

Math 103H

Fall 2010

Prof. Miller

HW Assignment #5 (Due in class Tuesday December 7)

1. Use the Pollard Rho factoring method to factor the integers a) 91 and b) 187. Show your work.
2. Use the Pollard Rho algorithm for discrete logarithms to find the discrete logarithm of a) 80, b) 70, and c) 78 (all mod  $p=97$ ), with  $g=5$  the generator. Again, make sure to show all your work.

3. This question is about *Random Reducibility* which we discussed in class. Let  $p=113$ , and  $g=3$  be a generator. Here is a table of the discrete logarithms of all integers from 30 to 60:

30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49
96	50	60	75	17	91	26	67	111	23	7	94	21	47	98	85	53	31	49	16

50	51	52	53	54	55	56	57	58	59	60
66	6	46	52	15	45	44	100	101	71	108

Use the method of random reducibility to find the discrete logarithms of these numbers:

- a) 25
  - b) 26
  - c) 63
4. Compute the first 10 values of the linear congruential generator  $3x+7 \pmod{100}$ , starting with  $x=54$ .
  5. Suppose we have a linear congruential generator given by the formula  $ax+b \pmod{100}$ , where  $a$  and  $b$  are secret. Suppose that we know the first few outputs are as follows:  
1,0,77,48,81,40,97,8,61,80,17  
Predict the next term in the sequence (one way to do this is to find what  $a$  and  $b$  are, using some detective work in the beginning of the sequence).