COMBINATORIAL PROOFS OF FERMAT'S, LUCAS'S, AND WILSON'S THEOREMS

PETER G. ANDERSON, ARTHUR T. BENJAMIN, AND JEREMY A. ROUSE

In this note, we observe that many classical theorems from number theory are simple consequences of the following combinatorial lemma.

Lemma 1. *Let S be a finite set, let p be prime, and suppose $f : S \to S$ has the property that $f^p(x) = x$ for any x in S, where f^p is the p-fold composition of f. Then $|S| \equiv |F| \pmod{p}$, where F is the set of fixed points of f.*

Proof. S is the disjoint union of sets of the form $\{x, f(x), \dots, f^{p-1}(x)\}$. Since p is prime, each set either has size one or size p. $\diamond$

The Lucas numbers, $2, 1, 3, 4, 7, 11, 18, 29, 47, \dots$, named in honor of Edouard Lucas (1842-1891), are defined by $L_0 = 2$, $L_1 = 1$, and $L_n = L_{n-1} + L_{n-2}$ for $n \geq 2$. It is easy to show that, for $n \geq 1$, L_n counts the ways to create a bracelet of length n using beads of length one or two, where bracelets that differ by a rotation or a reflection are still considered distinct. For example, there are four bracelets of length three. (Such a bracelet can have three beads of length one, or it can have a bead of length two and a bead of length one, where the bead of length one can be in position one, two, or three.) Let f act on bracelets of prime length p by rotating each bead clockwise one unit. Clearly f^p leaves any bracelet unchanged. Since f has just one fixed point (when all beads have length one), we conclude that $L_p \equiv 1 \pmod{p}$ for each prime p.

More generally, as defined in [4], for nonnegative integers a and b, the *Lucas sequence (of the second kind)* is defined by $V_0 = 2, V_1 = a$, and $V_n = aV_{n-1} + bV_{n-2}$ for $n \geq 2$. Again, it is easy to show [1] that V_n with $n \geq 1$ counts colored bracelets of length n, where there are a color choices for beads of length one and b color choices for beads of length two. By the same argument as earlier, with the exception of those bracelets consisting of length one beads all of the same color, when p is prime every bracelet can be rotated to create p distinct bracelets. Thus, for p prime,

$$V_p \equiv a \pmod{p}.$$

In the special case where $b = 0$, it is clear that $V_p = a^p$. Consequently, we have *Fermat's Theorem:* If p is a prime, then

$$a^p \equiv a \pmod{p}.$$

This combinatorial proof of Fermat's theorem was originally given in [2].

Next, consider colored bracelets of length pk, where p is prime. If we rotate the beads k units at a time, then there are exactly V_k fixed points, obtained by taking any colored bracelet of length k and "replicating" it p times. Our lemma concludes that for p prime

$$V_{pk} \equiv V_k \pmod{p}.$$

In particular, $V_{p^e} \equiv V_{p^{e-1}}$ when $e \geq 1$. Consequently, for p prime, and e nonnegative,

$$V_{p^e} \equiv a \pmod{p}.$$

Now consider the set S of permutations of $\{0, 1, \ldots, p-1\}$ with exactly one cycle; thus, $|S| = (p-1)!$. Define $f : S \to S$ by $f((a_0, a_1, \ldots, a_{p-1})) = (1 + a_0, 1 + a_1, \ldots, 1 + a_{p-1})$, where addition is done modulo p. For each π in S, $f^p(\pi) = \pi$. For a satisfying $1 \leq a \leq p-1$ those permutations of the form $\pi_a = (0, a, 2a, 3a, \ldots, (p-1)a)$ (with multiplication done modulo p) are fixed points of f since $f(\pi_a)$ remains an "arithmetic progression." Conversely, if π is a fixed point of f and $\pi(0) = a$, then $\pi = f^a(\pi)$ must send a to $2a$ and, in general, $\pi = f^{ka}(\pi)$ sends ka to $(k+1)a$. Thus $\pi = \pi_a$, and f has exactly $p-1$ fixed points. This establishes *Wilson's Theorem:* If p is a prime, then

$$(p-1)! \equiv (p-1) \pmod{p}.$$

The same approach can be applied to the set S of k-element subsets of $\{0, 1, \ldots, p-1\}$. Define $f : S \to S$ by $f(\{a_1, a_2, \ldots, a_k\}) = \{1 + a_1, 1 + a_2, \ldots, 1 + a_k\}$, where again addition is done modulo p. When $1 \leq k \leq p-1$ there are no fixed points of f. Consequently, for p prime and k satisfying $1 \leq k \leq p-1$,

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

We conclude with *Lucas's Theorem:* For p prime, let n and k have base p notation $n = \sum_{i \geq 0} b_i p^i$ and $k = \sum_{i \geq 0} c_i p^i$, where $0 \leq b_i, c_i < p$. Then

$$\binom{n}{k} \equiv \prod_{i \geq 0} \binom{b_i}{c_i} \pmod{p}.$$

Proof. It suffices to show $\binom{pn+r}{pk+s} \equiv \binom{n}{k}\binom{r}{s} \pmod{p}$, for $0 \leq r, s < p$, and then proceed inductively. Let S denote the set of ordered pairs (A, v), where A is a binary $p \times n$ matrix and v is a binary $r \times 1$ vector, such that among the $pn + r$ entries of A and v, exactly $pk + s$ are equal to one. Hence $|S| = \binom{pn+r}{pk+s}$. Let Q denote the $p \times p$ permutation matrix with nonzero entries $q_{1p} = 1$ and $q_{i,i-1} = 1$ for $i = 2, 3, \ldots, p$. Thus QA has the same rows as A, each shifted "down" by one row.

Define $f : S \to S$ by $f((A, v)) = (QA, v)$. Thus $f^p((A, v)) = (Q^p A, v) = (A, v)$. There are $\binom{n}{k}\binom{r}{s}$ fixed points of f, consisting of those pairs (A, v) such that the first row of A contains exactly k ones, the other rows of A are the same as the first row, and v contains exactly s ones in its r positions. Note that if $s > r$, then $\binom{r}{s} = 0$. Thus, by our lemma, $\binom{pn+r}{pk+s} \equiv \binom{n}{k}\binom{r}{s} \pmod{p}$, as desired. ◇

For another fine combinatorial proof of Lucas's theorem, see [3].

ACKNOWLEDGMENT. The authors gratefully acknowledge valuable suggestions from David Gaebler and the anonymous referee.

References

[1] A. T. Benjamin and J. J. Quinn, *Proofs That Really Count, The Art of Combinatorial Proofs,* Mathematical Association of America, Providence, 2003.

[2] L. E. Dickson, *History of the Theory of Numbers,* vol. 1, Carnegie Institution of Washington, Washington, D.C., 1919.

[3] N. J. Fine, Binomial coefficients modulo a prime, *Amer. Math. Monthly* **54** (1947) 589–592.

[4] P. Ribenboim, *The Little Book of Big Primes.* Springer-Verlag, New York, 1991.

Department of Computer Science, Rochester Institute of Technology, Rochester, NY 14623-5608
E-mail address: anderson@cs.rit.edu

Department of Mathematics, Harvey Mudd College, Claremont, CA 91711
E-mail address: benjamin@hmc.edu

Department of Mathematics, University of Wisconsin, Madison, WI 53706
E-mail address: rouse@math.wisc.edu