This is a customised assignment for ag14774.

More SAGE

Finite Fields

A finite field can be defined using the command `FiniteField`. Alternatively, you can use the command `GF`. As an example, the following code defines the fields $\mathbb{F}_{19}$:

```
sage: F=FiniteField(19)
sage: F
Finite Field of size 19
sage: F.list()
[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18]
```

The following code defines the field $\mathbb{F}_{2^8}$:

```
sage: F=FiniteField(2^8,'x')
sage: F
Finite Field in x of size 2^8
sage: F.modulus()
x^8 + x^4 + x^3 + x^2 + 1
```

Polynomial Rings Over a Field

Example of defining a univariate polynomial ring over a field.

```
sage: F=GF(23)
sage: F
Finite Field of size 23
sage: R.<x>=F[]
sage: R
Univariate Polynomial Ring in x over Finite Field of size 23
```

1 Inversion

Write a function `invert(n, m)` that takes two positive integers $0 \leq n < m$ and returns $1/n \pmod{m}$ if this expression makes sense and raises an exception if it does not. Do not use Sage's modular inversion (i.e. computing $1/x$ in a group). You may use functions that you wrote in previous assignments.

```
def invert(n,m):
    (g,a,b) = MyXGCD(n,m)
    if g!=1:
        raise Exception("Not invertible!")
    return Integers(m)(a)
```

2 Monic Irreducibles

Find all the monic (leading coefficient 1) irreducible polynomials of degree two over $GF(7)[X]$. You should get 21.

```
X^2 + 1
X^2 + 2
X^2 + 4
X^2 + X + 3
X^2 + X + 4
X^2 + X + 6
X^2 + 2*X + 2
X^2 + 2*X + 3
X^2 + 2*X + 5
X^2 + 3*X + 1
X^2 + 3*X + 5
X^2 + 3*X + 6
```

Note: in SAGE, you can use the method `is_irreducible()` to check whether a polynomial is irreducible. Also, the method `is_monic()` tells you whether the polynomial is monic.

3 Degree 3

Find one monic, irreducible polynomial of degree 3 over $GF(7)[X]$.

4 Classification of elements

Classify all elements of $GF(2)[X]/(X^3+1)$ as zero, unit, zero-divisor or neither.

5 Automorphisms

Let $A = GF(5)[X]/(X^2+2X+4)$ and $B = GF(5)[Y]/(Y^2+Y+2)$.

1. Find the automorphisms of A and B.

2. Find the isomorphisms from A to B.

6 GF 2^8

Let $p(X) = X^8+X^6+X^5+X^4+1$.

1. Compute $(X^6+X^5+X^4)(X^7+X^5+X^2)+(X^6+X^4+X^3)$ in $GF(2^8)$ using the representation modulo $p(X)$.

2. Solve the equation $X^3+X^2+X = w(X)\cdot(X^5+1)$ for $w(X)$ in $GF(2^8)$ represented modulo $p(X)$.

3. Compute the powers of the Frobenius map in $GF(2^8)$ modulo $r(Z) = Z^8 + Z^7 + Z^6 + Z + 1$ (this is irreducible).

4. Find an isomorphism from $GF(2)[Z]/r(Z)$ to $GF(2)[X]/p(X)$ — just find the image of Z.

7 Degree three

In this question we consider the field $GF(3^3)$ with two representations modulo the irreducible polynomials $p(X) = X^3 + X^2 + 2X + 1$ and $q(Y) = X^3 + X^2 + X + 2$.

1. Reduce X^3 and X^4 modulo $p(X)$ and Y^3 and Y^4 modulo $q(Y)$.

2. How many elements does the group of automorphisms of $GF(2^3)$ have? What are these elements "called"?

3. Compute the Frobenius map for the representations modulo $p(X)$ and $q(Y)$. That is, for $\phi(a + bX + cX^2) = (u + vX + wX^2)$ find u, v, w in terms of a, b, c.

4. Do the same for all powers of the Frobenius map (hint: there aren't too many.)

5. Find all the isomorphisms from the representation modulo $p(X)$ to the representation modulo $q(Y)$. Hint: how many are there?

6. Find the explicit multiplication formulas in both representations. That is, for $(a + bX + cX^2)(d + eX + fX^2) = (u + vX + wX^2)$ find u, v, w in terms of a – f. Repeat the same working over Y.