1. This problem concerns a sharpening of the result about polynomials and functions from the end of class on W 9/18, and an application thereof. In this problem, denote by $\mathbb{F}_q$ a finite field with exactly q elements.

   (a) Prove that if two polynomials $f, g \in \mathbb{F}_q[x]$ induce the same function $\mathbb{F}_q \to \mathbb{F}_q$ (that is, $f(\alpha) = g(\alpha)$ for all $\alpha \in \mathbb{F}_q$), then either $f = g$ or $\max\{\partial f, \partial g\} \geq q$.

   (b) Consider the polynomial
   $$f(x) = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha).$$
   Prove that f is the *unique monic* polynomial of degree $\leq q$ that satisfies $f(\alpha) = 0$ for all $\alpha \in \mathbb{F}_q$.

   (c) Prove that for all $\alpha \neq 0$ in $\mathbb{F}_q$, $\alpha^{q-1} = 1$ (hint: what is the order of the unit group of $\mathbb{F}_q$?), and deduce from this that
   $$x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha).$$

   (d) Consider the case $q = p$, where p is an odd prime. Deduce from the previous part the following formula (called *Wilson's theorem*):
   $$(p-1)! \equiv -1 \mod p.$$

2. Let K be a subfield of $\mathbb{C}$, and $f \in K[t]$. Call f *separable* if f contains no "multiple roots" in $\mathbb{C}$, i.e. there is no $\alpha \in \mathbb{C}$ such that $(x - \alpha)^2 \mid f$ (where we view these as elements of $\mathbb{C}[t]$ for this statement). Prove that f is separable if and only if $\gcd(f, f') = 1$, where f' is the derivative of f.

   Note Note in particular that separability is really a property of polynomials over $\mathbb{C}$, and yet we can "detect" it using the Euclidean algorithm, using arithmetic over K alone. In fact, there is nothing special about K being a subfield of $\mathbb{C}$, though one must of course define "derivative" differently when working over an abstract field.

3. Let K be a field, and $f_1, f_2, \cdots, f_n \in K[t]$ be polynomials. The following generalizes from class some facts discussed for $n = 2$.

   (a) Give a precise definition of a (or "the") greatest common divisor of the set $\{f_1, \cdots, f_n\}$.

   (b) Prove that g is a greatest common divisor of $\{f_1, f_2, \cdots, f_n\}$ if and only if
   $$\langle f_1, \cdots, f_n \rangle = \langle g \rangle.$$

   (c) Deduce that if g is a greatest common divisor of $\{f_1, f_2, \cdots, f_n\}$, then there exist polynomials $h_1, h_2, \cdots, h_n \in K[t]$ such that
   $$g = h_1 f_1 + h_2 f_2 + \cdots + h_n f_n,$$
   and describe a procedure by which these polynomials could be computed in practice.

4. (Textbook 3.7)
   Say that a polynomial f over a field K is *irreducible* if it cannot be written as the product of two nonconstant polynomials over K, and call f *prime* if whenever $f \mid gh$ for some $g, h \in K[t]$, then either $f \mid g$ or $f \mid h$. Prove that a nonzero polynomial f is prime if and only if it is irreducible.