A short proof of one of Fermat's theorems.

Consider the n^p distinct "words" of p "characters" that can be formed from an "alphabet" of n distinct characters. Draw from each word an arrow to the word that is obtained by rotating its characters over one place to the left, i.e. from $n_0, n_1, \ldots, n_{p-1}$ an arrow is drawn to $n_1, \ldots, n_{p-1}, n_0$. Because p successive rotations transform a word into itself, the arrows form cycles of lengths that are divisors of p.

Hence, if p is prime, 1 and p are the only possible cycle lengths. Because a cycle of length 1 corresponds to a word all characters of which are equal, exactly n distinct words occur in a cycle of length 1. Hence the remaining $n^p - n$ words occur in cycles of length p, i.e. for any n and any prime p, $n^p - n$ is a multiple of p.

Plataanstraat 5
5671 AL NUENEN
The Netherlands

27 May 1980

prof. dr. Edsger W. Dijkstra
Burroughs Research Fellow.