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.
   Solution.

   $$P(x)+Q(x) = x^3+2x+3+x^2+4x+3 = x^3+x^2+6x+6 \equiv x^3+x^2+x+1 \pmod 5$$

   (b) Simplify $P(x) * Q(x)$ mod 5.
   Solution.

   $$\begin{aligned} P(x)*Q(x) &= (x^3+2x+3)(x^2+4x+3) \\ &= x^5+2x^3+3x^2+4x^4+8x^2+12x+3x^3+6x+9 \\ &= x^5+4x^4+5x^3+16x^2+18x+9 \\ &\equiv x^5+4x^4+x^2+3x+4 \pmod 5 \end{aligned}$$

   (c) Can you simplify $P(x) * Q(x)$ further, using Fermat's little theorem?
   Solution. Recall Fermat's little theorem says $x^{p-1} \equiv 1 \pmod p$ if $\gcd(x, p) = 1$. So it almost looks like we could replace x^4 with 1 – but that wouldn't quite be right, since it fails when $x \equiv 0$. However, for p prime the equivalence $x^p \equiv x \pmod p$ always holds; it clearly holds for $x \equiv 0$, and for nonzero x it holds by multiplying both sides of Fermat's little theorem by x. Therefore, we can further simplfy $x^5 + 4x^4 + x^2 + 3x + 4$ to $4x^4 + x^2 + 4x + 4$.

2. (a) Find a polynomial P of degree 1 such that $P(2) = 4, P(4) = 2$, mod 11.
   Solution. Applying Lagrange interpolation,

   $$\begin{aligned} \Delta_2(x) &= \frac{x-4}{2-4} = -2^{-1}(x-4) \\ \Delta_4(x) &= \frac{x-2}{4-2} = 2^{-1}(x-2) \end{aligned}$$

   Therefore,

   $$\begin{aligned} P(x) &= 4\Delta_2(x) + 2\Delta_4(x) \\ &= -4 \cdot 2^{-1}(x-4) + 2 \cdot 2^{-1}(x-2) \\ &= -2(x-4) + (x-2) \\ &= -x+6 \\ &\equiv 10x+6 \pmod{11} \end{aligned}$$

(b) Find a polynomial P of degree 2 such that $P(1)=1, P(3)=3, P(5)=2$, mod 7.

Solution. Applying Lagrange interpolation,

$$\begin{aligned}
\Delta_1(x) &= \frac{(x-3)(x-5)}{(1-3)(1-5)} = 8^{-1}(x-3)(x-5) \equiv (x-3)(x-5) \pmod 7 \\
\Delta_3(x) &= \frac{(x-1)(x-5)}{(3-1)(3-5)} = (-4)^{-1}(x-1)(x-5) \equiv 3^{-1}(x-1)(x-5) \pmod 7 \\
\Delta_5(x) &= \frac{(x-1)(x-3)}{(5-1)(5-3)} = 8^{-1}(x-1)(x-3) \equiv (x-1)(x-3) \pmod 7
\end{aligned}$$

Therefore,

$$\begin{aligned}
P(x) &\equiv 1\Delta_1(x) + 3\Delta_3(x) + 2\Delta_5(x) \\
&\equiv (x-3)(x-5) + 3\cdot 3^{-1}(x-1)(x-5) + 2(x-1)(x-3) \\
&\equiv x^2 - 8x + 15 + x^2 - 6x + 5 + 2(x^2 - 4x + 3) \\
&\equiv 4x^2 - 22x + 26 \\
&\equiv 4x^2 + 6x + 5 \pmod 7
\end{aligned}$$

(c) Find a polynomial P of degree 3 such that $P(1)=1, P(2)=2, P(3)=3, P(4)=1$, mod 5

Solution. Applying Lagrange interpolation,

$$\begin{aligned}
\Delta_1(x) &= \frac{(x-2)(x-3)(x-4)}{(1-2)(1-3)(1-4)} = (-6)^{-1}(x-2)(x-3)(x-4) \equiv -(x-2)(x-3)(x-4) \pmod 5 \\
\Delta_2(x) &= \frac{(x-1)(x-3)(x-4)}{(2-1)(2-3)(2-4)} = 2^{-1}(x-1)(x-3)(x-4) \equiv 3(x-1)(x-3)(x-4) \pmod 5 \\
\Delta_3(x) &= \frac{(x-1)(x-2)(x-4)}{(3-1)(3-2)(3-4)} = -2^{-1}(x-1)(x-2)(x-4) \equiv -3(x-1)(x-2)(x-4) \pmod 5 \\
\Delta_4(x) &= \frac{(x-1)(x-2)(x-3)}{(4-1)(4-2)(4-3)} = 6^{-1}(x-1)(x-2)(x-3) \equiv (x-1)(x-2)(x-3) \pmod 5
\end{aligned}$$

Therefore,

$$\begin{aligned}
P(x) &\equiv 1\Delta_1(x) + 2\Delta_2(x) + 3\Delta_3(x) + 1\Delta_4(x) \\
&\equiv -(x-2)(x-3)(x-4) + 6(x-1)(x-3)(x-4) - 9(x-1)(x-2)(x-4) + (x-1)(x-2)(x-3) \\
&\equiv -3x^3 + 18x^2 - 27x + 18 \\
&\equiv 2x^3 + 3x^2 + 3x + 3 \pmod 5
\end{aligned}$$

3. (a) Prove that a parabola and a line can intersect at most twice.

Solution. Recall a parabola is a degree-2 polynomial, while a line has degree ≤ 1. On the other hand, two distinct degree-2 polynomials can agree on at most 2 points. Since a line and parabola don't agree everywhere, they can agree on at most 2 points.

(b) Prove that a parabola and a cubic can intersect at at most three times.

Solution. Recall a cubic is a degree-3 polynomial, while a parabola has degree 2. On the other hand, two distinct degree-3 polynomials can agree on at most 3 points. Since a cubic and parabola don't agree everywhere, they can agree on 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).

Solution. For example, let $d = 1$, and suppose our single point is $(0,0)$. There are many lines that pass through $(0,0)$; for example, $P(x) = 0$ and $P(x) = x$. So specifying only 1 point does not completely characterize a line.

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 $P(x) = Q(x) \bmod p$ for every x.

(b) If P and Q are distinct degree $p-1$ polynomials, show that $P(x) \neq Q(x) \bmod p$ 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

$$a_1P_1(x) + a_2P_2(x) + \ldots + a_{d+2}P_{d+2}(x) = 0 \bmod p$$

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.