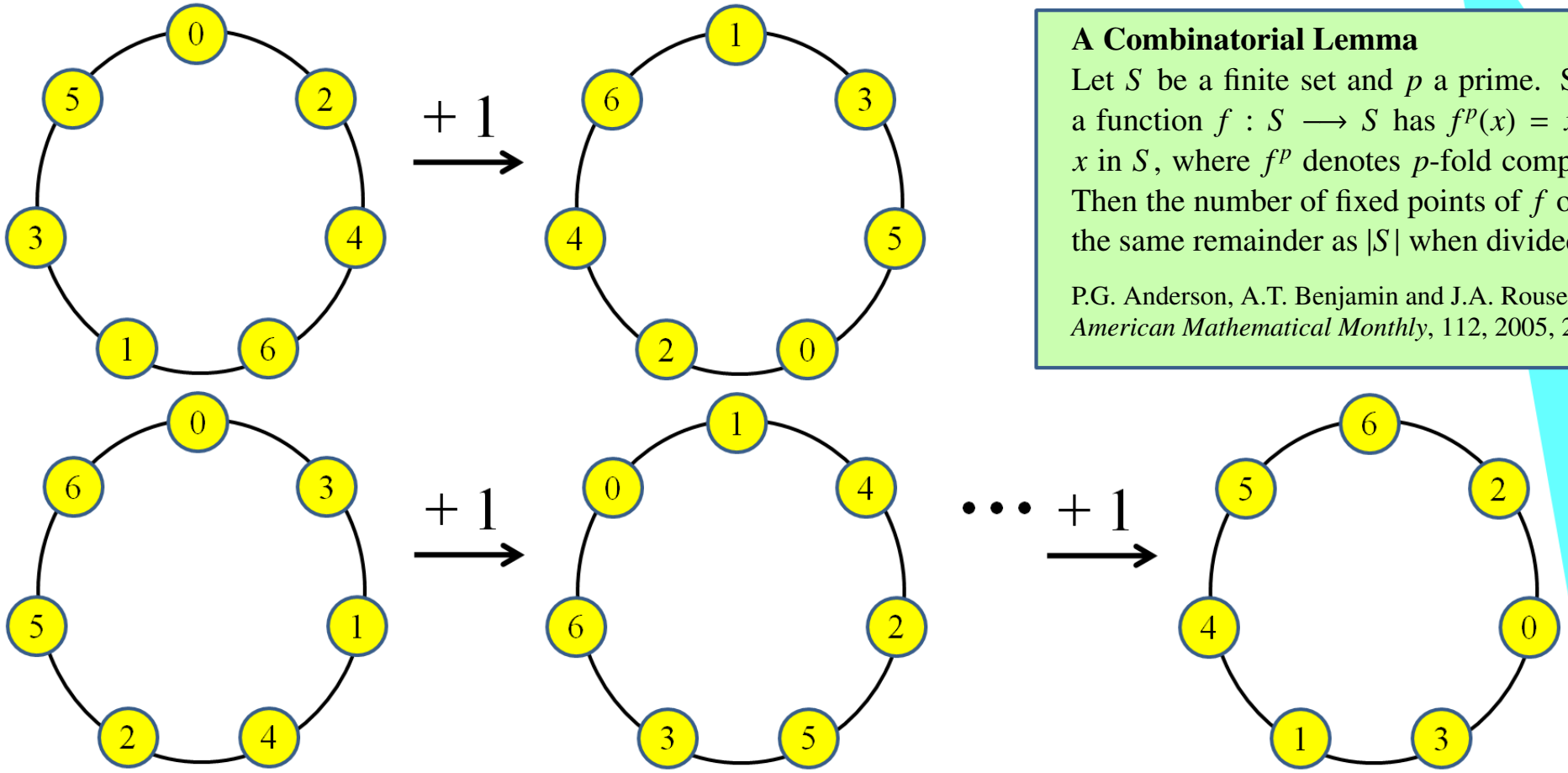
THEOREM OF THE DAY

Wilson's Theorem *An integer $n > 1$ is prime if and only if $(n-1)!$ has remainder $n-1$ on division by n.*



A Combinatorial Lemma

Let S be a finite set and p a prime. Suppose a function $f : S \longrightarrow S$ has $f^p(x) = x$ for all x in S, where f^p denotes p-fold composition. Then the number of fixed points of f on S has the same remainder as $|S|$ when divided by p.

P.G. Anderson, A.T. Benjamin and J.A. Rouse
American Mathematical Monthly, 112, 2005, 266–268

E.g.

$$\frac{6!}{7} = \frac{720}{7} = \frac{714+6}{7} = 102 \text{ rem. } 6$$

Let S be the set of cycles of length n. Define f to be the function which adds 1 to every cycle element, reducing modulo n as necessary. In the illustration above, where $n = 7$, the top two cycles are identical under this function, except for a cyclic shift, so we say that (0 2 4 6 1 3 5) is a fixed point of f. There are precisely $n-1$ such fixed points because they are precisely the cycles of the form $(0\ a\ 2a\ 3a \ldots (n-1)a)$ for $1 \le a \le n-1$ (the above fixed point cycle uses $a = 2$, reducing modulo 7). We check that n-fold composition leaves a cycle unchanged: indeed, it just adds n to every element (the bottom cycles above show the situation after $n-1$ compositions: one more returns us to the start). So if n is prime, the Combinatorial Lemma applies: $n-1$ has the same remainder on division by n as $|S|$. And $|S|$ is exactly $(n-1)!$ because fixing 0 at the top of a cycle, to avoid double-counting cyclic shifts, there are $(n-1)!$ ways to rearrange the remaining $n-1$ elements.

The 'only if' part, proved above, attributed by Edward Waring in 1770 to his student John Wilson, was known to Leibniz many years, and to Ibn al-Haytham many centuries, earlier. The first published proof is by Lagrange, 1771, who adjoins the (easy) 'if' half. Gauss, aged 21, gave an extension to arbitrary positive integers in his classic *Disquisitiones Arithmeticae* of 1798.

Web link: Anderson et al, www.cs.rit.edu/~pga/abstracts.php ("Combinatorial Proofs of ..."), gives the above and proofs of two other theoremsoftheday. For the same approach in a group theoretic setting see: qchu.wordpress.com/2013/07/09.

Further reading: *Proofs that Really Count: The Art of Combinatorial Proof* by Arthur Benjamin &Jennifer Quinn, MAA, 2003, chapter 8.