

MATH 343, PROBLEM SET 3

ANDREW J. BLUMBERG

1. PROBLEMS

- (1) For this problem, you will write an efficient discrete log solver, using the Shank's solver you wrote for last homework as a base.
 - (a) Implement the “shifting” technique for reducing discrete log mod p^n to discrete log mod p and arithmetic; the result should be a function which takes g, h, p , and n as inputs and solves $g^x = h \pmod{p^n}$.
 - (b) Implement the Pohlig-Hellman algorithm, using the function from the first part as your “black box” discrete log solver.
- (2) From the text: 2.3, 2.10, 2.27.