CLASSROOM NOTES

EDITED BY G. B. THOMAS, Massachusetts Institute of Technology

Because of the large number of papers on hand, consideration of new papers for this department has been temporarily suspended.

COMBINATORIAL PROOF OF FERMAT'S "LITTLE" THEOREM

S. W. GOLOMB, University of Oslo

It is possible to give an interesting, purely combinatorial proof of Fermat's theorem that n^p-n is divisible by p, for any positive integer n, and any prime number p.

Suppose we have beads in n different colors, and we wish to make necklaces using exactly p beads. First we put p beads on a string. Since each of the beads can be chosen in n ways, there are n^p possible strings. For each of the n colors, there is one string entirely of that color. We throw these away, leaving n^p-n strings. We will join the two ends of each of these strings to form necklaces. But we observe that if two strings differ only by a cyclic permutation of the beads, the resulting necklaces will be indistinguishable. Since there are p cyclic permutations of the p beads on a string, the number of *distinguishable* necklaces is $(n^p-n)/p$, which must therefore be an integer.

If it is permitted to flip the necklaces over, there are only $(n^p-n)/2p$ distinguishable cases, so that this too must be an integer, unless $p=2$.

If this proof is used in the classroom, it is of pedagogic value to ask the class:

1) Where is the hypothesis that p is prime used in the proof?

and

2) In view of the fact that there are $n!$ ways to permute the n colors, is it further true that $n!$ divides $(n^p-n)/p$?

A somewhat analogous combinatorial proof of Wilson's Theorem is given by R. D. Carmichael (*The Theory of Numbers*, p. 50), who shows that $((p-1)!-(p-1))/2p$ is the precise number of distinct irregular stellated p-gons.

CONGRUENCES AND CARD SHUFFLING

PAUL B. JOHNSON, Occidental College

Congruences are some of the most powerful tools in the theory of numbers, yet they are among the more difficult to motivate. To the beginning student the usual illustrations appear either absurdly simple, or merely tricky manipulations set up to illustrate this particular theory.

The majority of people in the United States will immediately recognize the following illustration as a serious and significant problem in its own right, and yet it is one easily solved using congruences but is very difficult without them. The illustration is the simple question "How thoroughly does the ordinary riffle shuffle mix up the cards in a bridge deck?" The average person thinks a pure riffle shuffle thoroughly mixes the cards, implying that all of the 52! or 8×10^{67}