Cryptography Assignment - 6

Pramod Aravind Byakod

1: Compute the multiplicative inverse of $x^4 + 1$ modulo $x^10 + x^5 + 1$ over $Z/2Z$ using Extended Euclidean Algorithm. You need to show steps.

$x10 + x5 + 1 = (x6 + x2 + x)\ (x4 + 1) + (x2 + x + 1)$
$x4 + 1 = (x2 + x)(x2 + x + 1) + (x + 1)$
$x2 + x + 1 = x(x + 1) + 1$
$x + 1 = x\ (1) + 1$
$1 = 1 * 1 + 0$
Now Applying the Extended Euclidean Algorithm, we get
$1 = (x + 1) - x$
$1 = (x+1) - ((x2 + x + 1) - x(x+1))\ x$
$1 = (x+1) - x\ (x2 + x + 1) + x2(x+1)$
$1 = (1+x)\ (1+x2) - x\ (x2 + x + 1)$
$1 = (x2 + 1)\ (x4 + 1) + (x4 + x3 + x2)\ (x2 + x + 1)$
$1 = (x4 + x3 + x2)\ (x10 + x5 + 1) + (x10 + x9 + x8 + x6 + x3 + x2 + 1)\ (x4 + 1)$
Thus the multiplicative inverse of x4 + 1 modulo x10 + x5 over Z/2Z is
$(x10 + x9 + x8 + x6 + x3 + x2 + 1)$

2: List all the monic irreducible polynomials over Z/3Z of degree 4.

Program:

```
for cof1 in range (2):
   for cof2 in range (2):
     for cof3 in range (2):
        for cof4 in range (2):
          if (x^4+cof1*x^3+cof2*x^2+cof3*x^1+cof4).is_irreducible():
            x^4+cof1*x^3+cof2*x^2+cof3*x^1+cof4
```

Output:

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

3: Find one irreducible polynomial f(x) of degree 17 over GF(2). Then find a multiplicative generator for GF(2)[x]/(f(x)), and prove that it is a multiplicative generator by using Corollary 2.14.3 in the Buchmann book.

Program:

```
P = PolynomialRing(GF(2),'x')
for p in P.monics(of_degree = 17):
    if p.is_irreducible():
        print(p)
```

Output:

x^17 + x^3 + 1
x^17 + x^3 + x^2 + x + 1
x^17 + x^5 + 1
x^17 + x^5 + x^3 + x^2 + 1
x^17 + x^5 + x^4 + x + 1
x^17 + x^5 + x^4 + x^3 + x^2 + x + 1
x^17 + x^6 + 1
x^17 + x^6 + x^4 + x^2 + 1
x^17 + x^6 + x^5 + x^3 + 1
x^17 + x^6 + x^5 + x^4 + x^3 + x + 1

x^17 + x^7 + x^3 + x^2 + 1

……..

Let's take f(x) = x^17 + x^3 + 1

R.<x>=GF(2)[ ]

F.<a> = GF(2^17, modulus = x^17 + x^3 + 1)

F.multiplicative_generator() = a

a.multiplicative_order () = 131071

Irreducible polynomial f(x) of degree 17 over GF(2) = x^17 + x^3 + 1
Multiplicative generator for GF(2)[x]/(f(x)) = a

According to corollary 2.14.3, Let n E N. If g^n = 1 and g^n/p !=1 for each prime divisor p of n, then n is the order of g.

In the above example, g = 2 and n = 17 and 2^17 = 1 mod 131071
Prime divisors of n are 1 and 17. So, g^(2/1) != 1 and g^(2/17) != 1.
Hence the corollary holds good.

4: Let d be the last three digits of your id number, viewed as an integer. Find one irreducible polynomial of degree d over GF(2).

ID = 113436879 therefore d = 879

Program:

```
P = PolynomialRing(GF(2),'x')
for p in P.polynomials(of_degree = 879):
   if p.is_irreducible():
      print(p)
      break;
```

Output:

x^879 + x^9 + x^5 + x^3 + 1