These equations lead to

$$0 = g_4 = g_1 \qquad g_2 = g_3 = g_5 = g_6$$

Therefore

$$g(x) = x^6 + x^5 + x^3 + x^2 + g_0$$

We find the HCF of $g(x)$ with $g_0 = 1$ and $f(x)$:

$$\begin{array}{l} x^6 + x^5 + x^3 + x^2 + 1 \quad \overline{\left) \begin{array}{l} x^7 \quad + x^5 + x^4 \quad + x^2 + x + 1 \\ x^7 + x^6 \quad + x^4 + x^3 \quad + x \end{array} \right.} \\ \qquad\qquad\qquad\quad x^6 + x^5 \quad + x^3 + x^2 \quad + 1 \end{array}$$

Thus HCF is $x^6 + x^5 + x^3 + x^2 + 1$ and

$$x^7 + x^5 + x^4 + x^2 + x + 1 = (x + 1)(x^6 + x^5 + x^3 + x^2 + 1) \qquad (7.5)$$

Observe that the dimension of the null space of $\mathbf{Q} - \mathbf{I}$ is 2. Therefore, $f(x)$ has two distinct irreducible factors. Therefore, either $h(x) = x^6 + x^5 + x^3 + x^2 + 1$ is irreducible or it is square of a binary cubic irreducible polynomial or it is cube of a binary quadratic irreducible polynomial. However,

$$\begin{aligned} (x^2 + x + 1)^3 &= x^6 + x^2(x + 1)(x^2 + x + 1) + (x + 1)^3 \\ &= x^6 + (x^3 + x^2)(x^2 + x + 1) + x^3 + x(x + 1) + 1 \\ &= x^6 + x^5 + x^4 + x^3 + x^4 + x^3 + x^2 + x^3 + x^2 + x + 1 \\ &= x^6 + x^5 + x^3 + x + 1 \neq h(x) \\ (x^3 + x + 1)^2 &= x^6 + x^2 + 1 \neq h(x) \\ (x^3 + x^2 + 1)^2 &= x^6 + x^4 + 1 \neq h(x) \end{aligned}$$

Hence $h(x)$ is irreducible and (7.5) expresses $f(x)$ as a product of prime factors.

The Chinese remainder theorem for integers states that given primes $p_1, p_2, \ldots, p_k$ and integers $a_1, a_2, \ldots, a_k$, the simultaneous congruences

$$x \equiv a_i (\text{mod } p_i^{e_i})$$

e_i, $1 \leq i \leq k$, positive integers, have a unique solution

$$\text{mod} \prod_i p_i^{e_i}$$

The main tool in the proof of this theorem is Euclid's division algorithm which holds for integers. If F is a field, the polynomial ring $F[x]$ is a Euclidean domain and so Euclid's division algorithm is also true for the ring $F[x]$.

Theorem 7.6 – Chinese remainder theorem for polynomials
Given irreducible polynomials $f_1(x), f_2(x), \ldots, f_k(x)$ and arbitrary polynomials $a_1(x), a_2(x), \ldots, a_k(x)$ over a field F, the simultaneous congruences

$$h(x) \equiv a_i(x) (\text{mod } f_i(x)^{e_i})$$

where $e_1, e_2, \ldots, e_k$ are positive integers, have a unique solution for

$$h(x) \bmod \prod_i f_i(x)^{e_i}$$

Proof

The ring $F[x]$ being a Euclidean domain, any two elements in $F[x]$ have a greatest common divisor and a g.c.d. of $f(x), g(x) \in F[x]$ can be expressed in the form

$$a(x)f(x) + b(x)g(x)$$

for some $a(x), b(x)$ in $F[x]$. Since the polynomials

$$\prod_{j \neq i} f_j(x)^{e_j} \quad \text{and} \quad f_i(x)^{e_i}$$

are relatively coprime, it follows from the above observation that there exist polynomials $b_i(x) \in F[x]$ such that

$$b_i(x) \prod_{j \neq i} f_j(x)^{e_j} \equiv 1 (\bmod f_i(x)^{e_i})$$

Then

$$a_i(x)b_i(x) \prod_{j \neq i} f_j(x)^{e_j} \equiv a_i(x) (\bmod f_i(x)^{e_i})$$

and

$$a_i(x)b_i(x) \prod_{j \neq i} f_j(x)^{e_j} \equiv 0 (\bmod f_l(x)^{e_l}) \quad \text{for } l \neq i$$

Set

$$h(x) = \sum_i a_i(x)b_i(x) \prod_{j \neq i} f_j(x)^{e_j}$$

Then

$$h(x) \equiv a_i(x) (\bmod f_i(x)^{e_i}) \quad \forall i, 1 \leq i \leq k$$

For proving uniqueness, suppose that $H(x)$ is also a solution of the simultaneous congruences, i.e.

$$H(x) \equiv a_i(x) (\bmod f_i(x)^{e_i}) \quad \forall i, 1 \leq i \leq k$$

Then

$$H(x) - h(x) \equiv 0 (\bmod f_i(x)^{e_i}) \quad \forall i, 1 \leq i \leq k$$

Since no two of the irreducible polynomials $f_1(x), f_2(x), \ldots, f_k(x)$ are equal, it

follows that

$$H(x) - h(x) \equiv 0 (\text{mod} \prod f_i(x)^{e_i})$$

or

$$H(x) \equiv h(x) (\text{mod} \prod f_i(x)^{e_i})$$

Proof of Theorem 7.5
Suppose that

$$f(x) = \prod_{i=1}^{n} p_i(x)^{e_i}$$

where each $p_i(x)$ is an irreducible polynomial over $F = \text{GF}(q)$, each e_i is a positive integer and no two of $p_1(x), p_2(x), \ldots, p_n(x)$ are equal. A polynomial $g(x) \in F[x]$ is in the null space of $\mathbf{Q} - \mathbf{I}$ iff

$$f(x) | g(x)^q - g(x) = \prod_{a_i \in F} (g(x) - a_i)$$

But this is so iff each

$$p_i(x)^{e_i} | g(x) - a_i$$

for some $a_i \in F$. On the other hand, given any elements $a_1, a_2, \ldots, a_n \in F$, it follows from Theorem 7.6 that there exists a unique $g(x) (\text{mod} f(x))$ in $F[x]$ with

$$g(x) \equiv a_i (\text{mod} p_i(x)^{e_i}) \quad 1 \leq i \leq n$$

As each a_i has q choices, we can choose $a_1, \ldots, a_n$ in q^n ways and hence there are q^n elements $g(x)$ in $F[x]$ with

$$g(x)^q - g(x) \equiv 0 (\text{mod} f(x))$$

Thus the null space of $\mathbf{Q} - \mathbf{I}$ has q^n elements and, therefore, its dimension over F is n – the number of distinct irreducible factors of $f(x)$.

7.4 BERLEKAMP'S ALGORITHM – A SPECIAL CASE

As mentioned earlier, we are most of the time concerned with factorization of the polynomial $x^n - 1$. For such a polynomial, Berlekamp's algorithm takes a much simpler form as, in that case, we do not need to find the **Q**-matrix. In this case, as we can assume that g.c.d.$(n, q) = 1$, the **Q**-matrix $\mathbf{Q} = (\mathbf{Q}_{ij})$ has exactly one non-zero entry in every row and since for a given j there is exactly one i with

$$q(i-1) \equiv j (\text{mod} n)$$

there is exactly one non-zero entry in every column also. Moreover, this

non-zero entry is always 1. In fact

$$Q_{i+1,j+1} = 1 \quad \text{iff } qi \equiv j (\text{mod } n)$$

From this it follows that if $(g_0 \quad g_1 \quad \cdots \quad g_{n-1})$ is in the null space of $\mathbf{Q} - \mathbf{I}$ and $qi \equiv j (\text{mod } n)$, then $g_i = g_j$. As a consequence we have

$$g_j = g_i \quad \forall j \in C_i$$

where C_i is the cyclotomic class modulo n relative to q containing i. Set

$$\bar{C}_i = \sum_{j \in C_i} x^j$$

Then the result of Theorem 7.4 takes the form

$$x^n - 1 = \prod_{s \in F} [\text{g.c.d.}(x^n - 1, g(x) - s)]$$

where $g(x)$ is a linear combination of $\bar{C}_i$ over F.

Examples 7.4

Case (i)

First, let $p = 23$, and consider the cyclotomic cosets modulo p relative to 2:

$$C_0 = \{0\}$$
$$C_1 = \{1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12\}$$
$$C_5 = \{5, 10, 20, 17, 11, 22, 21, 19, 15, 7, 14\}$$

so $x^{23} - 1$ factors as a product of $x - 1$ and two irreducible polynomials of degree 11 each (Corollary of Theorem 7.3). To achieve this factorization we use the algorithm of Berlekamp. The irreducible factors are among the common divisors of $x^{23} - 1$ and

$$1 + a(x + x^2 + x^3 + x^4 + x^6 + x^8 + x^9 + x^{12} + x^{13} + x^{16} + x^{18}) + b(x^5 + x^7 + x^{10} + x^{11} + x^{14} + x^{15} + x^{17} + x^{19} + x^{20} + x^{21} + x^{22})$$

where $a, b \in \mathbb{B}$. We use the Euclidean algorithm to find the HCFs.

$$x^{18} + x^{16} + x^{13} + x^{12} + x^9 + x^8 + x^6 + x^4 + x^3 + x^2 + x + 1 \overline{)x^{23} + 1}$$

The 1st remainder is:

$$x^{21} + x^{18} + x^{17} + x^{14} + x^{13} + x^{11} + x^9 + x^8 + x^7 + x^6 + x^5 + 1$$

The 2nd remainder is:

$$x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^8 + x^4 + x^3 + 1$$

The 3rd remainder is:

$$x^{18}+x^{16}+x^{15}+x^{12}+x^{10}+x^9+x^8+x^7+x^5+x^2+x+1$$

The 4th remainder is:

$$x^{15}+x^{13}+x^{10}+x^7+x^6+x^5+x^4+x^3$$

$$x^{15}+x^{13}+x^{10}+x^7+x^6+x^5+x^4+x^3\overline{)x^{18}+x^{16}+x^{13}+x^{12}+x^9+x^8+x^6+x^4+x^3+x^2+x+1}$$

The 1st remainder is:

$$x^{12}+x^{10}+x^7+x^4+x^3+x^2+x+1$$

Thus the HCF is:

$$\begin{aligned}&x^{12}+x^{10}+x^7+x^4+x^3+x^2+x+1\\&=(x+1)\{x^{10}(x+1)+x^4(x^2+x+1)+x^2+1\}\\&=(x+1)(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1)\end{aligned}$$

To find the other irreducible factor of $x^{23}+1$ of degree 11, we divide $x^{23}+1$ by the HCF:

$$x^{12}+x^{10}+x^7+x^4+x^3+x^2+x+1\overline{)x^{23}+1}\qquad x^{11}+x^9+x^7+x^6+x^5+x+1$$

The 1st remainder is:

$$x^{21}+x^{18}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+1$$

The 2nd remainder is:

$$x^{19}+x^{18}+x^{16}+x^{15}+x^{14}+x^{10}+x^9+1$$

The 3rd remainder is:

$$x^{18}+x^{17}+x^{16}+x^{15}+x^{11}+x^8+x^7+1$$

The 4th remainder is:

$$x^{17}+x^{15}+x^{13}+x^{11}+x^{10}+x^9+x^6+1$$

The 5th remainder is:

$$x^{13}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+1$$

The 6th remainder is:

$$x^{12}+x^{10}+x^7+x^4+x^3+x^2+x+1$$

The 7th remainder is 0

Hence,

$$x^{23}+1=(x+1)(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1)$$
$$\times(x^{11}+x^9+x^7+x^6+x^5+x+1)$$

Case (ii)

Next we consider the factorization of $x^{11}-1$ over GF(3). The cyclotomic cosets modulo 11 are:

$$C_0=\{0\} \qquad C_1=\{1,3,9,5,4\} \qquad C_2=\{2,6,7,10,8\}$$

Therefore, $x^{11}-1$ factors as a product of $x-1$ and two irreducible factors of degree 5 each (Corollary of Theorem 7.3). The factors of $x^{11}-1$ are among the HCF of $x^{11}-1$ with

$$a+b(x+x^3+x^4+x^5+x^9)+c(x^2+x^6+x^7+x^8+x^{10})$$

where a, b, $c\in F_3=\mathrm{GF}(3)$. We apply Euclid's algorithm to the case $a=1=b, c=0$.

$$\begin{array}{r|l}
x^9+x^5+x^4+x^3+x+1 & x^{11}\qquad\qquad\qquad\qquad -1 \\
 & x^{11}+x^7+x^6+x^5+x^3+x^2 \\
\hline
 & -x^7-x^6-x^5-x^3-x^2-1
\end{array}$$

$$\begin{array}{r|l}
-x^7-x^6-x^5-x^3-x^2-1 & x^9\qquad\qquad +x^5+x^4+x^3\qquad +x+1 \\
 & x^9+x^8+x^7\qquad +x^5+x^4\qquad +x^2 \\
\hline
 & -x^8-x^7\qquad\qquad +x^3-x^2+x+1 \\
 & -x^8-x^7-x^6\qquad -x^4-x^3\qquad -x \\
\hline
 & x^6\qquad +x^4-x^3-x^2-x+1
\end{array}$$

$$\begin{array}{r|l}
x^6+x^4-x^3-x^2-x+1 & +x^7+x^6+x^5\qquad +x^3+x^2\qquad +1 \\
 & x^7\qquad +x^5-x^4-x^3-x^2+x \\
\hline
 & x^6\qquad +x^4-x^3-x^2-x+1
\end{array}$$

Thus one of the factors of $x^{11}-1$ is $x^6+x^4-x^3-x^2-x+1$. We find the