Homework 21, due November 17

(1) (Page 304, problem 8) There are four people in a room, exactly one of whom is a foreign agent. The other three people have been given pairs of numbers corresponding to a Shamir secret sharing scheme in which any two people can determine the secret. The foreign agent has randomly chosen a pair. The people and pairs are as follows. All numbers are modulo 11.

$$\text{Alice} : (1, 4) \ \text{Bob} : (3, 7) \ \text{Charles} : (5, 1) \ \text{Donald} : (7, 2)$$

Determine who the foreign agent is and what the message is.

(2) (Page 304, problem 5) Mark doesn't like modular arithmetic, so he wants to implement a $(2, 30)$ Shamir secret sharing scheme without them. His secret is a positive integer M, and he gives person i the share $(i, M + si)$ for a positive integer s that he randomly chooses. Bob receives the share $(20, 97)$. Describe how Bob can narrow down the possibilities for M and determine what values of M are possible.

(3) (Page 306, problem 2) For a Shamir (4,7) secret sharing scheme, let $p = 8737$ and let the shares be (1, 214), (2, 7543), (3, 6912), (4, 8223), (5, 3904), (6, 3857), (7, 510). Take a set of four shares and find the secret using a linear system.

(4) Now take another set of four shares and calculate the secret using Lagrange interpolating polynomials.