1. Do problems 5.3: 1b, 2, 3, 5, 7, 16

2. As we saw in class, when $p > 3$ is prime it follows that $(p-1)! \equiv -(2 \cdot 3 \cdots (p-2)) \pmod{p}$, so to prove that $(p-1)! \equiv -1 \pmod{p}$ it is enough to show that $2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}$. We do this as follows:

a) For each $a \in \{2, \ldots, (p-2)\}$ let $S_a = \{ b \in \{2, \ldots, (p-2)\} \mid ab \equiv 1 \pmod{p} \} \cup \{a\}$. Argue that $S_a \neq \emptyset$ for all $a \in \{2, \ldots, (p-2)\}$.

b) Argue that $S_a \subseteq \{2, \ldots, (p-2)\}$, for all $a \in \{2, \ldots, (p-2)\}$.

c) Argue that $\bigcup_{a \in \{2, \ldots, (p-2)\}} S_a = \{2, \ldots, (p-2)\}$.

d) Prove that for all $a, b \in \{2, \ldots, (p-2)\}$, either $S_a \cap S_b = \emptyset$ or $S_a = S_b$.

e) It follows (by definition) that $\{S_a \mid a \in \{2, \ldots, (p-2)\}\}$ is a partition of $\{2, \ldots, (p-2)\}$. Argue that there are $a_1, \ldots, a_r \in \{2, \ldots, (p-2)\}$ such that $\{2, \ldots, (p-2)\}$ is equal to the disjoint union of $S_{a_1}, \ldots, S_{a_r}$.

f) Prove that $|S_a| = 2$ for all $a \in \{2, \ldots, (p-2)\}$.

g) Prove that for all $i \in \{1, \ldots, r\}$, \[ \prod_{a \in S_{a_i}} a = 1. \]

h) Conclude that $2 \cdot 3 \cdots (p-2) = \prod_{a \in \{2, \ldots, (p-2)\}} a = \prod_{i=1}^{r} \left( \prod_{a \in S_{a_i}} a \right) \equiv \prod_{i=1}^{r} (1) = 1 \pmod{p}$ as required.

3. Do problems from 6.1: 8

The grader will carefully consider 5.3.5 and 5.3.16.