COL 202

TUTORIAL SHEET 12

1. A polynomial $p(x)$ of degree n over a field F has at most n roots. But it does not need to have n roots, nor it must have roots at all (Recall that F_p denotes the field $\{0, 1, 2, \ldots, p-1\}$ for a prime p).
   - Write all polynomials in F_2 having no roots over F_2.
   - Write all polynomials in F_3 having no roots over F_3.
   - Find a polynomial $p(x)$ which has roots over F_3, but not over Z, the set of integers.
2. In our exposition of secret sharing, we always set the secret to be $P(0)$, i.e. the constant term of the polynomial P used to generate the keys in the field F_q.
   - Could the scheme be generalized to have the secret chosen to be $P(k)$ for k such that $0 < k < q$?
   - More concretely, suppose now that $q = 7, k = 2$ and P has degree 2. Given $P(1) = 5; P(3) = 6, P(4) = 5$, use Lagranges Interpolation to recover the secret $P(k)$.
   - Finally, suppose $q = 7, k = 0$ and P has degree 2, but this time you are given $P(1) = 3; P(3) = 4; P(4) = 2$. Use Lagranges Interpolation to recover the secret $P(0)$. Now, can you see why $P(0)$ is a good choice for the secret?
3. A secret sharing scheme is k-secure if and only if any group of k or fewer people has probability at most $1/q$ of recovering the secret, where q is the number of possible choices for the secret (this means that the best strategy such a group has is to guess the secret at random). In the typical secret sharing scheme, the secret is $P(0)$, the value of a certain degree k polynomial (that we construct) at 0. Suppose that, instead, the secret is $P(0), P(1)$ (the values at both 0 and 1). Is this scheme still k-secure? Prove your answer.
4. In this question we will go through an example of error-correcting codes. Since we will do this by hand, the message we will send is going to be short, consisting of $n = 3$ numbers, each modulo 5, and the number of errors will be $k = 1$.
   - First, construct the message. Let $a_0 = 4$ and $a_1 = 3, a_2 = 2$; then use the polynomial interpolation formula to construct a polynomial $P(x)$ of degree 2 (remember that all arithmetic is mod 5) so that $P(0) = a_0, P(1) = a_1$, and $P(2) = a_2$; then extend the message to length $N + 2k$ by adding $P(3)$ and $P(4)$. What is the polynomial $P(x)$ and what are $P(3)$ and $P(4)$?
   - Suppose the message is corrupted by changing a_0 to 0. Use the Berlekamp-Welsh method to find a polynomial $g(x)$ of degree 2 that passes through 4 of the 5 points. Show all your work.