

### Sample problems - Chapter 4 - Math 1350 - Fall 2010

There will be NO CALCULATORS for the final exam. These sample questions only refer to chapter 4. The final exam is CUMULATIVE. Any topic from the entire course may appear. There will be more questions on chapter 4 than any other. There will be the usual list of letters and their corresponding numerical value. Also there will be the following instruction:

Trial and error methods which would not be effective for large numbers when other methods are available will receive at most half credit, even if 100% correct, and NO partial credit if incorrect.

1. Compute the greatest common divisor of 91 and 221.
2. Compute  $17^{-1} \text{ MOD } 48$
3. Compute  $4^{21} \text{ MOD } 61$ .
4. Compute  $7^{2012} \text{ MOD } 2011$ . You may assume that 2011 is prime.
5. Compute  $6^{50} \text{ MOD } 65$ .
6. Find the prime factorization of 9991.
7. Is 2 a primitive root mod 11? Is 3 a primitive root mod 11?
8. A Diffie-Hellman key agreement protocol has been set up with public prime 29 and public base 2. Alice and Bob want to use this to generate a key for private communications. Alice sends Bob  $\alpha = 16$ . Bob chooses constant  $b = 15$ , so he sends Alice  $2^{15} \text{ MOD } 29 = 27$ . What is the agreed upon key?
9. Find a solution to  $120 \cdot n = 15 \text{ MOD } 195$ . Hint: The gcd of 120 and 195 is 15.
10. Bob decides to use RSA encryption. He chooses  $p = 13$  and  $q = 23$ , so he publishes 299 as his modulus ( $299 = 13 \cdot 23$ ) and exponent  $e = 121$ . Is this a valid RSA scheme?
11. Alice decides to use a Merkle-Hellman public key scheme. She uses the prime 97 with secret key  $w = 49$ . She publishes the sequence 50, 51, 5, 60, 21. If Bob wants to encipher the plaintext 10111 what is the cipher text? What was Alice's original superincreasing sequence?