CS 487: Assignment #4 Due: Wed Apr 5, 2023 at 11:59pm

Submission Instructions: Submit your solutions for each question to Crowdmark.

1. Compute the distinct-degree decomposition of the following squarefree polynomial using the algorithm described in class.
$$f = x^{17} + 2x^{15} + 4x^{13} + x^{12} + 2x^{11} + 2x^{10} + 3x^9 + 4x^8 + 4x^4 + 3x^3 + 2x^2 + 4x \in \mathbb{Z}_5[x].$$
Tell from the output only how many irreducible factors of degree i the polynomial f has, for all i.
Note: For your convenience, file `a4q1.mpl` gives the polynomial in Maple format.

2. Let $q \in \mathbb{N}$ be a prime power.
   (a) If r is a prime number, prove that there are $(q^r - q)/r$ distinct monic irreducibles of degree r in $\mathsf{F}_q[x]$. *Hint:* Use what you know about the polynomials of the form $x^{q^d} - x$.
   (b) Now suppose that r is a prime power. Find a simple formula for the number of monic irreducible polynomials of degree r in $\mathsf{F}_q[x]$.

3. Suppose $p \geq 5$ is a prime, $f \in \mathbb{Z}_p[x]$ has degree 4, and $\gcd(x^p - x, f) = \gcd(x^{p^2} - x, f) = 1$.
   (a) What can you say about the factorization of f in $\mathbb{Z}_p[x]$?
   (b) Enumerate all possibilities for f. In other words, derive, with explanation, a formula in terms of p for the number of polynomials f which satisfy the stated requirements.

4. The squarefree polynomial
$$\begin{aligned} f &= x^{18} - 7x^{17} + 4x^{16} + 2x^{15} - x^{13} - 7x^{12} + 4x^{11} + 7x^{10} + 4x^9 \\ &\quad -3x^8 - 3x^7 + 7x^6 - 7x^5 + 7x^4 + 7x^3 - 3x^2 + 5x + 5 \in \mathbb{Z}_{17}[x] \end{aligned}$$
splits into 3 irreducible factors of degree 6.
   (a) How would you check the above statement without factoring f, by computing at most three gcd's? (You need not actually compute the gcd's.)
   (b) In a Maple session, trace the equal-degree factorization algorithm on computing these factors.
   Note: File `a4q4.mpl` gives the polynomial in Maple format. The Maple commands `Powmod` and `Randpoly` will be useful. See `?Powmod` and `?Randpoly`.

5. Let q be an odd prime, and suppose $f = h_1 h_2 \in \mathsf{F}_q[x]$ has degree $2d$, with h_1 and h_2 distinct, monic irreducibles of degree d. Consider using the following approach to factor f.

   Choose a random $u \in \mathsf{F}_q[x]$ of degree $< d$ and compute $\gcd(u^{(q^d-1)/2} - 1, f)$; if this gcd is equal to 1 or f then repeat with a new random $u \in \mathsf{F}_q[x]$ of degree $< d$.

   Give a concrete input example for which this approach is guaranteed to run forever, i.e., specify q, d and $h_1, h_2 \in \mathsf{F}_q[x]$.