1. CRT Decomposition

In this problem we use the Chinese Remainder Theorem to compute $3^{302} \mod 385$.

(a) Write 385 as a product of prime numbers in the form $385 = p_1 \times p_2 \times p_3$.

(b) Use Fermat’s Little Theorem to find $3^{302} \mod p_1$, $3^{302} \mod p_2$, and $3^{302} \mod p_3$.

(c) Let $x = 3^{302}$. Use part (b) to express the problem as a system of congruences. Argue that there is a unique solution mod 385, and find it. What is the final answer $3^{302} \mod 385$?

2. Roots

Let’s make sure you’re comfortable with roots of polynomials in the familiar real numbers $\mathbb{R}$. Recall that a polynomial of degree $d$ has at most $d$ roots. In this problem, assume we are working with polynomials over $\mathbb{R}$.

(a) Suppose $p(x)$ and $q(x)$ are two different nonzero polynomials with degrees $d_1$ and $d_2$ respectively. What can you say about the number of solutions of $p(x) = q(x)$? How about $p(x) \cdot q(x) = 0$?

(b) Consider the degree 2 polynomial $f(x) = x^2 + ax + b$. Show that, if $f$ has exactly one root, then $a^2 = 4b$. 
(c) What is the minimal number of real roots that a nonzero polynomial of degree $d$ can have? How does the answer depend on $d$?

3. Roots: The Next Generations

Which of the facts from Problem 2 stay true when $\mathbb{R}$ is replaced by $GF(p)$ (i.e., if you are working modulo a prime number $p$)? Which change, and how?

4. Interpolation Practice

(a) Find a linear polynomial $p(x)$ over $\mathbb{R}$ such that $p(1) = 1$ and $p(3) = 4$.

(b) Find a linear polynomial $q(x)$ over $GF(5)$ such that $q(1) \equiv 1 \pmod{5}$ and $q(3) \equiv 4 \pmod{5}$.