, Springer-Verlag, New York, 1991, Complex analytic dynamical systems. MR 1128089
2. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, sixth ed., Oxford University Press, Oxford, 2008, Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles. MR 2445243
3. John Milnor, *Dynamics in one complex variable*, third ed., Annals of Mathematics Studies, vol. 160, Princeton University Press, Princeton, NJ, 2006. MR 2193309

