## Chapter 4

4.1 If the polynomial $p(x) = x^4 + x + 1$ is irreducible, then it can not be factorized, hence

$$p(x) \neq a(x) \cdot b(x)$$

where the polynomials $a(x)$ and $b(x)$ both have degree less than $p(x)$. We only need to show that $p(x)$ is not divisible with irreducible polynomials of degree less than or equal to half of the degree of $p(x)$. Possible polynomials are

$$a(x) \in \{x, x+1, x^2+x+1\}$$

which is the set of all irreducible polynomials of degree at most $2 (= \deg\{p(x)\}/2)$.

None of the above polynomials divides $p(x)$ and thus, $p(x)$ is irreducible.

4.2 The polynomial in 4.1 is not only irreducible, it is also primitive, i.e., the element $\alpha = x$ will generate all elements except 0.

| $i$ | $\alpha^i$ | polynomial | vector |
|---|---|---|---|
| 1 | $\alpha^1$ | $\alpha$ | 0010 |
| 2 | $\alpha^2$ | $\alpha^2$ | 0100 |
| 3 | $\alpha^3$ | $\alpha^3$ | 1000 |
| 4 | $\alpha^4$ | $\alpha+1$ | 0011 |
| 5 | $\alpha^5$ | $\alpha^2+\alpha$ | 0110 |

| $i$ | $\alpha^i$ | polynomial | vector |
|---|---|---|---|
| 6 | $\alpha^6$ | $\alpha^3+\alpha^2$ | 1100 |
| 7 | $\alpha^7$ | $\alpha^3+\alpha+1$ | 1011 |
| 8 | $\alpha^8$ | $\alpha^2+1$ | 0101 |
| 9 | $\alpha^9$ | $\alpha^3+\alpha$ | 1010 |
| 10 | $\alpha^{10}$ | $\alpha^2+\alpha+1$ | 0111 |

| $i$ | $\alpha^i$ | polynomial | vector |
|---|---|---|---|
| 11 | $\alpha^{11}$ | $\alpha^3+\alpha^2+\alpha$ | 1110 |
| 12 | $\alpha^{12}$ | $\alpha^3+\alpha^2+\alpha+1$ | 1111 |
| 13 | $\alpha^{13}$ | $\alpha^3+\alpha^2+1$ | 1101 |
| 14 | $\alpha^{14}$ | $\alpha^3+1$ | 1001 |
| 15 | $\alpha^{15}$ | 1 | 0001 |

From the table we get that the element (0110) can also be written as $\alpha^5$. Further we see that $\alpha^{15} = 1$. From this it follows

$$(0110)^{\frac{1}{2}} = (\alpha^5)^{\frac{1}{2}} = (1 \cdot \alpha^5)^{\frac{1}{2}} = (\alpha^{15} \cdot \alpha^5)^{\frac{1}{2}} = (\alpha^{15+5})^{\frac{1}{2}} = \alpha^{\frac{20}{2}} = \alpha^{10} = (0111)$$

4.3 The elements in the field can be written as two-tuples where every component is one of $\{0, 1, 2\}$. Thus, the elements are

$$(00, 01, 02, 10, 11, 12, 20, 21, 22).$$

The given polynomial is not of interest if we are not defining the operations in the field. We use $\pi(\alpha) = 0$. This gives

$$\alpha^2 + \alpha + 2 = 0 \Leftrightarrow \alpha^2 = -\alpha - 2 = 2\alpha + 1$$

The result of a multiplication of two elements is given by

$$\alpha^i \cdot \alpha^j = \alpha^{i+j \pmod{3^2-1}}.$$

To do this we must define $\alpha^i$.

| $i$ | $\alpha^i$ | polynomial | vector |
|---|---|---|---|
| 1 | $\alpha^1$ | $\alpha$ | 10 |
| 2 | $\alpha^2$ | $2\alpha+1$ | 21 |
| 3 | $\alpha^3$ | $2\alpha+2$ | 22 |
| 4 | $\alpha^4$ | 2 | 02 |

| $i$ | $\alpha^i$ | polynomial | vector |
|---|---|---|---|
| 5 | $\alpha^5$ | $2\alpha$ | 20 |
| 6 | $\alpha^6$ | $\alpha+2$ | 12 |
| 7 | $\alpha^7$ | $\alpha+1$ | 11 |
| 8 | $\alpha^8$ | 1 | 01 |

As an example we give

$$(12) \cdot (11) = (\alpha+2) \cdot (\alpha+1) = \alpha^6 \cdot \alpha^7 = \alpha^{6+7 \pmod 8} = \alpha^5 = 2\alpha = (20)$$

4.4 The number of elements in each field is a prime. We define the operations as modulo operations

a)

| $+$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

| $\star$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

b)

| $+$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 0 | 1 | 2 | 3 | 4 | 5 |

| $\star$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 0 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 0 | 6 | 5 | 4 | 3 | 2 | 1 |

4.5

| $\star$ | 0 | 1 | $x$ | $x+1$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | $x$ | $x+1$ |
| $x$ | 0 | $x$ | $x+1$ | 1 |
| $x+1$ | 0 | $x+1$ | 1 | $x$ |

4.6 Let $(c)x = \underbrace{x + x + \cdots + x}_{c}$. The binomial theorem gives

$$(x+y)^p = x^p + (c_1)x^{p-1}y + \cdots + (c_{p-1})xy^{p-1} + y^p,$$

where $c_i = \binom{p}{i}$. For $1 \le i \le p-1$ all $c_i$ will now contain a factor $p$. Since the characteristic is $p$ we get $(c_i)x^{p-i}y^i = 0$ for $1 \le i \le p-1$ and $(x+y)^p = x^p + y^p$.

4.7 Using Euclid's algorithm.

$$\begin{aligned} z^{-7}+1 &= (z^{-1}+1)\cdot(z^{-6}+z^{-5}+z^{-2}+1) + z^{-5}+z^{-3}+z^{-2}+z^{-1} \\ z^{-6}+z^{-5}+z^{-2}+1 &= (z^{-1}+1)\cdot(z^{-5}+z^{-3}+z^{-2}+z^{-1}) + z^{-4}+z^{-2}+z^{-1}+1 \\ z^{-5}+z^{-3}+z^{-2}+z^{-1} &= z^{-1}\cdot(z^{-4}+z^{-2}+z^{-1}+1) + 0 \end{aligned}$$

When the remainder is 0, the previous remainder is the gcd.

$$\gcd(z^{-7}+1, z^{-6}+z^{-5}+z^{-2}+1) = z^{-4}+z^{-2}+z^{-1}+1.$$

4.8 a) In a distinguishing attack we try to distinguish the keystream, z, from a completely random sequence. In a random sequence, the probability that 2 consecutive bits are the same is $1/2$. For the stop-and-go-generator the probability that two consecutive keystream bits are the same is given by

$$P(z_i = z_{i-1}) = P(L_{1_i} = 0) + P(L_{1_i} = 1)P(L_{2_j} = L_{2_{j-1}}) = 1/2 + 1/2 \cdot 1/2 = 3/4.$$

So by looking at all pairs of keystream bits we can determine if the sequence was produced by the stop-and-go-generator or if it is a random keystream.

b) We have the following 3 possible keystream sequences:

$\hat{z}_1 = C \oplus m_1 = (0111\ 0101\ 1101\ 0110\ 1100\ 0011\ 1001\ 1001)$
$\hat{z}_2 = C \oplus m_2 = (0100\ 0111\ 1010\ 1100\ 1000\ 1111\ 0101\ 1010)$
$\hat{z}_3 = C \oplus m_3 = (0011\ 0001\ 1111\ 1111\ 1001\ 0111\ 1100\ 0000)$

The number of bit pairs with both bits equal is 14, 13 and 23 respectively. We can draw the conclusion that $m_3$ was the message sent.

4.9 a) In the field $\mathbb{F}_3$ the additive inverse is given by:

| a | 0 | 1 | 2 |
|---|---|---|---|
| -a | 0 | 2 | 1 |

so we get

$$\frac{1}{D^{-1}+2} = \frac{1}{D^{-1}(1+2D)} = \frac{D}{1-D} = D\frac{1}{1-D}$$

The sequence has period one and is given by $0[1]^\infty$.

c) In the field $\mathbb{F}_2$ we have $a = -a$ so we get

$$\frac{1}{D^{-2}+D^{-1}+1} = \frac{D^{-1}+1}{D^{-3}+1} = \frac{D^2+D^3}{1+D^3} = D\frac{D+D^2}{1-D^3}$$

The sequence has period 3 and is given by $0[011]^\infty$.

4.10 b) We have the polynomial $C(D) = 1+D+D^2+D^4$. We calculate $\frac{1}{C(D)}$ and look for the first remainder of the form $1 \cdot D^T$. This will give the period $T$. We get $T = 7$.

c) We have the polynomial $C(D) = 1 + D^3 + D^6$. We do the same as in b) and get $T = 9$