Math 115A Homework 6

1) Let \( n \in \mathbb{Z} \) with \( n > 1 \). Prove that \( n \) is a prime number if and only if \( (n - 2)! \equiv 1 \pmod{n} \).

2) Let \( p \) be an odd prime number.
   a) Prove that \( \left(\frac{p-1}{2}\right)! \equiv (-1)^{(p+1)/2} \pmod{p} \).
   b) If \( p \equiv 1 \pmod{4} \), prove that \( \left(\frac{p-1}{2}\right)! \) is a solution of the quadratic congruence \( x^2 \equiv -1 \pmod{p} \).
   c) If \( p \equiv 3 \pmod{4} \), prove that \( \left(\frac{p-1}{2}\right)! \) is a solution of the quadratic congruence \( x^2 \equiv 1 \pmod{p} \).

3) Using Fermat’s Little Theorem, find the residue \( \pmod{m} \) of each integer \( n \) below
   a) \( n = 29^{202}, m = 13 \).
   b) \( n = 71^{71}, m = 17 \).
   c) \( n = 3^{1000000}, m = 19 \).

4) Let \( n \) be an integer. Prove that \( n^{21} \equiv n \pmod{30} \).

5) Let \( a \) and \( b \) be integers not divisible by the prime number \( p \).
   a) If \( a^p \equiv b^p \pmod{p} \), prove that \( a \equiv b \pmod{p} \).
   b) If \( a^p \equiv b^p \pmod{p} \), prove that \( a^p \equiv b^p \pmod{p^2} \).

6) How difficult was this homework? How long did it take?