Homework 1

For all problems below, assume the finite field is $p = 71$.

Remember, this is done in a finite field so your answer should only contain numbers [0-70] inclusive. There should be no fractions or negative numbers.

Problem 1

Find the elements in a finite field that are congruent to the following values:

- -1
- -4
- -160
- 500

Solution:

- $-1 \equiv 70$ as $1 + 70 \mod 71 = 0$
- $-4 \equiv 67$ as $4 + 67 \mod 71 = 0$
- $-160 \equiv 53$ as $160 + 53 \mod 71 = 0$
- $500 \equiv 3$ as $500 \mod 71 = 3$

Problem 2

Find the elements that are congruent to $a = \frac{5}{6}, b = \frac{11}{12}$, and $c = \frac{21}{12}$. Verify your answer by checking that $a + b = c$ (in the finite field).

- 1. we factorize and compute 5 * 1/6 seperately: $\frac{1}{6} * 6 = 1$ thus we want to find a number x st $x * 6 \equiv 1 \mod 71 \implies x * 6 = 72$ $x = 72/6 = 12$

  thus the answer is: $5 * 12 = 60$
- 2. we factorize and compute 11 * 1/12 seperately: $\frac{1}{12} * 12 = 1$ thus we want to find a number x st $x * 12 \equiv 1 \mod 71 \implies x * 12 = 72$ $x = 72/12 = 6$ thus the answer is: $11 * 6 = 66$
- 3. we factorize and compute 21 * 1/12 seperately: $\frac{1}{12} * 12 = 1$ thus we want to find a number x st $x * 12 \equiv 1 \mod 71 \implies x * 12 = 72$ $x = 72/12 = 6$ thus the answer is: $(21 * 6) \mod 71 = 126 \mod 71 = 55$

we can verify this by checking that $a + b = c$ $60 + 66 = 126 \mod 71 = 55$

Problem 3

Find the elements that are congruent to $a = \frac{2}{3}, b = \frac{1}{2}$, and $c = \frac{1}{3}$.

- a. we find $\frac{1}{3}$ by solving

  $$3x = 1 = 72 \mod 71 \implies x = \frac{72}{3} = 24$$

  thus the answer is $2 * 24 = 48$ $\frac{2}{3} \equiv 48$

- b. we find $\frac{1}{2}$ by solving

  $$2x = 1 = 72 \mod 71 \implies x = \frac{72}{2} = 36$$

  $\frac{1}{2} \equiv 36$

- c. we find $\frac{1}{3}$ by solving

  $$3x = 1 = 72 \mod 71 \implies x = \frac{72}{3} = 24$$

  $\frac{1}{3} \equiv 24$

$$(36 \times 48) \mod 71 = 24$$

Problem 4

What is the modular square root of 12? Verify your answer by checking that $x \cdot x = 12 \pmod{71}$.

answer: 12 as

$$15^2 \mod 71 = 225 \mod 71 = 12$$

Problem 5

The inverse of a 2×2 matrix A is

$$A^{-1} = \frac{1}{\det} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

where A is

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

And the determinant det is

$$\det = a \times d - b \times c$$

Compute the inverse of the following matrix:

$$\begin{bmatrix} 1 & 1 \\ 1 & 4 \end{bmatrix}$$

Verify your answer by checking that

$$AA^{-1} = I$$

Where I is the identity matrix.

$$det = 1 * 4 - 1 * 1 = 3$$

$$\frac{1}{3} \begin{bmatrix} 4 & -1 \\ -1 & 1 \end{bmatrix}$$

we note that $\frac{1}{3} \equiv 24$ and $-1 \equiv 70$
thus we have the matrix

$$A^{-1} = 24 \begin{bmatrix} 4 & 70 \\ 70 & 1 \end{bmatrix} = \begin{bmatrix} 25 & 47 \\ 47 & 24 \end{bmatrix}$$

$$AA^{-1} = \begin{bmatrix} 1 & 1 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} 25 & 47 \\ 47 & 24 \end{bmatrix} = \begin{bmatrix} (25+47) \mod 71 & (47+24) \mod 71 \\ (25+188) \mod 71 & (47+96) \mod 71 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Problem 6

Suppose we have the following polynomials:

$$p(x) = 52x^2 + 24x + 61$$

$$q(x) = 40x^2 + 40x + 58$$

What is $p(x) + q(x)$? What is $p(x) \cdot q(x)$?

$$p(x)+q(x) = ((52+40) \mod 71)x^2+((24+40) \mod 71)x+((61+58) \mod 71) = 21x^2+64x+48$$

$$p(x)\cdot q(x) = (52x^2+24x+61)\cdot(40x^2+40x+58) = (52\cdot40)\cdot x^4+(52\cdot40+24\cdot40)\cdot x^3+(52\cdot58+24\cdot40+61\cdot40)\cdot x^2+(24\cdot58 \tag{1}$$

Use the `galois` library in Python to find the roots of $p(x)$ and $q(x)$.

```python
import galois
from galois import Poly, GF

# Define the finite field
Field = GF(71)
```

```python

p_coeffs = Field([52, 24, 61])  # 52x^2 + 24x + 61
q_coeffs = Field([40, 40, 58])  # 40x^2 + 40x + 58

p = Poly(p_coeffs)
q = Poly(q_coeffs)

p_roots = p.roots()
q_roots = q.roots()

print("Roots of p(x):", p_roots)
print("Roots of q(x):", q_roots)

pq = p * q

pq_roots = pq.roots()

print("Roots of p(x) * q(x):", pq_roots)
```

The roots of $p(x)$, $q(x)$, and $p(x)q(x)$ are:

- Roots of $p(x)$: `p_roots`
- Roots of $q(x)$: `q_roots`
- Roots of $p(x)q(x)$: `pq_roots`

What are the roots of $p(x)q(x)$?

Problem 7

Find a polynomial $f(x)$ that crosses the points $(10, 15)$, $(23, 29)$

Since these are two points, the polynomial will be of degree 1 and be the equation for a line ($y = ax + b$).

The solution will be of the form $f(x) = ax + b$

$$a = \frac{29 - 15}{23 - 10} = \frac{14}{13} = (14 * 11) \mod 71 = 12$$

$$b = 15 - 12 * 10 = 15 - 120 = 15 + 22 = 37$$

we can verify this by checking that $f(23) = 29$

$$f(23) = 12 * 23 + 37 = 313 \mod 71 = 29$$

Problem 8

What is Lagrange interpolation and what does it do?

Lagrange interpolation is a method for finding the unique polynomial of degree $n - 1$ that passes thorugh all n points.

Find a polynomial that crosses through the points $(0, 1)$, $(1, 2)$, $(2, 1)$.

```python
import galois

GF = galois.GF(71)

x = GF([0, 1, 2])
y = GF([1, 2, 1])

f = galois.lagrange_poly(x, y)

print(f"Lagrange polynomial: {f}")

# Verify the polynomial passes through the given points
for xi, yi in zip(x, y):
    if not f(xi) == yi:
        assert False, f"f({xi}) = {f(xi)} (expected {yi})"
```

the answer is: $70x^2 + 2x + 1$

Use this Stack Overflow answer as a starting point: `https://stackoverflow.com/a/73434775`