EECS 70 Discrete Mathematics and Probability Theory
Fall 2014 Anant Sahai

Discussion 7M

1. Lagrange Interpolation in Finite Field

Find a unique polynomial $p(x)$ of degree at most 3 that passes through points $(-1,3)$, $(0,1)$, $(1,2)$, and $(2,0)$ in modulo 5 arithmetic using the Lagrange interpolation.

(a) Find $p_{-1}(x)$ where $p_{-1}(0) \equiv p_{-1}(1) \equiv p_{-1}(2) \equiv 0 \pmod 5$ and $p_{-1}(-1) \equiv 1 \pmod 5$.

(b) Find $p_0(x)$ where $p_0(-1) \equiv p_0(1) \equiv p_0(2) \equiv 0 \pmod 5$ and $p_0(0) \equiv 1 \pmod 5$.

(c) Find $p_1(x)$ where $p_1(-1) \equiv p_1(0) \equiv p_1(2) \equiv 0 \pmod 5$ and $p_1(1) \equiv 1 \pmod 5$.

(d) Find $p_2(x)$ where $p_2(-1) \equiv p_2(0) \equiv p_2(1) \equiv 0 \pmod 5$ and $p_2(2) \equiv 1 \pmod 5$.

(e) Construct $p(x)$ using a linear combination of $p_{-1}(x)$, $p_0(x)$, $p_1(x)$ and $p_2(x)$.

2. Secret Sharing

Prof. Sahai would like to share a secret number s among us, with s could be any integer from 0 to 10. He chose a polynomial with degree 1 such that $P(0) \equiv s \pmod{11}$, but he only shared $P(1)$ to your GSI. Another key is on your hands. The way he distributed the second key $w = P(2)$ $(0 \leq w \leq 58)$ is by choosing a polynomial $Q(x)$ of degree ≤ 2 such that $Q(0) \equiv w \pmod{59}$. Here are your x and $Q(x)$:

(a) At least how many students would we need in order to find w?

(b) Please find w.

(c) Please help your GSI find the secret number s.

3. Secrets in the United Nations

The United Nations (for the purposes of this question) consists of n countries, each having k representatives. A vault in the United Nations can be opened with a secret combination s. The vault should only be opened in one of two situations. First, it can be opened if all n countries in the UN help. Second, it can be opened if at least m countries get together with the Secretary General of the UN.

(a) Propose a scheme that gives private information to the Secretary General and n countries so that s can only be recovered under either one of the two specified conditions.

(b) The General Assembly of the UN decides to add an extra level of security: in order for a country to help, all of the country's k representatives must agree. Propose a scheme that adds this new feature. The scheme should give private information to the Secretary General and to each representative of each country.