Multiplicative Order

1. Let $n$ be a pseudoprime to base 2 (recall that this means $2^{n-1} \equiv 1 \pmod{n}$). Show that $m = 2^n - 1$ is also a pseudoprime to base 2.

   *Hint:* Show that $n | m - 1$ and use the fact that you know the order of 2 mod $m$.

2. Let $p$ be a prime divisor of the $n$th Fermat number $F_n = 2^{2^n} + 1$.
   (a) Find the order of 2 mod $p$.
   (b) Show that $p \equiv 1 \pmod{2^{n+1}}$.
   (c) Show that for any $a \geq 1$ there are infinitely many primes $p$ for which the order of 2 mod $p$ is divisible by $2^a$.

   **RMK** Note that (b) simplifies the search for prime divisors of Fermat numbers. We will later show that $p \equiv 1 \pmod{2^{n+2}}$ holds.

3. Elements of order 2 mod $m$.
   (a) Let $p$ be odd, and let $k \geq 1$. Show that the congruence $x^2 \equiv 1 \pmod{p^k}$ has only the two obvious solutions $x \equiv \pm 1 \pmod{p^k}$.

   *Hint:* Can both $x - 1, x + 1$ be powers of $p$?

   (*b*) Let $n$ be an odd number, divisible by exactly $r$ distinct primes. Set up a bijection between congruence classes mod $n$ satisfying $x^2 \equiv 1 \pmod{n}$ and functions $f \in \{-1, 1\}^r$. Conclude that there are precisely $2^r$ congruence classes mod $n$ which solve the equation.

4. Using Fermat’s Little Theorem, show that for all integers $n$, $30 | n^9 - n$.

   *Hint:* For each prime $p | 30$ show that $n^p - n | n^9 - n$ as polynomials.

Wilson’s Theorem

5. We will show that if $n \geq 6$ is composite then $(n - 1)! \equiv 0 \pmod{n}$.
   (a) (The easy case) Assume first that $n$ is divisible by at least two distinct primes, that is that $n = \prod_{j=1}^r p_j^{k_j}$ for some distinct primes $p_j$ where $k_j \geq 1$ for all $j$ and $r \geq 2$. Show that $(n - 1)! \equiv 0 \pmod{n}$.

   *Hint:* It is enough to show the congruence mod each $p_j^{k_j}$ separately. Why is $(n - 1)!$ divisible by $p_j^{k_j}$?

   (b) Let $p$ be prime and let $k \geq 3$. Show that $p^k | (p^k - 1)!$.

   *Hint:* Find some powers of $p$ dividing the factorial.

   (c) Let $p \geq 3$ be prime. Show that $p^2 | (p^2 - 1)!$.

   *Hint:* Now you need to consider multiples of $p$ as well.

   **RMK** Note that $3! \not\equiv 0 \pmod{4}$. Ensure that your solution to (c) used the fact that $p \neq 2$ at some point!
The Euler Function and RSA

Recall that \( \varphi(m) = \# \{1 \leq a \leq m \mid (a, m) = 1\} \), and that for \( p \) prime \( \varphi(p) = p - 1 \).

6. Explicit calculations.
   (a) Calculate \( \varphi(4), \varphi(9), \varphi(12), \varphi(15) \).
   (b) Show that \( \varphi(12) = \varphi(3)\varphi(4) \) and \( \varphi(15) = \varphi(3)\varphi(5) \) but that \( \varphi(4) \neq \varphi(2)\cdot\varphi(2) \), \( \varphi(9) \neq \varphi(3)\cdot\varphi(3) \).

7. Let \( p, q \) be distinct primes and let \( m = pq \).
   (a) Show that there are \( p + q - 1 \) integers \( 1 \leq a \leq m \) which are not relatively prime to \( m \).
      Hint: What are the possible values of \( \gcd(a, m) \)? For which \( a \) do they occur?
   (b) Show that \( \varphi(pq) = (p-1)(q-1) \).
      RMK This means in particular that \( \varphi(pq) = \varphi(p)\varphi(q) \).
   (c) Give a formula for \( p + q \) in terms of \( m, \varphi(m) \).
      SUPP Show how to factor \( m \) given \( m, \varphi(m) \).

8. Fix an integer \( m \) and two positive integers \( d, e \) so that \( de \equiv 1 (\varphi(m)) \). Define functions \( E, D \) by \( E(x) = x^e \mod m \) and \( D(y) = y^d \mod m \) (in other words, raise to the appropriate power and keep remainder \( \mod m \)).
   (a) Let \( M = \{1 \leq a \leq m \mid (a, m) = 1\} \) be the set of invertible residues (\( \varphi(m) \) is the size of this set). Show that both \( D, E \) map the set \( M \) into itself.
   (b) Show that for any \( x, y \in M \), \( D(E(x)) = x \) and \( E(D(y)) = y \).
      Hint: Euler’s Theorem.

Supplementary problems (not for submission)

A. (The binomial formula) Prove by induction on \( n \geq 0 \) that for all \( x, y \),
   \[
   (x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.
   \]

B. Let \( p \) be an odd prime.
   (a) Show that \( (p - 1)! \equiv (-1)^{\frac{p-1}{2}} \left( \frac{p-1}{2} \right)!^2 (p) \). Conclude that if \( p \equiv 1 (4) \) then there is \( a \in \mathbb{Z} \) such that \( a^2 \equiv -1 (p) \).
   (b) Conversely, assume that \( a^2 \equiv -1 (p) \) for some integer \( a \). Show that the order of \( a \mod p \) is exactly 4 and conclude that \( p \equiv 1 (4) \).

C. Let \( p \) be a prime and let \( 0 \leq k < p \). Show that \( (\frac{p-1}{k}) \equiv (-1)^k (p) \).