Sample Exam 1
Math 127, Fall 2023

1. (12 points)

(a) List all polynomials of degree 2 in $\mathbf{F}_2[x]$. No explanation necessary.

(b) How many polynomials of degree 5 are there in $\mathbf{F}_2[x]$? Briefly **justify** your answer.

2. (12 points)

(a) Define what it means for $a \in \mathbf{Z}/(17)$ to be a quadratic residue mod 17.

(b) Find an integer b that is a quadratic residue mod 17, but is **not** a perfect square as an integer. Briefly **explain** how you know that b is a quadratic residue mod 13.

3. (12 points) Use the Signed Euclidean Algorithm to find $\gcd(136, 98)$. Show all your work. (If you don't know/remember how to use the Signed Euclidean Algorithm, you can use the unsigned Euclidean Algorithm for partial credit.)

4. (12 points)

n	1	2	3	4	5	6	7	8	9	10
$7^n \pmod{11}$										

(a) Fill in the above table, where all powers of 7 (i.e., all 7^n) are computed in $\mathbf{Z}/(11)$.

(b) Is 7 primitive mod 11? Briefly (1 or 2 sentences) **EXPLAIN** your answer in terms of the definition of primitive.

5. (13 points) Use the Euclidean Algorithm to find the multiplicative inverse of 70 in $\mathbf{Z}/(101)$. Show all your work.

6. (13 points) Use the Euclidean Algorithm to find $\gcd(x^5 + 1, x^4 + x^3 + x^2 + 1)$ in $\mathbf{F}_2[x]$. Show all your work.

7. (13 points) For $a \in \mathbf{Z}$, use the definition of "divides" (and not other results from the homework, etc.) to prove that if 3 divides a, then 3 divides $7a - 39$.

(cont. on next page)

8. (13 points) Consider the following (somewhat strange) algorithm.

- Start with an input list of length n.
- Look through the input list (of length n) to find the smallest element, and delete that smallest element, leaving a list of length $n-1$.
- Look through the new input list of length $n-1$, find the smallest element of the new list, and delete it, leaving a list of length $n-2$.
- Continue looking through the remaining part of the list and deleting the smallest element until the list is empty.

Suppose it takes k units of time to look through a list of length k to find the smallest element and delete it, and suppose all other operations take a negligible amount of time.

(a) If we start with a list of length 4, how many units of time does it take to run the algorithm? Go through all of the steps and find the total amount of time required.

(b) Given a big-O estimate of the time it takes to run the algorithm on a list of length n. Express your answer in the form $O(n^k)$ for some constant k.