1 Problems

1. Please implement Pollard’s \( \rho \) algorithm for solving discrete log problems in \( \mathbb{F}_p \). (Use the same input/output format as previous discrete log solver problems.)

2. Work out the details for remark 3.57 (about the index calculus) in the text.

3. Implement the RSA blind signature algorithm. Write a program to generate the key pair for Alice, so that the only input you need to take is the message.

4. From the text: 4.8, 5.30, 5.38, 5.43.