

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

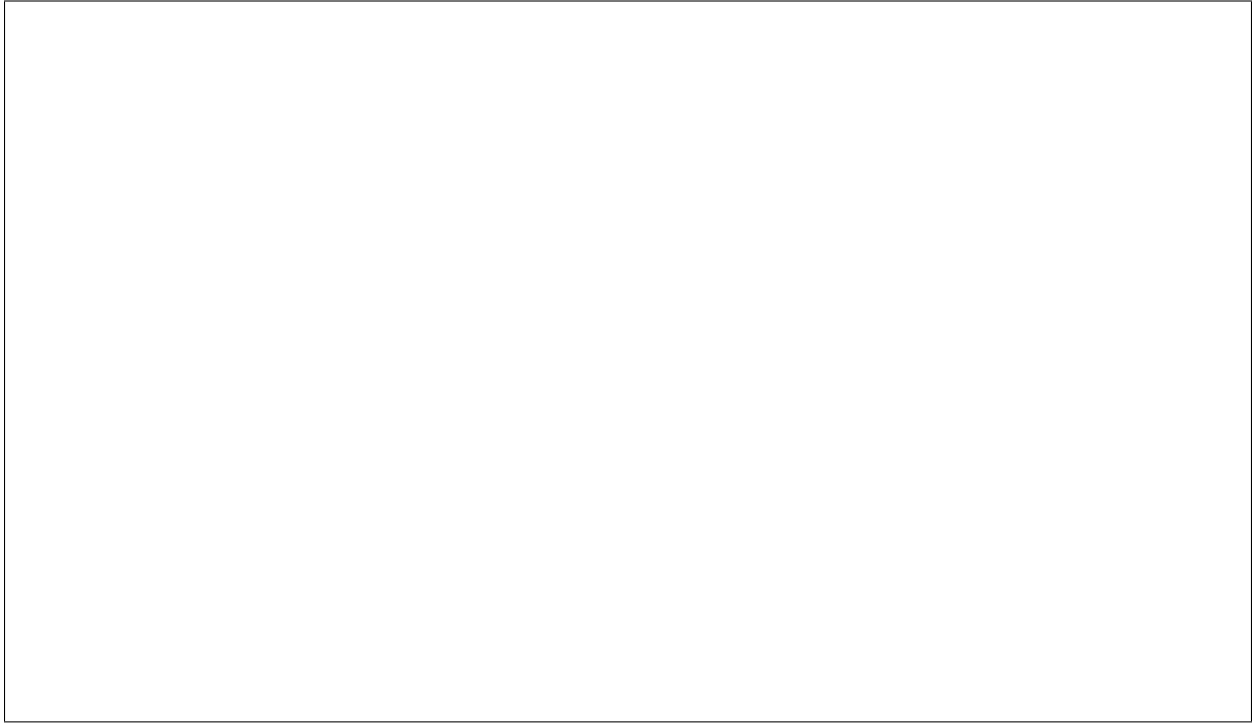
GUIDELINES

- 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.

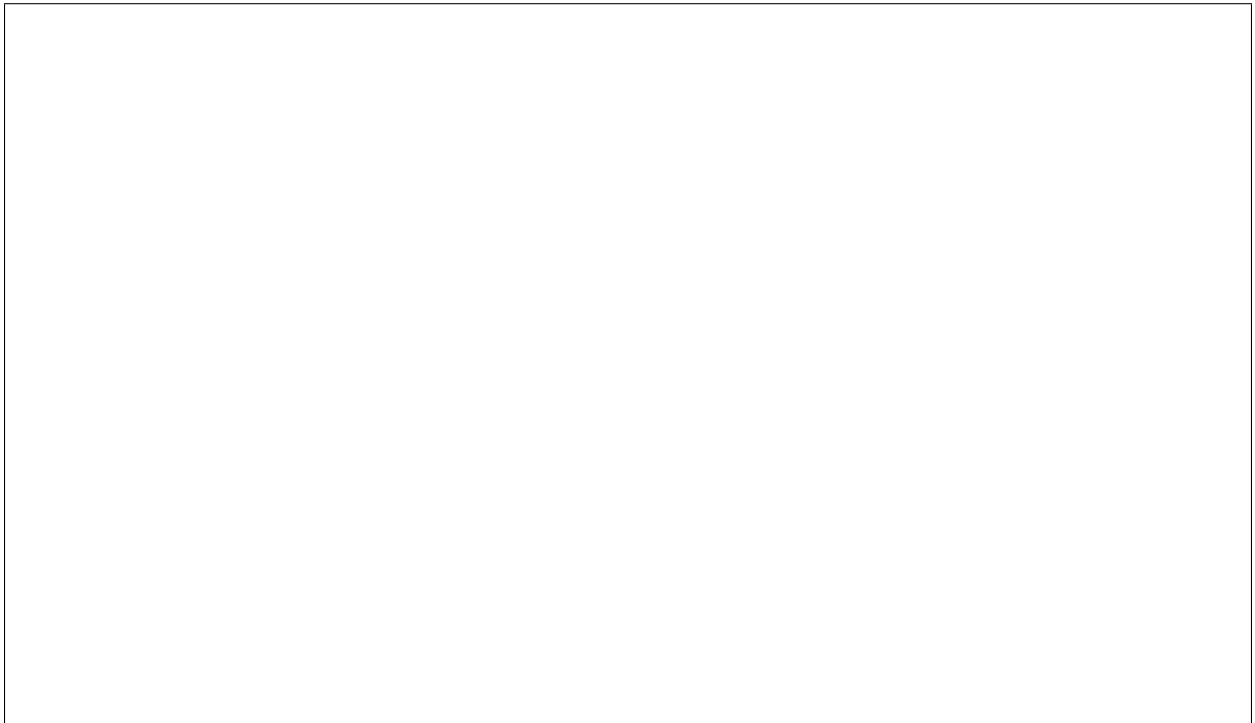
1. GRADED PROBLEMS

1. Use the rules for Legendre symbols (not Jacobi symbols) and quadratic reciprocity to determine whether 41 is a square modulo 71.


2. Repeat question 1 using the rules for Jacobi Symbols instead to determine whether 41 is a square modulo 71.



3. Let $p \equiv 3 \pmod{4}$ be prime, and write $p = 4k + 3$. Give a proof that the equation $x^2 \equiv 1 \pmod{p}$ has no solutions. (Hint: Suppose x exists. Raise both sides to the power $(p-1)/2$ and use Fermats theorem.)



4. Use Fermat's primality test to test 31 and 33 for primality using the bases 2 and 5.



5. Use Euclid's algorithm to find the inverse of $f(x) = x^2$ in the field \mathbb{F}_8 with irreducible polynomial $x^3 + x + 1$.

