1.
   - Show that $a = 833$ and $b = 372$ are relatively prime. Find s and t such that $as + bt = 1$ by the extended Euclidean algorithm.
   - What is the multiplicative inverse of 372 modulo 833?
   - Find a number a such that $a = 17 \pmod{372}$ and $a = 38 \pmod{833}$.
2. Find at least 8 roots to $x^2 = 1 \pmod{231}$. **Hint:** Use the Chinese Remainder Theorem.
3. Wilson's Theorem says that a number N is prime if and only if

$$(N-1)! = -1 \pmod{N}.$$

   - If p is prime, then we know every number $1 < x < p$ is invertible modulo p. Which of these numbers are their own inverse?
   - By pairing up multiplicative inverses, show that $(p-1)! = -1 \pmod{p}$ for prime p.
   - Show that if n is *not* prime, then $(N-1)! \neq -1 \pmod{N}$. **Hint:** Consider $d = \gcd(N, (N-1)!)$.

18.310 Principles of Discrete Applied Mathematics
Fall 2013