CS 70 Discrete Mathematics and Probability Theory
Fall 2013 Week 4 Discussion

Polynomials

Note: you aren't expected to complete even all of the non-challenge problems. Extra problems are included to help with practice.

1. Suppose $P(x) = x^3 + 2x + 3$ and $Q(x) = x^2 + 4x + 3$.
   (a) Simplify $P(x) + Q(x)$ mod 5.
   (b) Simplify $P(x) * Q(x)$ mod 5.
   (c) Can you simplify $P(x) * Q(x)$ further, using Fermat's little theorem?
2. (a) Find a polynomial P of degree 1 such that $P(2) = 4, P(4) = 2$, mod 11.
   (b) Find a polynomial P of degree 2 such that $P(1) = 1, P(3) = 3, P(5) = 2$, mod 7.
   (c) Find a polynomial P of degree 3 such that $P(1) = 1, P(2) = 2, P(3) = 3, P(4) = 1$, mod 5
3. (a) Prove that a parabola and a line can intersect at most 2 points.
   (b) Prove that a parabola and a cubic can intersect at at most 3 points.
   (c) Show that if you do Lagrange interpolation with $d+1$ points you always recover the correct polynomial, but if you do it with d points you might not (where d is the degree of the polynomial).
4. **Challenge problem**:
   (a) Prove that for every polynomial P and every prime p, there exists a Q of degree at most $p-1$ such that $P(x) = Q(x)$ mod p for every x.
   (b) If P and Q are distinct degree $p-1$ polynomials, show that $P(x) \neq Q(x)$ mod p for some x.
   (c) Using the above facts, show that every function from $\{0, 1, \ldots, p-1\}$ to $\{0, 1, \ldots, p-1\}$ is equivalent to some degree $p-1$ polynomial.
   (d) Using Lagrange interpolation, show that every function from $\{0, 1, \ldots, p-1\}$ to $\{0, 1, \ldots, p-1\}$ is equivalent to some degree $p-1$ polynomial.
5. **Challenge problem**: Given $d+2$ degree d polynomials $P_1, P_2, \ldots, P_{d+2}$, show that there exist numbers $a_1, a_2, \ldots a_{d+2} \in \{0, \ldots, p-1\}$ which are not all zero such that

   $$a_1 P_1(x) + a_2 P_2(x) + \ldots + a_{d+2} P_{d+2}(x) = 0 \bmod p$$

   for every x.
6. **Challenge problem**:
   (a) If $P(k)$ is a degree d polynomial, show that $P(k+1) - P(k)$ is a degree $d-1$ polynomial.
   (b) **Harder**: If $P(k)$ is a degree d polynomial, show that $\sum_{k=1}^{n} P(k)$ is a degree $d+1$ polynomial in n.