CS 4823: Homework #6

Due on March 2, 2018

Christopher Tse

Problem 1

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

Solution

Let $f(x)=x^4+1$ and $g(x)=x^{10}+x^5+1$. Applying the Extended Euclidean Algorithm using long division:

$$\begin{aligned} g(x) &= f(x)(x^6+x^2+x)+(x^2+x+1) \\ f(x) &= (x^2+x+1)(x^2+x)+(x+1) \\ x^2+x+1 &= (x+1)x+1 \\ x+1 &= 1(x+1)+0 \end{aligned}$$

Verifying that $gcd(f(x),g(x))=1$ we know that an inverse exists. Substituting back up to rewrite in the form of Bezout's Identity:

$$\begin{aligned} 1 &= (x^2+x+1)-(x+1)(x) \\ x+1 &= f(x)-(x^2+x+1)(x^2+x) \\ x^2+x+1 &= g(x)-f(x)(x^6+x^2+x) \end{aligned}$$

$$\begin{aligned} 1 &= (x^2+x+1)-[f(x)-(x^2+x+1)(x^2+x)](x) \\ &= g(x)-f(x)(x^6+x^2+x)-\{f(x)-[g(x)-f(x)(x^6+x^2+x)](x^2+x)\}(x) \\ &= g(x)-f(x)(x^6+x^2+x)-f(x)+g(x)(x^2+x)(x)-f(x)(x^6+x^2+x)(x^2+x)(x) \\ &= g(x)[1+x(x^2+x)]+f(x)(-1)[1+x(x^2+x)(x^6+x^2+x)] \\ 1 &= g(x)(x^3+x^2+1)+f(x)(x^9+x^8+x^5+1) \end{aligned}$$

The multiplicative inverse of x^4+1 modulo x^10+x^5+1 over $\mathbb{Z}/2\mathbb{Z}$ is $x^9+x^8+x^5+1$.

Problem 2

List all the monic irreducible polynomials over $\mathbb{Z}/3\mathbb{Z}$ of degree 4.

Solution

A polynomial $p(x)$ is irreducible if it does not have any linear or quadratic factors. Let M be the set of all polynomials of degree 4 over $\mathbb{Z}/3\mathbb{Z}$.

Any polynomial of degree 4 where $p(0) = 0$, $p(1) = 0$, $p(-1) = 0$ has a linear factor. For cases where $p(0) = 0$, we can remove all polynomials from M where the constant is 0. For cases $p(1) = 0$ and $p(-1) = 0$, we can determine them by trial and eliminate the ones that meet those conditions from M.

After eliminating the polynomials with linear factors, we must also remove from M the polynomials which have quadratic factors. To determine these, we can find all monic irreducible polynomials of degree 2, take the products of all pairs, then remove those products from M. The resulting answer set of M is then:

$$
\begin{aligned}
M = \{&x^4 + x + 2,\\
&x^4 + 2x + 2,\\
&x^4 + 2x + 2,\\
&x^4 + x^2 + 2,\\
&x^4 + x^2 + 2x + 1,\\
&x^4 + 2x^2 + 2,\\
&x^4 + x^3 + 2,\\
&x^4 + x^3 + 2x + 1,\\
&x^4 + x^3 + x^2 + 1,\\
&x^4 + x^3 + x^2 + x + 1,\\
&x^4 + x^3 + x^2 + 2x + 2,\\
&x^4 + x^3 + 2x^2 + 2x + 2,\\
&x^4 + 2x^3 + 2,\\
&x^4 + 2x^3 + x + 1,\\
&x^4 + 2x^3 + x + 2,\\
&x^4 + 2x^3 + x^2 + 1,\\
&x^4 + 2x^3 + x^2 + x + 2,\\
&x^4 + 2x^3 + x^2 + 2x + 1,\\
&x^4 + 2x^3 + 2x^2 + x + 2\}
\end{aligned}
$$

Problem 3

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

Solution

Using Sage:

```
sage: PR = GF(2)['x']
sage: PR.irreducible_element(17)
```

We get an irreducible polynomial of $x^{17} + x^3 + 1$.

To find the generator for this polynomial, we first find the number of elements in the field. Since modulo over a polynomial of degree 17 results in polynomials of degree 16 or less, the number of elements n is $n = 2^{17} - 1 = 131071$ (removing 0).

Using Corollary 2.14.3, we can find some generator g such that $g^n = 1$.

Using sage and testing an arbitrary polynomial $g = a^2 + 1$:

```
sage: F2.<x> = GF(2)[]
sage: f = x^17 + x^3 + 1
sage: Q.<a> = F2.quotient(f)
sage: g = a^2 + 1
sage: g ^ 131071 # outputs 1
```

We can see that g^n indeed results in 1. Since n is prime, there are no other divisors to check. Therefore, g is a generator for this field.

Problem 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).

Solution

ID number is 112971666, therefore $d = 666$

Using Sage:

```
sage: d = 666
sage: PR = GF(2)['x']
sage: PR.irreducible_element(666)
```

We get an output of $x^{666} + x^{10} + x^7 + x^2 + 1$