Instructions

- This assignment is due on Tuesday, October 20, 2020 at 2:00 PM EDT. Late submissions will **not** be accepted.
- This assignment consists of two problems. You should choose one for submission.
- Your solution needs to be formatted using the LaTeXtemplate available on OWL.
- All solutions must be written in full sentences.
- You are not allowed to work with others or use any online resources.
- This assignment is worth 5 points.

Problem 1.

1. Suppose $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ where each $a_i \in \mathbb{Z}$ (it is a monic polynomial with integer coefficients). Let p be a prime such that $p \mid a_i$ for all i and $p^2 \nmid a_0$.

   Prove that $f(x) \in \mathbb{Z}[x]$ is an irreducible polynomial.

2. Let p be a prime. Use Part 1 to show that $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p-1}{x-1}$ is irreducible.

   Hint: consider $f(x+1)$.

3. Let $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. Prove or disprove: f is irreducible over any finite field.

Problem 2.

In this exercise, you will be implementing arithmetic in the ring $\mathbb{F}_p[x]/(m(x))$.

Statement

The assignment has two parts.

1. Write a function in Python3 called `solve` that, given a prime p and three polynomials $m(x)$, $q_1(x)$ and $q_2(x)$, computes the sum $q_1(x)+q_2(x)$ and the product $q_1(x)\cdot q_2(x)$ in $\mathbb{F}_p[x]/(m(x))$.

   The polynomials should be stored and passed as lists of coefficients. For example, a polynomial of degree n

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

should be stored/passed as a list

```
coeff_f = [a_0, a_1, ..., a_n]
```

2. Download the file `generate_input.py` from OWL, use it to obtain three sets of inputs, each set consisting of a prime p and three lists corresponding to the polynomials $m(x)$, $q_1(x)$, and $q_2(x)$ respectively, by running

```
python generate_input.py [last three digits of your student
```

and run your program on these three inputs.

Your submission must consist of a single PDF file containing:

1. the *Python code* implementing your solution;
2. and the three *inputs you generated*, and the *output of your program* run on these three inputs.

Examples

Here is an example of what your function `solve` should do:

```
>>> solve(2,[1,1,0,1],[1,1,0],[0,1,1])
sum = 1 + x^2
product = 1
>>> solve(2,[1,1,0,1],[1,0,1],[1,0,1])
sum = 0
product = 1 + x + x^2
>>> solve(2,[1,1,0,1],[1,1,0],[1,1,1])
sum = x^2
product = x
>>> solve(5,[1,0,2,0,3,0,4],[1,0,0,0,0,3],[4,0,3,0,2,2])
sum = 3x^2 + 2x^4
product = 2x + 3x^2 + 2x^4 + 2x^5
```

Notes

- The file `generate_input.py` is written in Python3, and so should be your solution. Make sure you are using a 64bit version of Python3
- Your submission must use the LaTeX template available on OWL.
- Your code should not make use of any external libraries such as `numpy` or `math`. All the auxiliary functions should be implemented by you, and should be included in your submission. You should only use the most basic arithmetic operations such as `+`, `-`, `*`, `//`, `%`.

- Comments in the code are not mandatory. However in the case of an incorrect solution, the comments can provide grounds for partial credit.