Math 441

Homework 4

Due Monday, April 6

1. Textbook problem 11.4
2. Textbook problem 11.6
3. Say you are encrypting a message using plain RSA encryption (construction 11.26 in the book). Say that the key generation algorithm picks p and q to be 503 and 521 and that we are using $e = 3$. What is the public key? What is the private key? Say $m = 1435$. What will the encryption of m be? Say you saw a ciphertext of $c = 130$. What would the decryption of that ciphertext be?
4. Alice has a complaint about RSA encryption. In particular, the message space is the group $\mathbb{Z}_N^*$, since numbers not in that group can't be multiplied (or exponentiated) in an invertible way mod N. But without knowing the factors of N, how can the sender check to make sure the message is in that group? Is Alice's complaint a serious concern? Why or why not?