

## HW 6 CMSC 389. DUE Jan 10

1. (0 points) What is your name? Write it clearly. Staple your HW. What is the day and time of the second midterm? Are you free then? (if not then SEE ME IMMEDIATELY) When is the final? Are you free then? (if not then SEE ME IMMEDIATELY)
  
2. (40 points)
  - (a) Find the inverse of 40 mod 101 using the GCD method. Show all work.
  - (b) Find the inverse of 41 mod 101 using the GCD method. Show all work.
  
3. (10 points) Find the GCD of 102 and 22 using the method in class. The answer is 2. Write 2 as a linear combo of 102 and 22. Mod that equation out by 102. What does this tell you?
  
4. (50 points)
  - (a) Let  $p = 101$ . Find all generators of  $\{2, \dots, 100\}$  between 10 and 20.
  - (b) Let  $g$  be the LEAST generator found in the last part. Find  $g, g^2, g^3, g^4, g^5, g^6, g^7, g^8, g^9, g^{10}$ . Form the list  $(i, g^i)$ . Sort based on second coordinate. WRITE DOWN the sorted list on your HW.
  - (c) Write a program that finds inverses of numbers mod 101.
  - (d) Find  $g^{10}, g^{20}, g^{30}, g^{40}, g^{50}, g^{60}, g^{70}, g^{80}, g^{90}, g^{100}$ .
  - (e) Find  $g^{-10}, g^{-20}, g^{-30}, g^{-40}, g^{-50}, g^{-60}, g^{-70}, g^{-80}, g^{-90}, g^{-100}$ .
  - (f) Use all of this information to find the DISCRETE LOG of 20,21,22,23,24. (You can use a calculator or even write a program but write down enough of your work so we know that you know how to do this.)