Chapter 12 Homework 2-5

2. You set up a $(2, 30)$ Shamir threshold scheme, wording mod the prime 101. Two of the shares are $(1, 13)$ and $(3, 12)$. Another person received the share $(2,^*)$, but the part denoted by * is unreadable. What is the correct value of *?

   Since we have a $(2, 30)$ Shamir scheme, we need two shares to find M, so we want to find $S(x) = M + si(x)$.

$$M + 1 \cdot s \equiv 13 \pmod{101}$$
$$M + 3 \cdot s \equiv 12 \pmod{101}$$

$$\begin{bmatrix} 1 & 1 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} \text{M} \\ S_1 \end{bmatrix} \equiv \begin{bmatrix} 13 \\ 12 \end{bmatrix} \pmod{101}$$
$$\Rightarrow \begin{bmatrix} \text{M} \\ S_1 \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 \\ 1 & 3 \end{bmatrix}^{-1} \begin{bmatrix} 13 \\ 12 \end{bmatrix} \pmod{101}$$
$$\equiv \frac{1}{2} \begin{bmatrix} 3 & \text{-1} \\ \text{-1} & 1 \end{bmatrix} \begin{bmatrix} 13 \\ 12 \end{bmatrix} \pmod{101}$$
$$\equiv 51 \begin{bmatrix} 3 & \text{-1} \\ \text{-1} & 1 \end{bmatrix} \begin{bmatrix} 13 \\ 12 \end{bmatrix} \pmod{101}$$
$$\equiv 51 \begin{bmatrix} 27 \\ \text{-1} \end{bmatrix} \pmod{101}$$
$$\equiv \begin{bmatrix} 64 \\ \text{-51} \end{bmatrix} \pmod{101}$$

   So, We have

$$s(x) = 64 - 51(x) \pmod{101}$$

   Now, for $(2,^*)$, we have

$$s(2) = 64 - 51(2) \pmod{101} \equiv 63$$

   That is, $^* = 63$.

3. In a $(3, 5)$ Shamir secret sharing scheme with modulus $p = 17$, the following were given to Alice, Bob and Charles: $(1, 8), (3, 10), (5, 11)$. Calculate the corresponding Lagrange interpolating polynomial, and identify the secret.

$$l_1 = \frac{x-3}{1-3} \cdot \frac{x-5}{1-5} \equiv \frac{x^2 - 8x + 15}{8} \pmod{17}$$
$$l_2 = \frac{x-1}{3-1} \cdot \frac{x-5}{3-5} \equiv \frac{x^2 - 6x + 5}{-4} \pmod{17}$$
$$l_3 = \frac{x-1}{5-1} \cdot \frac{x-3}{5-3} \equiv \frac{x^2 - 4x + 3}{8} \pmod{17}$$

$$
\begin{aligned}
p(x) &= \sum_{k=1}^{3} y_k l_k(x) \\
&\equiv 8 \cdot \frac{x^2 - 8x + 15}{8} + 10 \cdot \frac{x^2 - 6x + 5}{-4} + 11 \cdot \frac{x^2 - 4x + 3}{8} \\
&\equiv \frac{1}{8}(8x^2 - 64x + 120 - 20x^2 + 120x - 100 + 11x^2 - 44x + 33) \\
&\equiv \frac{1}{8}(-x^2 + 12x + 53) \\
&\equiv 15(-x^2 + 12x + 53) \\
&\equiv -15x^2 + 180x + 795 \\
&\equiv 2x^2 + 10x + 13 \pmod{17}
\end{aligned}
$$

So,

$$
\boxed{p(x) = 2x^2 + 10x + 13 \pmod{17}}
$$

where the secret is 13.

4. In a Shamir secret sharing scheme, the secret is the constant term of a degree 4 polynomial mod the prime 1093. Suppose three people have the secrets $(2, 197), (4, 874)$ and $(13, 547)$. How many possibilities are there for the secret?

   If we assume that the secret is not the trivial $M = 0$, there are 1092 possibilities. Since we know 3 shares, we would need two more to discover the secret. So any value would be possible.

5. Mark doesn't like mods, so he wants to implement a $(2, 30)$ Shamir secret sharing scheme without them. His secret is M (a positive integer) 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.

   We know $i = 20$ and that $M + si = 97$.

$$
M + 20s = 97 \Rightarrow M = 97 - 20s \text{ for } s \in \mathbb{Z}^+
$$

   So, we have

$$
\begin{array}{ll}
s = 1 & M = 77 \\
s = 2 & M = 57 \\
s = 3 & M = 37 \\
s = 4 & M = 17
\end{array}
$$