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?

Solution 1: The answer is $\boxed{d}$ points. To see why, let P, Q be distinct polynomials of degree d. Then their difference $D(x) = P(x) - Q(x)$ is nonzero and is also a degree d polynomial. Thus, it has at most d roots. This means that there are at most d points x_i such that $D(x_i) = P(x_i) - Q(x_i) = 0$, hence there are at most d points where $P(x) = Q(x)$, as claimed.

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?

Solution 2: The answer is $\boxed{s = 3}$. To solve this, we plug in the points $x = 1$ and $x = 2$ in the symbolic definition of P. This generates the system of linear congruences

$$\begin{aligned} 3 + a_1 + s &\equiv 3 \pmod 5 \\ 2 + 2a_1 + s &\equiv 4 \pmod 5, \end{aligned}$$

which we can solve to get that $a_1 \equiv 2 \pmod 5$ and $s \equiv 3 \pmod 5$.

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)

Solution 3: The answer is $\boxed{r = d_1 + d_2 + 1, q = d_2 + 1}$. In order to guarantee that we can reverse engineer R from the r points given, we need to have r be larger than the degree of $R(x)$. Thus the minimum value of r is $\deg(R) + 1 = d_1 + d_2 + 1$. Similarly, we need to be able to uniquely determine Q, so we need $q = \deg Q + 1 = d_2 + 1$. With both R and Q, we can find P using polynomial long division, so we're done.

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 $d_p + d_q$?

Solution 4: The answer is $\boxed{d_p + d_q = 7}$. This value is achievable, as we can always find a degree 4 polynomial P and a degree 3 polynomial Q that agree at 4 given points. Now, we show that this value is minimal. Firstly, we know that there are four points on P and Q that lie on a nondegenerate cubic - this in particular means that $d_p = \deg P \geq 3$ and similarly, $d_q = \deg Q \geq 3$. Adding the two inequalities together, it then follows that $d_p + d_q \geq 6$. So, it remains to show that 6 is unachievable. Indeed, the only way this can happen is if P and Q are both cubic. But, we know that P and Q intersect at 4 points, so if they are both cubic, then they would have to be the same polynomial. This contradicts the fact that $P \neq Q$, so 6 is impossible. Thus, the minimum value is 7.

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 $P(a) = a$. (NOTE: this problem is at its heart a counting problem and so is out of scope for this midterm)

Solution 5: The answer is $\boxed{\binom{p}{5} \cdot (p-1)}$. We just need to pick the 5 fixed points of P, then pick a value for a sixth point in such a way that doesn't generate any more fixed points. We can do this by setting the sixth

point so that it itself is not fixed, and then we get a polynomial with exactly 5 fixed points. Hence the total number of such polynomials is $\binom{p}{5}(p-1)$. (If this stuff seems unfamiliar don't worry, its out of scope)

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 $(3, 3)$.

Solution 6: The answer is $\boxed{\text{True}}$, and we can prove this by explicitly constructing a bijection. Let $\mathcal{P}$ denote the set of polynomials that satisfy the conditions outlined in the problem. Now, consider the map $\phi : \mathbb{R}^3 \to \mathcal{P}$ defined in the following way: for a triple $(a, b, c) \in \mathbb{R}^3$, set $\phi(a, b, c)$ to be the unique polynomial $P \in \mathcal{P}$ satisfying $P(0) = a, P(1) = b, P(2) = c$. This is a well defined map, as the additional condition of $P(3) = 3$ allows us to uniquely determine a polynomial P for any triple (a, b, c). Thus, it remains to show that ϕ is bijective. Firstly, ϕ is injective because if $\phi(a, b, c) = \phi(a', b', c') = P$, then $a = P(0) = a'$ and similar. Secondly, it is surjective because if P is an arbitrary polynomial in $\mathcal{P}$, then $\phi(P(0), P(1), P(2)) = P$. Thus, ϕ is both injective and surjective, so it is a bijection.

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.]

Solution 7: The official solution here does an amazing job explaining the solution.