Name:

Problem 1: *What is the remainder when* 17! *is divided by* 19*?*
Hint: Use Wilson's theorem.

Solution:
Solution 1: By Wilson's Theorem, we have

$$18! \equiv -1 \pmod{19}$$

We have

$$18! = 17! \cdot 18 \equiv -17! \pmod{19}.$$

Therefore

$$-17! \equiv -1 \pmod{19}.$$

Since -1 is a unit in $\mathbb{Z}/19\mathbb{Z}$, we can divide both sides by -1 and

$$17! \equiv 1 \pmod{19}.$$

Therefore the remainder is 1.

Solution 2: We have show in class that the congruence classes

$$2, 3, \ldots (p-3), (p-2)$$

break up into $\frac{p-3}{2}$ pairs of residue classes (a, b) such that

$$ab \equiv 1 \pmod{p}.$$

Therefore

$$2 \cdot 3 \cdots (p-3) \cdot (p-2) \equiv 1 \pmod{p}$$

and multiplying both sides by 1 we have

$$(p-2)! = 1 \cdot 2 \cdots (p-3) \cdot (p-2) \equiv 1 \pmod{p}.$$

When $p = 19$, this is

$$17! \equiv 1 \pmod{19}$$

and again the remainder is 1.