Section 6

1. Find (and prove) an upper-bound on the number of times two distinct degree d polynomials can intersect. What if the polynomials' degrees differ?

2. Recall the Lagrange interpolation method: Given $d+1$ data points $(x_0, y_0), ..., (x_d, y_d)$, the unique polynomial of degree $\leq d$ which passes through these points is given by $P(x) = \sum_{i=0}^{d} y_i \Delta_i(x)$, where $\Delta_i(x) = \prod_{\substack{0 \leq j \leq d \\ j \neq i}} \frac{x - x_j}{x_i - x_j}$.

(a) Use the Lagrange interpolation method to determine the coefficients of the polynomial of degree ≤ 2 that fits the points (-1, 2), (0, 1), (1, 2) in the real numbers (i.e., familiar, non-modular arithmetic).

(b) Use the Lagrange interpolation method to determine the coefficients of the polynomial of degree ≤ 2 that fits the points (-1, 2), (0, 1), (1, 2) in GF(3) (i.e., arithmetic modulo 3).

3. Your GSI has (let us imagine) chosen to distribute a secret number s among 10 students, with s being one of the eleven values from 0 through 10. The way your GSI distributed this secret is by choosing a polynomial $P(x)$ of degree ≤ 2 such that $P(0) \equiv s \pmod{11}$. They then told their favorite student the value of $P(1)$ modulo 11, their second favorite student the value of $P(2)$ modulo 11, and so on, up through $P(10)$.

(a) Suppose you were told that $P(6) \equiv 7 \pmod{11}$ and your neighbor was told that $P(7) \equiv 5 \pmod{11}$. What can the two of you determine about s from this information?

(b) You and your neighbor begin speculating about what the eighth-favorite student heard from the GSI. What can the two of you determine about the value of P(8)?

(c) Suppose that the eighth-favorite student, hearing your whispers, comes along and tells you outright that $P(8) \equiv 4 \pmod{11}$. What can the three of you determine about s now?

(d) Were a wave of amnesia to suddenly hit parts of the classroom, how many students would need to retain their memories in order to be able to re-determine the values each student received from the GSI?

4. Professor Rao has also grown quite fond of polynomials. They have also chosen a polynomial $Q(x)$ of degree ≤ 2, and told the value of $Q(1)$ to their favorite student, $Q(2)$ to their second favorite student, and so on, up through $Q(11)$ this time. (All of this is modulo 11, just as before)

(a) Alas, you are not among Professor Rao's favorite eleven students. How many of those students would you need to talk to before you could figure out the coefficients of Q(x)?

(b) That's assuming the students are honest. But, it turns out, four of Professor Rao's favorite students are morally bankrupt and perfectly willing to lie to you. (The rest are, thankfully, completely trustworthy). Unfortunately, you don't know *which* four are untrustworthy.

If you talk to 7 students, what is the minimum number of correct answers you will receive?

(c) If you talk to 7 students, how can you tell whether at least one of them is lying? [Hint: You may find it useful to think back to the top question on this sheet]

(d) Is there a group of 7 students with no liars?

(e) With access to all 11 students, how can you figure out the polynomial $Q(x)$, despite the fact that 4 students are untrustworthy? [Do not worry how efficient your method is]

(f) If Professor Rao's polynomial had been of degree up to 4, instead, how many untrustworthy students could there be before this method would stop working? What should all the 7s above be changed to in that case?