

It used to be expensive to make things public and cheap to make them private. Now its expensive to make things private and cheap to make them public.

— Clay Shirky

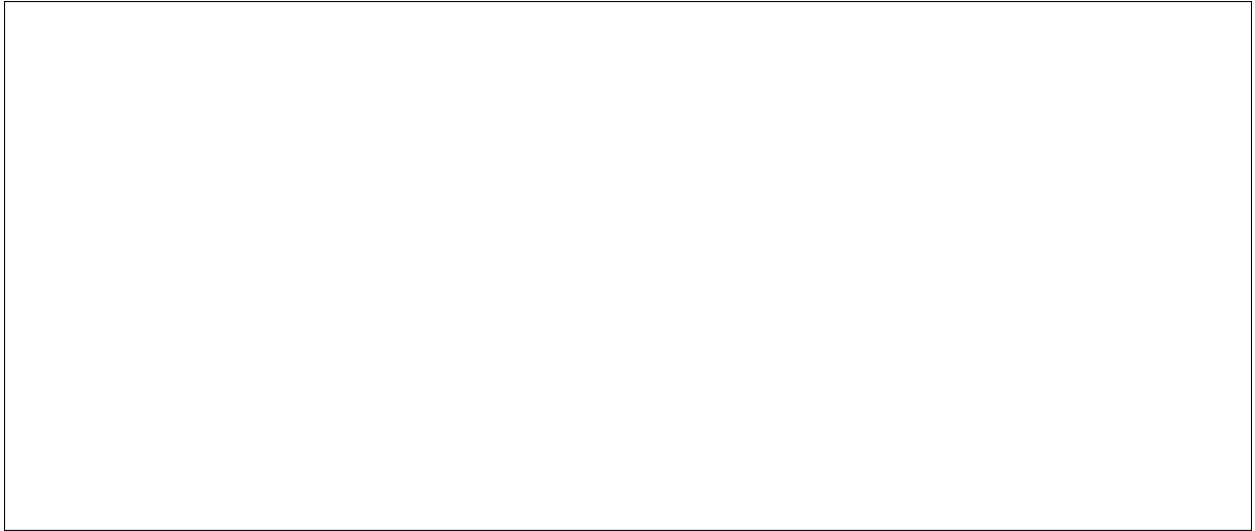
GUIDELINES

- All work must be shown for full credit.
- You can choose to use SageMath code to help you solve the problems. If you do, print out your code.
- Either print out this assignment and write your answers on it, or edit the latex source. Make sure you still show your work! There is one point of extra credit available on this assignment if you use \LaTeX
- You may work with classmates, but be sure to turn in your own written solutions. Write down the name(s) of anyone who helps you.
- Check one:
 - I worked with the following classmate(s): _____
 - I did not receive any help on this assignment.

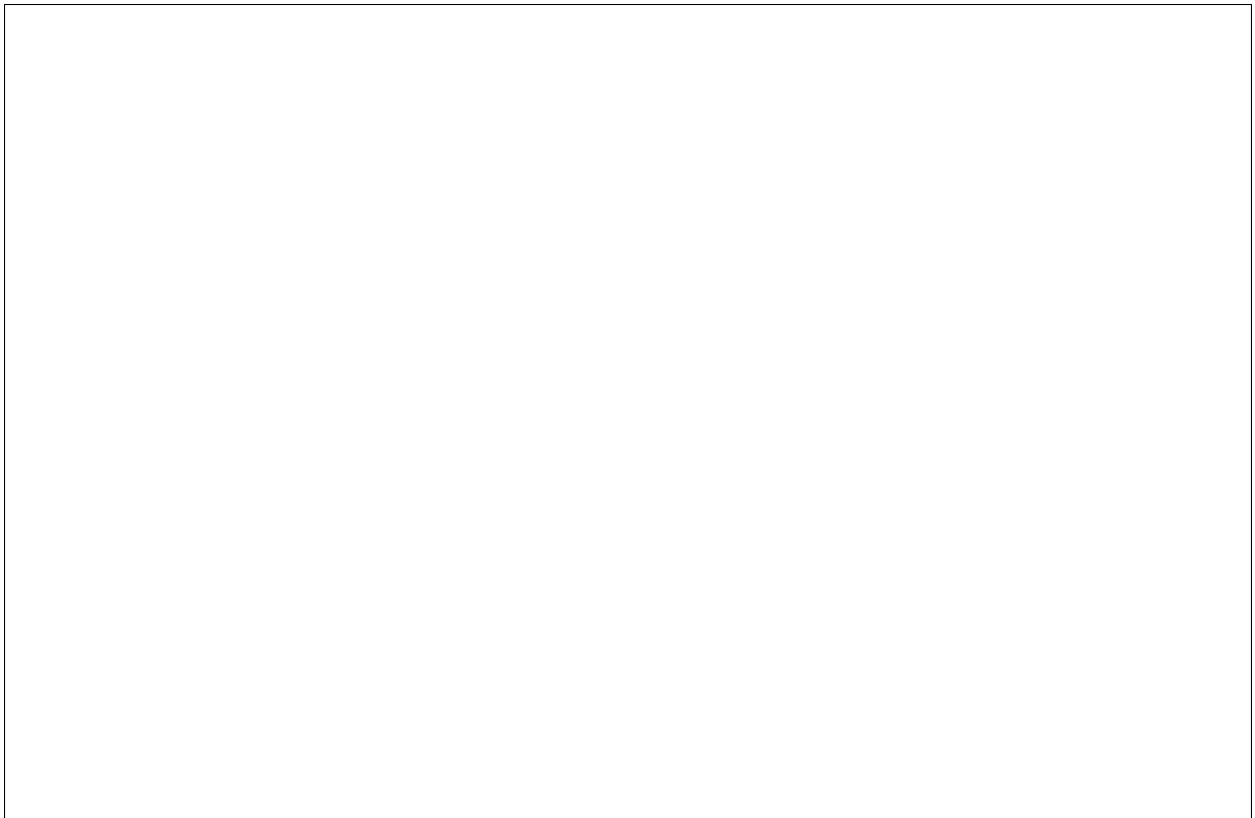
1. GRADED PROBLEMS

1. Let $f(x) = x^5 + x^3 + x^2 + 1$ and $g(x) = x^2 + x + 1$ be polynomials with coefficients in \mathbb{F}_2 , the ring (field) of integers modulo 2. Compute $f(x) + g(x)$ and $f(x) \times g(x)$.

2. Compute $\varphi(60)$ and $\varphi(91)$.



3. Use the rules for Legendre symbols and quadratic reciprocity to determine whether 31 is a square modulo 41.



4. Alice wants to send a message to Bob using the 3-pass protocol. She decides to use the prime $p = 17$, and picks her key, $a = 11$. Bob picks his key, $b = 13$.

(a) What are Alice and Bob's decryption keys?

(b) Alice wants to send the message $m=3$. Find the values of each of the messages that Alice and Bob send back and forth. Does Bob recover Alice's plaintext at the end?

5. Construct the finite field \mathbb{F}_8 using the irreducible polynomial $x^3 + x + 1$. Write down all of the 8 elements of field, and write down the rows of the addition and multiplication table corresponding to the element $x^2 + x$. (In other words add this element to each polynomial in \mathbb{F}_8 , and also multiply it by each element of \mathbb{F}_8 .)