Bonus problem solutions 1

Bonus problem (not graded). Let p be an odd prime. Prove that p divides $(p-1)!+1$.

Solution. The key here is that every element of $\{1, 2, \ldots, p-1\}$ has an inverse modulo p. So we can pair up each element $a \in \{1, 2, \ldots, p-1\}$ with some other element b in the same set, such that $ab \equiv 1 \pmod{p}$. Then in the product

$$(p-1)! = (p-1) \cdot (p-2) \cdots 2 \cdot 1,$$

the terms a and b cancel out $\pmod{p}$.

The exceptions are that 1 and $p-1$ are their own inverses, so they do not pair with anything, so in the product we are left with

$$(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}.$$

To verify that 1 and $p-1$ are the only elements are their own inverses, we note that x being its own inverse is equivalent to $x^2 \equiv 1 \pmod{p}$, or $(x-1)(x+1) \equiv 0 \pmod{p}$. Since p is prime, this implies $x \equiv 1$ or $-1 \pmod{p}$.

This is known as Wilson's theorem.

Bonus problem (not graded). Let $n > 1$ be a positive integer. Prove that n does not divide $2^n - 1$.

Solution. Assume for the sake of contradiction that $n | 2^n - 1$. Let p be the smallest prime dividing n. Then $2^n \equiv 1 \pmod{p}$.

Let h be the order of 2 $\pmod{p}$, i.e., h is the order of 2 as an element of the group $(\mathbb{Z}/p\mathbb{Z})^\times$. Recall that this means that h is the smallest positive integer such that $2^h \equiv 1 \pmod{p}$. Note that $h > 1$.

By properties of orders, we have $h | n$ since $2^n \equiv 1 \pmod{p}$ by assumption. Also, by Fermat's little theorem (or Lagrange's theorem), we have that $h | p-1$. This means that $1 < h < p$ and $h | n$. But then n must have a prime divisor which is less than p, which is a contradiction.

Note that it is necessary to consider the *smallest* prime p dividing n, and not just any prime dividing n, in order to arrive at the contradiction in the last step.

Bonus problem (not graded). Find the smallest integer n such that S_n contains a subgroup isomorphic to D_{1013}, the dihedral group with 2026 elements.

Solution. The answer is $n = \boxed{1013}$. First note that there is an injective map $D_{1013} \to S_{1013}$ given by the action of D_{1013} on the vertices of a regular 1013-gon, so S_{1013} does contain a subgroup isomorphic to D_{1013}.

In addition, if S_n has a subgroup isomorphic to D_{1013}, then by Lagrange's theorem, 2026 must divide the order of S_n, which is $n!$. Since $2026 = 2 \cdot 1013$, and 1013 is prime, 1013 divides $n!$ only if $n \geq 1013$.