From Mathematics to Generic Programming

Brooks Mershon

March 2017

5.1

Solution.

Let us first expand the factorial:

$$(n-1)! = (n-1)(n-2)(n-3)\cdots(n-(n-1))$$

We know n is composite, which means we can either find two positive integers a and b, both less than n which when multiplied together give us n, *or* we may find n is a composite number equal to a^2.

In the first case, we can simply choose the numbers a and b from the set $\{n-1, n-2, n-3, \ldots, 1\}$. These two integers do appear as factors in the expanded factorial, so we know (n - 1)! is a multiple of n.

In the latter case, we need two "copies" of some factor a. What to do, since we only have a set of integers in the interval $[1, n-1]$? Since we are looking to show that $(n-1)! = mn$ for some multiple m of n, we can (when $n > 4$) go ahead and just multiply a by $2a$ in order to obtain a multiple of n among the factors multiplied together in the expanded factorial. We are guaranteed when $n > 4$ that the factor 2 exists for us to choose from when forming $2a$.

In both cases we have produced a multiple of n (or simply n itself) and then expect to multiply this multiple by whatever other factors were not used in our explicit construction.