HW6: yanliang 11288948 2018/3/1

1.

The inverse should be:

X^9+x^8+x^6+x^5+x^3+x^2

And the step is like this first find the

x^10+x^5+1=(x^4+1)*(x^6+x^2+x)+x^2+x+1

x^4+1=(x^2+x+1)*(x^2+x)+x+1

x^2+x+1=(x+1)*(x)+1

x+1=(x+1)*1+0.

So we know that gcd(x^10+x^5+1,x^4+1)=1

Which means x^4+1 is invertible

And trace back we get

1=x^2+x+1+(x+1)x

-->1=x^2+x+1+(x^4+1+(x^2+x+1)*(x^2+x))x=(x^4+1)*x+(x^2+x+1)(x^3+x^2+1)

-->1=(x^4+1)*x+((x^10+x^5+1)+(x^4+1)*(x^6+x^2+x))(x^3+x^2+1)

---> the poly before x^4+1 is x^9+x^8+x^6+x^5+x^3+x^2 so that is the inverse

Verification through sage:

```
age: f2x.<x>=GF(2)[]
sage: qqr.<a>=QuotientRing(f2x,x^10+x^5+1)
sage: (a^4+1)*(a^9+a^8+a^6+a^5+a^3+a^2)
1
```

2.

Code to do this:

```
f3x=GF(3)[];
for i in set([1,1]):
        for j in range(3):
                for m in range(3):
                        for n in range(3):
                                for k in range(3):
                                        poly=i*x^4+j*x^3+m*x^2+n*x+k
                                        if(poly.is_irreducible()):
                                                print poly
```

The irreducible polynomials of degree 4 over Z/3Z is the following, so the idea is loop through all the possible of {0,1,2} for the coefficient and check if that is irreducible in sage or not

x^4 + x + 2

x^4 + 2*x + 2

x^4 + x^2 + 2

x^4 + x^2 + x + 1

x^4 + x^2 + 2*x + 1

x^4 + 2*x^2 + 2

x^4 + x^3 + 2

x^4 + x^3 + 2*x + 1
x^4 + x^3 + x^2 + 1
x^4 + x^3 + x^2 + x + 1
x^4 + x^3 + x^2 + 2*x + 2
x^4 + x^3 + 2*x^2 + 2*x + 2
x^4 + 2*x^3 + 2
x^4 + 2*x^3 + x + 1
x^4 + 2*x^3 + x^2 + 1
x^4 + 2*x^3 + x^2 + x + 2
x^4 + 2*x^3 + x^2 + 2*x + 1
x^4 + 2*x^3 + 2*x^2 + x + 2

3.
Do this in sage will find an irreducible polynomial for you:
f131072.<x>=GF(**2^17**)
x.minpoly()
----
x^17 + x^3 + 1 is the irreducible polynomial with degree 17.

sage: order=**2^17-1**
sage: order.factor()
131071
sage: (x+**1**)^**1**
x + 1
sage: (x+**1**)^**131071**
1
sage:

Since the order of this field is a prime, so everything should be a generator except 1,
So x+1 can be the generator of this field.

4.
My last digit of my id is 478,
Do the following sage command will find it.
So need to find a field with 2^478 elements then find the min polynomial on it.
sage: fx.<x>=GF(**2^478**)
sage: x.minpoly()
x^478 + x^121 + 1
sage: x.minpoly().factor()
x^478 + x^121 + 1

So based on the above stuff the irreducible polynomial should be :
$x^{478} + x^{121} + 1$