<u>A sequel to EWD740</u>

For some p we define "rings" as circular arrangements of the numbers from 0 through $p-1$. By "circular" we mean that rotation of an arrangement does not change the ring it represents (e.g. 02341 and 34102 represent the same ring). Obviously, there are $(p-1)!$ different rings. From each ring we draw an arrow towards the ring one obtains when each number is increased by 1, <u>mod</u> p. Because a succession of p such transformations transforms a ring into itself, the arrows form cycles the lengths of which 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 ring with a constant difference <u>mod</u> p between each number and its clockwise neighbour and that difference may range from 1 through $p-1$, exactly $p-1$ rings occur in a cycle of length 1. Hence, the remaining $(p-1)!-(p-1)$ rings occur in cycles of length p, i.e. for any prime p $(p-1)!-(p-1)$ is a multiple of p.

Plataanstraat 5
5671 AL NUENEN
The Netherlands

30 May 1980

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