Warm Ups

Problem 1 (Spring 2018 MT2 3.4)**:** What is the maximum number of points at which two distinct degree d polynomials can intersect?

Problem 2 (Spring 2019 MT2 3.1)**:** Consider that $P(x) = 3x^2 + a_1x + s \pmod 5$ encodes a secret s as $P(0)$; given that $P(1) = 3$ and $P(2) = 4$, what is the secret?

Problem 3 (Spring 2018 MT2 3.1)**:** Given two polynomials $P(x)$ and $Q(x)$ of degrees d_1 and d_2 respectively, consider $R(x) = P(x)Q(x)$. We claim that we can recover $P(x)$ and $Q(x)$ with any r points on $R(x)$ and any q points on $Q(x)$. What are r and q? (You should give the minimum possible values for r and q here)

Medium/Harder Problems

Problem 4 (Fall 2017 MT2 2.9)**:** Let $P(x)$ and $Q(x)$ be distinct polynomials of degrees d_p and d_q, respectively, that intersect at exactly 4 points. If the lowest degree polynomial that contains those 4 points has degree 3, what is the minimum value of $d_p + d_q$?

Problem 5 (Spring 2019 MT2 3.7)**:** How polynomials of degree at most 5 in $GF(p)$ have **exactly** 5 fixed points? Assume that p is a prime larger than 5, and recall that a fixed point of a polynomial P is a value a such that $P(a) = a$.

Problem 6 (Spring 2017 MT2 3.8)**:** True or False: There exists a bijection between the set of triples (a, b, c) of real numbers and the set of polynomials of degree at most 3 that pass through the point $(3, 3)$.

Problem 7 (Fall 2018 MT2 3)**:** Alice sets up a secret sharing scheme with her n friends $\text{Bob}_1, \text{Bob}_2, \ldots, \text{Bob}_n$, in which each Bob_i gets a point (x_i, y_i) where $y_i = P(x_i)$ for some fixed polynomial P over $GF(q)$, where $q > 2n$. The secret is kept at $P(0) = s$. When Alice is distributing these points to the Bobs, an adversary Eve can tamper with the points, and thus change the value of the secret that will be recovered. For each scenario in (a)–(c) below, give the value of the new secret that will be recovered; your answers may depend on s or on P. In each case, prove that your answer is correct.

(a) Eve replaces each point (x_i, y_i) with $(x_i, 2y_i + 1)$.

(b) Eve replaces each point (x_i, y_i) with $(2x_i, y_i)$.

(c) Eve replaces each point (x_i, y_i) with $(x_i - 1, y_i)$ [You may assume that $x_i \neq 1$ for any i.]