Discrete Mathematics: Homework 8

(Deadline: 10:00am, May 1, 2020)

1. (20 points) Let $\mathbb{Z}^2 = \{(a, b) : a, b \in \mathbb{Z}\}$. Define $\oplus$ and $\otimes$ over $\mathbb{Z}^2$ such that
   - $(a, b) \oplus (c, d) = (a + c, b + d)$; and
   - $(a, b) \otimes (c, d) = (ac, bd)$.

   for all $(a, b), (c, d) \in \mathbb{Z}^2$. Prove or disprove that $(\mathbb{Z}^2, \oplus, \otimes)$ is a ring.

2. (20 points) Let $\mathbb{Z}[X] = \{f_0 + f_1 + \cdots + f_d X^d : d \geq 0, f_0, f_1, \ldots, f_d \in \mathbb{Z}\}$ be the set of all polynomials over $\mathbb{Z}$. Prove or disprove that $(\mathbb{Z}[X], +, \cdot)$ is a ring, where $+$ and $\cdot$ are the addition and the multiplication of polynomials over $\mathbb{Z}$.

3. (25 points) Write a computer program to reconstruct the secret $s \in \mathbb{Z}_{1125899906900597}$ in Shamir's $(5, 9)$-threshold secret sharing scheme. In the devised program, the reconstruction of s should be based on the Lagrange interpolation formula. Use your program to reconstruct the secret s, given that the 9 shares are as follows:

i	s_i
1	75044643784737
2	940519894412855
3	941263003333598
4	736739711411826
5	254180887785524
6	940382343666996
7	132205297839880
8	63775631863924
9	1111084448671404

.

4. (25 points) An officer stored in his safe a very important letter. He shared the password $s \in \mathbb{Z}_{1125899906900597}$ to the safe among 9 soldiers using Shamir's $(5, 9)$-threshold secret sharing scheme. After the officer was killed in a battle, the 9 soldiers need to open the safe. Suppose that they provided the following shares in the reconstruction process:

i	s_i
1	150550125355646
2	944474507418938
3	110040335185999
4	676042268761809
5	193274108888331
6	904128547609081
7	354197665334455
8	416432161112962
9	283942097426448

.

Among the 9 soldiers 2 were spies and provided wrong shares in order to prevent the other soldiers from opening the safe. Use your computer program in Question 3 to find the spies and then recover the password s from the correct shares.

5. (15 points) Let $\mathcal{P} = \{P_1, P_2, P_3, P_4, P_5\}$. Design a secret sharing scheme that realizes an access structure with basis

$$\Gamma_0 = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4, P_5\}, \{P_2, P_3, P_4\}, \{P_2, P_3, P_5\}, \{P_2, P_4, P_5\}, \{P_3, P_4, P_5\}\}.$$

6. (15 points) Let $\mathcal{P} = \{P_1, P_2, \ldots, P_{20}\}$ be a set of 20 participants. Let $\Gamma = \{A : A \subseteq \mathcal{P}, |A| \geq 11\}$ be an access structure.

   (a) If Γ is realized with the monotone circuit construction, how many numbers are there in the share of each participant?

   (b) If Γ is realized with Shamir's $(11, 20)$-threshold secret sharing scheme, how many numbers are there in the share of each participant?