Homework 6/ Practice Midterm 2

Liubomir Chiriac

1. (a) A common error in banking is to interchange two of the digits in an amount. Prove that the difference between the correct amount and the amount with the two digits interchanged is always divisible by 9.

   (b) A palindrome is a number that reads the same backward and forward, e.g. 1991, 23577532. Prove that a palindrome with an even number of digits is always divisble by 11.

2. (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.)

3. Suppose that both p and $2p-1$ are both 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.)

4. 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.