CS 70 Discrete Mathematics and Probability Theory
Summer 2018 Sinho Chewi and Vrettos Moulos **DIS 3A**

1 Count and Prove

(a) Over 1000 students walked out of class and marched to protest the war. To count the exact number of students protesting, the chief organizer lined the students up in columns of different length. If the students are arranged in columns of 3, 5, and 7, then 2, 3, and 4 people are left out, respectively. What is the minimum number of students present? Solve it with Chinese Remainder Theorem.

(b) Prove that for $n \geq 1$, if $935 = 5 \times 11 \times 17$ divides $n^{80} - 1$, then 5, 11, and 17 do not divide n.

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 *minimum* 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

Now go back and do it all over in modular arithmetic...

Which of the facts from above stay true when $\mathbb{R}$ is replaced by GF(p) [i.e., integer arithmetic modulo the prime p]? Which change, and how? Which statements won't even make sense anymore?

4 Interpolate!

Find the lowest-degree polynomial $P(x)$ that passes through the points $(1,4),(2,3),(5,0)$ modulo 7.