

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. a. Compute $\varphi(60)$ and $\varphi(69)$.

b. Find an integer c such that $(a^5)^c \equiv a \pmod{69}$ for all a coprime to 69. (i.e. find a number that “undoes” raising something to the fifth power modulo 69.)

3. Find a solution to both the equations $x \equiv 5 \pmod{12}$ and $x \equiv 2 \pmod{7}$ modulo 84.

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. Write down all of the 8 elements of field \mathbb{F}_8 using the irreducible polynomial $x^3 + x + 1$. Multiply each element by $x^2 + 1$. (In other words find the row of the multiplication table for $x^2 + 1$.)



6. Find the last two digits of $3^{(3^{333})}$. (Note that this is not the same thing as $(3^3)^{333}$.) (Hint: Use Euler's theorem twice!)

