1056-BB-632 **Ira M. Gessel*** (gessel@brandeis.edu), Department of Mathematics, MS 050, Brandeis University, Waltham, MA 02453. *Combinatorial Proofs of Congruences.*

In 1872, Julius Petersen published a frequently rediscovered combinatorial proof of Fermat's theorem $a^p \equiv a \pmod p$, where $p$ is a prime: If we color the spokes of a $p$-spoke wheel in $a$ colors, and call two colorings equivalent if one can be rotated into the other, then every equivalence class contains $p$ colorings except for the $a$ equivalence classes consisting of a single monochromatic coloring. Petersen gave a similar proof of Wilson's theorem $(p-1)! \equiv -1 \pmod p$, and Lucas's theorem $\binom{ap+b}{cp+d} \equiv \binom{a}{c}\binom{b}{d} \pmod p$, where $0 \le b, d < p$ can be proved by the same idea: if a group of order $p$ (or a power of $p$) acts on finite set $S$ then the size of every orbit is either 1 or a multiple of $p$, so $|S|$ is congruent modulo $p$ to the number of fixed points.

I will describe how this approach can be applied to find congruences for Bell numbers, derangement numbers, and other sequences of combinatorial interest. (Received September 15, 2009)