Homework 10/ Practice Midterm 2

Liubomir Chiriac

1. (a) Show that $25 \mid 2^{65} + 3^{65}$. (Hint: Use Euler's Theorem.)
   (b) Let $p > 3$ be prime. Find the remainder when $3^p(p-2)!$ is divided by p. (Hint: Combine Wilson's Theorem and Fermat's Little Theorem.)
2. Suppose that both p and $2p-1$ are odd primes. Let $n = 2(2p-1)$. Prove that
$$\varphi(n) = \varphi(n+2).$$
   (Hint: Use the multiplicative property of φ, i.e., Lemma 9.2.8 in your textbook.)
3. Suppose the RSA algorithm is used with the modulus $n = 91$.
   (a) List four possible values for the encryption exponent e.
   (b) Let $e = 17$. First, encrypt the message 10 and then encrypt again the answer you obtained.
   (c) Based on your computations above, explain why the choice made for e in part (b) may not be considered too secure.
4. (a) Show that the order of any nonzero element in $\mathbb{Z}_{23}$ is either $1, 2, 11$ or 22.
   (b) Show that 5 is a primitive root modulo 23. (Hint: Use part (a).)
   (c) Part (b) implies that every nonzero element of $\mathbb{Z}_{23}$ appears exactly once in the list
$$\overline{5}, \overline{5}^2, \ldots, \overline{5}^{22}.$$
   Find all the elements in this list which are primitive roots in $\mathbb{Z}_{23}$.
   (d) Find the order of 5^{14} modulo 23.