Interpolation

Proposition 1 (Lagrange Interpolation)**.** *Let R be a domain with field of fractions F. Let (a_i, b_i), $0 \leq i \leq d$, be a list of $d+1$ pairs of elements of R such that the a_i are all distinct. Then there is a unique polynomial $q(x) \in F[x]$ of degree at most d such that $q(a_i) = b_i$ for each i.*

Proof. Define the polynomial $q(x) \in F[x]$ as follows:

$$q(x) = \sum_{i=0}^{d} b_i \prod_{j \neq i} \frac{x - a_j}{a_i - a_j}.$$

Certainly q has degree at most d, since it is a sum of polynomials of degree exactly d. Now consider the value of q at a particular a_k. In the product $\prod_{j \neq i}(a_k - a_j)/(a_i - a_j)$, if j is ever equal to k then we have 0 as a factor. Thus the only term of this sum which contributes to $q(a_k)$ is $i = k$. So

$$q(a_k) = b_k \prod_{j \neq k} \frac{a_k - a_j}{a_k - a_j} = b_k$$

as claimed.

To see that q is unique, use Corollary (blah). □

1. **A Factorization Algorithm.** In this exercise we will use interpolation to construct an algorithm capable of factoring polynomials over certain UFDs.

2. **Secret Sharing.** A *secret sharing scheme* is a method of dividing information into incomplete parts, called *shares*, so that the information can only be retrieved if one is in possession of all (or enough) of the shares. Polynomial interpolation can be used to design a secret sharing scheme.