Lior Silberman’s Math 312: Problem Set 4

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.
   
   \[ \text{Hint: Show that } n \mid m - 1 \text{ and use the fact that you know the class of } 2^n \pmod{m}. \]

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) For any \( k \geq 1 \) show that there are infinitely many primes \( p \) for which the order of 2 mod \( p \) is divisible by \( 2^k \).
   
   \[ \text{RMK Note that (b) simplifies the search for prime divisors of Fermat numbers. We will later show that } p \equiv 1 \pmod{2^{n+2}} \text{ holds.} \]

3. Elements of order 2 mod \( m \).
   (a) Let \( p \) be an odd prime, and let \( k \geq 1 \). Show that the congruence \( x^2 \equiv 1 \pmod{p^k} \) has only the two obvious solutions \( x \equiv \pm 1 \pmod{p^k} \).
   
   \[ \text{Hint: Can both } x - 1, x + 1 \text{ be powers of } p? \]

   (*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 \( f \in \{\pm 1\}^r \). 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 \( n \), \( 30 \mid n^9 - n \).
   
   \[ \text{Hint: For each prime } p \mid 30 \text{ show that } n^p - n \mid n^9 - n \text{ as polynomials.} \]

   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 \( (n-1)! \equiv 0 \pmod{n} \).
   
   \[ \text{Hint: It is enough to show the congruence mod each } p_j^{k_j} \text{ separately. Why is } (n-1)! \text{ divisible by } p_j^{k_j}? \]

   (b) Let \( p \) be prime and let \( k \geq 3 \). Show that \( p^k \mid (p^k - 1)! \)
   
   \[ \text{Hint: Find some powers of } p \text{ dividing the factorial.} \]

   (c) Let \( p \geq 3 \) be prime. Show that \( p^2 \mid (p^2 - 1)! \)
   
   \[ \text{Hint: Now you need to consider multiples of } p \text{ as well.} \]

   \[ \text{RMK Note that } 3! \neq 0 \pmod{4}. \text{ Ensure that your solution to (c) used the fact that } p \neq 2 \text{ at some point!} \]
The Euler Function and RSA

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

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

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 \( m \).
      \textit{Hint:} What are the possible values of \( \gcd(a, m) \)? For which \( a \) do they occur?
   (b) Show that \( \phi(pq) = (p - 1)(q - 1) \).
   RMK This means in particular that \( \phi(pq) = \phi(p)\phi(q) \).
   (c) Give a formula for \( p + q \) in terms of \( m, \phi(m) \).
   SUPP Show how to factor \( m \) given \( m, \phi(m) \).

8. Fix an integer \( m \) and two positive integers \( d, e \) so that \( de \equiv 1 \pmod{\phi(m)} \). 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 \( (\phi(m) \) 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 \( E(D(y)) = y \).
      \textit{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 \( (p - 1)! \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!^2 \pmod{p} \). Conclude that if \( p \equiv 1 \pmod{4} \) then there is \( \tilde{a} \in \mathbb{Z} \) such that \( a^2 \equiv -1 \pmod{p} \).
   (b) Conversely, assume that \( a^2 \equiv -1 \pmod{p} \) for some integer \( a \). Show that the order of \( a \) mod \( p \) is exactly \( 4 \) and conclude that \( p \equiv 1 \pmod{4} \).
C. Let \( p \) be a prime and let \( 0 \leq k < p \). Show that \( \binom{p-1}{k} \equiv (-1)^k \pmod{p} \).