$$r(x) = (x^3+x^2)g(x) + 1 + x + x^4 + x^5.$$

$$s_0(x) = 1 + x + x^4 + x^5.$$

Since $w(s_0) > 3$ we compute $s_1(x) = 1 + x^3 + x^5$ and proceed. We list the syndromes in the following table.

i	$s_i(x)$
0	110011
1	100101
2	101110
3	010111
4	110111
5	100111
6	101111
7	101011
8	101001
9	101000

Since $s_9(x)$ is a burst of length 3 we determine the error pattern as $\mathbf{e} = (0000\ 0010\ 1000\ 000)$. We decode $\mathbf{r}$ to

$$\mathbf{r} - \mathbf{e} = (1110\ 1100\ 0100\ 000).$$

Note that $s_8(x)$ is a syndrome of weight 3, but not a burst of length 3 or less.

As one might imagine from the computations necessary in example 20, many of the better burst-error correcting codes have been found by computer search. The table below gives a few examples of binary cyclic codes with generator polynomial $g(x)$, capable of correcting all burst errors of length t or less, for some small values of t.

$g(x)$	(n,k)	Burst-correctability t
$1+x^2+x^3+x^4$	(7,3)	2
$1+x^2+x^4+x^5$	(15,10)	2
$1+x^4+x^5+x^6$	(31,25)	2
$1+x^3+x^4+x^5+x^6$	(15,9)	3
$1+x+x^2+x^3+x^6$	(15,9)	3

A very simple and effective technique for increasing the ability of a code to correct burst errors is known as *interleaving*. This technique is discussed in Chapter 7.

Analytic methods have also been used to find burst error codes. The analytically constructible class of codes known as the *Fire codes* have very high rate and can be used to provide excellent burst-error correcting capability.

5.8 Finite Fields and Factoring x^n-1 over GF(q)

Factoring x^n-1 over $GF(q)$ is extremely important in the study of cyclic codes. We devote this section to a discussion of this problem.

Let $GF(q)$ have characteristic p. If n and q are not coprime, then $n = \hat{n}p^s$ for some positive integer s, where $\gcd(\hat{n}, q) = 1$; then by Lemma 2.7, $x^n-1 = (x^{\hat{n}}-1)^{p^s}$. Hence we shall assume that $\gcd(n, q) = 1$.

Let m be the order of q modulo n, i.e. the smallest positive integer such that $q^m \equiv 1 \pmod n$. Then $q^m-1 = kn$ for some integer k. Consider the finite field $F = GF(q^m)$. From Lemma 2.4, we know that every element of F is a root of the polynomial $x^{q^m} - x$. Using the formula to sum a geometric series, note that

$$x^n + x^{2n} + \cdots + x^{kn} = \frac{x^n(x^{kn}-1)}{x^n-1}.$$

Hence x^n-1 divides $x^{kn}-1 = x^{q^m-1}-1$. It follows that x^n-1 has all of its roots in $F = GF(q^m)$, and that $GF(q^m)$ is the splitting field of x^n-1 over $GF(q)$ (see § 6.1).

If $\gamma \in F$ is a root of x^n-1, then $\gamma^n = 1$ and γ is called an n^{th} *root of unity*. Suppose α is a primitive element in F, so that α has order q^m-1. Then $\alpha^k = \alpha^{(q^m-1)/n}$ has order n and is a root of x^n-1; α^k is called a *primitive* n^{th} root of unity, since $(\alpha^k)^n = 1$ and $(\alpha^k)^j \neq 1$ for all positive $j < n$. We shall next require the following definition.

Definition. Given q and n, and a fixed integer i, $0 \le i \le n-1$, the *cyclotomic coset* (of q modulo n) containing i is defined to be

$$C_i = \{i, iq, iq^2, \ldots, iq^{s-1}\}$$

where the elements of the set are taken mod n, and s is the smallest integer such that $iq^s \equiv i \pmod n$. We call $C = \{C_i : 0 \le i \le n-1\}$ the *set of cyclotomic cosets* of q modulo n.

Example 22.

For $n = 9$ and $q = 2$,

$$C_1 = \{1,2,4,8,7,5\} = C_2 = C_4 = C_8 = C_7 = C_5$$

$$C_3 = \{3,6\} = C_6$$

$$C_0 = \{0\}$$

The set of cyclotomic cosets of 2 mod 9 is then $\mathrm{C} = \{C_0, C_1, C_3\}$.

Example 23.

Consider $n = 13$, $q = 3$. Then

$$C_1 = \{1,3,9\} = C_3 = C_9$$

$$C_2 = \{2,6,5\} = C_6 = C_5$$

$$C_4 = \{4,12,10\} = C_{10} = C_{12}$$

$$C_7 = \{7,8,11\} = C_8 = C_{11}$$

$$C_0 = \{0\}.$$

If we define a relation R on the integers by the rule $a\,R\,b$ if and only if for some integer j, $a \equiv bq^j \pmod n$, then for $\gcd(n,q) = 1$, it is easy to show that this relation is an equivalence relation on the integers modulo n, and the equivalence classes are the cyclotomic cosets of q mod n (exercise 49). Hence if $S, T \in \mathrm{C}$ and are distinct, then $S \cap T = \varnothing$ and $\bigcup_{S \in \mathrm{C}} S = Z_n$. We will shortly proceed to show that the number of irreducible factors of $f(x) = x^n - 1$ over $GF(q)$ is equal to the number of distinct cyclotomic cosets of q modulo n.

We first review some material regarding minimal polynomials, but now with respect to $GF(q)$ (as opposed to $GF(p)$, as in §2.4). The *minimal polynomial* of an element $\beta \in GF(q^m)$, *with respect to* $GF(q)$, is the monic polynomial $m(x) \in GF(q)[x]$ of smallest degree satisfying $m(\beta) = 0$. As in Theorem 2.8 and Theorem 2.9, this minimal polynomial is easily shown to be unique and irreducible (over $GF(q)$ now). For any $\beta \in GF(q^m)$, the *conjugates* of β, with respect to $GF(q)$, are the elements $\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{t-1}}$, where t is the smallest positive integer such that $\beta^{q^t} = \beta$. Analogous to the result of Theorem 2.11 then, such an element β has minimal polynomial with respect to $GF(q)$ being precisely

$$m_\beta(x) = \prod_{i=0}^{t-1} (x - \beta^{q^i}).$$

Let us now return to the problem of determining the factors of $x^n - 1$ over $GF(q)$. Again, let α be a primitive element for $GF(q^m)$, and let $q^m - 1 = kn$, so that α^k is a primitive n^{th} root of unity. First, we note that $x^n - 1$ has n distinct roots over $GF(q^m)$. This follows because $x^n - 1$ and its derivative nx^{n-1} (which is non-zero, since $\gcd(n,q) = 1$) have no factors in common (see exercise 50). Furthermore, these roots are precisely $(\alpha^k)^i$, $i = 0, 1, \ldots, n-1$. Now if $\beta = \alpha^{ki}$ is a root of $x^n - 1$, then $\beta^n = 1$ and each of the conjugates of β with respect to $GF(q)$, β^{q^j}, is also a root, since $(\beta^{q^j})^n = (\beta^n)^{q^j} = 1$. Hence $m_\beta(x)$ is a factor of $x^n - 1$. The roots of $m_\beta(x)$ are the elements

$$\alpha^{ki}, \alpha^{kiq}, \alpha^{kiq^2}, \ldots, \alpha^{kiq^{t-1}},$$

where t is the smallest positive integer such that $kiq^t \equiv ki \pmod{kn}$. This condition can be simplified to t being the smallest positive integer such that $iq^t \equiv i \pmod n$. It follows that the degree of $m_\beta(x)$ is the cardinality of the cyclotomic coset (of q mod n) containing i, $|C_i|$. Thus we can partition the set of roots of $x^n - 1$ into $|\,\mathrm{C}\,|$ classes, each class being the set of roots of an irreducible factor of $x^n - 1$. We summarize these observations in the following theorem.

Theorem 5.14. Let $f(x) = x^n - 1$ be a polynomial over $GF(q)$. The number of irreducible factors of $f(x)$ is equal to the number of cyclotomic cosets of q modulo n.

The procedure described above will, in fact, produce the factorization of $x^n - 1$ but it requires that we do computations in the extension field $GF(q^m)$. We illustrate the method by example here, and describe a more convenient technique in §5.9.

Example 24.

Suppose we wish to factor $f(x) = x^{15} - 1$ over $GF(2)$. Here n=15, q=2 and m=4. We first compute the cyclotomic cosets of 2 mod 15. These are

$$C_0 = \{0\}$$

$$C_1 = \{1,2,4,8\}$$

$$C_3 = \{3,6,12,9\}$$

$C_5 = \{5,10\}$

$C_7 = \{7,14,13,11\}$.

This tells us that $x^{15}-1$ factors as a linear term, an irreducible quadratic and 3 irreducible quartics. One way to find these quartics is to proceed as in our earlier discussion. We will make use of the field $GF(2^4)$ generated using the polynomial $1+x+x^4$ (see Appendix D). If α is a primitive element of $GF(2^4)$, then α is a primitive 15^{th} root of unity, and is a root of $x^{15}-1$. Hence α^2, α^4, and α^8 are also roots, and

$$m_\alpha(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)$$

is a factor of $f(x)$. Expanding $m_\alpha(x)$ we get

$$m_\alpha(x) = x^4 + (\alpha+\alpha^2+\alpha^4+\alpha^8)x^3 + (\alpha^3+\alpha^5+\alpha^9+\alpha^6+\alpha^{10}+\alpha^{12})x^2$$
$$+ (\alpha^7+\alpha^{11}+\alpha^{13}+\alpha^{14})x + \alpha^{15}.$$

Using the Zech's log table it is easy to evaluate

$$\alpha+\alpha^2+\alpha^4+\alpha^8 = \alpha(1+\alpha)+\alpha^4(1+\alpha^4) = \alpha^5+\alpha^5 = 0,$$
$$\alpha^3+\alpha^5+\alpha^9+\alpha^6+\alpha^{10}+\alpha^{12} = \alpha^3(1+\alpha^6)+(\alpha^5+\alpha^{10})+\alpha^6(1+\alpha^6)$$
$$= \alpha+1+\alpha^4 = 0,$$
$$\alpha^7+\alpha^{11}+\alpha^{13}+\alpha^{14} = \alpha^7(1+\alpha^4)+\alpha^{13}(1+\alpha) = \alpha^8+\alpha^2 = 1.$$

Hence $m_\alpha(x) = x^4+x+1$ (as expected). In a similar manner, we can evaluate $m_{\alpha^3}(x)$, $m_{\alpha^5}(x)$ and $m_{\alpha^7}(x)$ to get

$$x^{15}-1 = (x-1)(x^4+x+1)(x^4+x^3+1)(x^2+x+1)(x^4+x^3+x^2+x+1).$$

As an alternative to finding the minimal polynomial of an element $\beta \in GF(q^m)$ by expanding and then simplifying the polynomial obtained as the product of linear factors corresponding to the conjugates of β, note that given the vector representations of the elements of $GF(q^m)$ (as included in the Zech's log tables in Appendix D – e.g. $\alpha^4 = (1100)$), a less arduous approach is to seek the coefficients of the first linear dependence over $GF(q)$ of the powers β^i of β ($i \le m$). For example, to determine $m_{\alpha^7}(x)$, note

$$(\alpha^7)^0 = (1\,0\,0\,0)$$

$$(\alpha^7)^1 = (1\,1\,0\,1)$$
$$(\alpha^7)^2 = (1\,0\,0\,1)$$
$$(\alpha^7)^3 = (0\,0\,1\,1)$$
$$(\alpha^7)^4 = (1\,0\,1\,1)$$

from which it can be determined that

$$1\cdot(\alpha^7)^0 + 1\cdot(\alpha^7)^3 + 1\cdot(\alpha^7)^4 = 0.$$

Hence $m_{\alpha^7}(x) = 1+x^3+x^4$.

Example 25.

We factor x^9-1 over $GF(2)$. The cyclotomic cosets of 2 modulo 9 are

$C_0 = \{0\}$

$C_1 = \{1,2,4,8,7,5\}$

$C_3 = \{3,6\}$.

Hence x^9-1 factors as a linear term, a quadratic term and an irreducible of degree 6. We observe that

$$x^9-1 = (x^3)^3-1 = (x^3-1)(x^6+x^3+1)$$
$$= (x-1)(x^2+x+1)(x^6+x^3+1).$$

This must be the complete factorization.

Before proceeding with the next example, we make two observations regarding the reciprocal polynomial introduced in §5.4. Let $g(x) = \sum_{i=0}^{t} a_i x^i$ be a polynomial of degree exactly t in $F[x]$, and let $g_R(x) = x^t \cdot g(1/x)$. First, if α is a non-zero root of $g(x)$, then α^{-1} is a root of $g_R(x)$, since

$$g_R(\alpha^{-1}) = \sum_{i=0}^{t} a_{t-i}\alpha^{-i} = \alpha^{-t}\sum_{i=0}^{t} a_{t-i}\alpha^{t-i} = \alpha^{-t}g(\alpha) = 0.$$

Secondly, if $g(x)$ is irreducible, then so is $g_R(x)$. This follows since $g_R(x) = x^t \cdot g(1/x)$, and if $g_R(x) = a(x)b(x)$, then

$$g(x) = x^t \cdot a(1/x) \cdot b(1/x)$$

where $x^{\deg a(x)} \cdot a(1/x) \in F[x]$ and $x^{\deg b(x)} \cdot b(1/x) \in F[x]$.

Example 26.

We factor $x^{11}-1$ over $GF(3)$. The cyclotomic cosets of 3 modulo 11 are

$$C_0 = \{0\}$$

$$C_1 = \{1,3,9,5,4\}$$

$$C_2 = \{2,6,7,10,8\}.$$

Hence $x^{11}-1$ factors as a linear and 2 irreducible quintics over $GF(3)$. We could find these quintics by working in $GF(3^5)$ and proceeding by one of the methods illustrated in example 24; however, these approaches require construction of either a Zech's log table for $GF(3^5)$, or explicit construction of this 243-element field. We may also proceed in the following somewhat ad hoc fashion. If α is an n^{th} root of unity, then so is α^{-1}, since

$$1 = (\alpha^1\alpha^{-1})^n = \alpha^n\alpha^{-n} = \alpha^{-n}.$$

Hence if $m_\alpha(x)$ is a factor of $x^n - 1$, then so is $m_{\alpha^{-1}}(x)$. It now follows with the two observations above that the quintics we are looking for are reciprocal polynomials of each other. If one is

$$a(x) = a + bx + cx^2 + dx^3 + ex^4 + fx^5$$

then the other is

$$b(x) = f + ex + dx^2 + cx^3 + bx^4 + ax^5$$

or a scalar multiple of $b(x)$, say $\lambda b(x)$ where $\lambda = 1$ or -1. Since

$$a(x)\,\lambda b(x) = (x^{11}-1)/(x-1)$$

$$= x^{10} + x^9 + x^8 + \ldots + x^3 + x^2 + x + 1,$$

we get the following system of equations.

$$\lambda af = 1$$

$$\lambda(ae+bf) = 1$$

$$\lambda(ad+eb+fc) = 1$$

$$\lambda(ac+db+ec+df) = 1$$

$$\lambda(ab+cb+dc+ed+fe) = 1$$

$$\lambda(a^2+b^2+c^2+d^2+e^2+f^2) = 1.$$

We can assume without loss of generality that $a = 1$. If we suppose $\lambda = 1$, then $f = 1$ and the first 4 equations show that the only possible solutions are

e	b	d	c
0	1	0	1
1	0	1	0

Neither of these satisfy the remaining equations. Hence $\lambda = -1$ and $f = -1$. From this, we immediately deduce that e=0, b=1, d=1, c=2 is a solution and gives

$$a(x) = 2 + 2x + x^2 + 2x^3 + x^5$$

$$b(x) = 1 + 2x^2 + x^3 + 2x^4 + 2x^5$$

$$a(x)(-b(x)) = (x^{11}-1)/(x-1).$$

5.9 Another Method for Factoring x^n-1 over $GF(q)$†

In this section we present an alternate method for factoring $x^n - 1$. We require a few preliminary results. The *greatest common divisor* (gcd) of two polynomials is defined in a manner analogous to that for two integers. For polynomials $a(x), b(x) \in F[x]$, the greatest common divisor of $a(x)$ and $b(x)$ is defined to be the monic polynomial of largest degree in $F[x]$ which divides both $a(x)$ and $b(x)$. We use the notation $\gcd(a(x), b(x))$ or simply $(a(x),b(x))$.

The following result shall prove to be central to the factorization technique.

† This section may be omitted without loss of continuity.

Theorem 5.15. Let $f(x)$ be a monic polynomial of degree n over $F = GF(q)$. Let $g(x)$ be a polynomial over F with $\deg g(x) \le n-1$ and satisfying $[g(x)]^q \equiv g(x) \pmod{f(x)}$. Then

$$f(x) = \prod_{s \in F} \gcd(f(x), g(x)-s).$$

Proof.

Certainly $\gcd(f(x), g(x)-s)$ divides $f(x)$ for any $s \in F$. Now since $\gcd(a,b) = \gcd(a, b-a)$, $\gcd(g(x)-s, g(x)-t) = (g(x)-s, s-t) = 1$ for $s \ne t$. It follows that $\gcd(\gcd(f(x), g(x)-s), \gcd(f(x), g(x)-t)) = 1$ for $s \ne t$, and hence

$$\prod_{s \in F} \gcd(f(x), g(x)-s)$$

divides $f(x)$. By definition of $g(x)$, $f(x)$ divides $[g(x)]^q - g(x)$. Now note (using Lemma 2.4) that

$$y^q - y = \prod_{s \in F} (y-s)$$

over F. It follows that

$$[g(x)]^q - g(x) = \prod_{s \in F} (g(x)-s)$$

and $f(x)$ divides $\Pi_{s \in F}(g(x)-s)$. But this implies that $f(x)$ divides

$$\prod_{s \in F} \gcd(f(x), g(x)-s).$$

Since $f(x)$ and $\Pi_{s \in F} \gcd(f(x), g(x)-s)$ are both monic, we conclude

$$f(x) = \prod_{s \in F} \gcd(f(x), g(x)-s).$$

□

Example 27.

Consider q=2, n=7, $f(x) = x^7-1$ and $g(x) = x + x^2 + x^4$. Clearly $g^2(x) \equiv g(x) \pmod{f(x)}$. Using the Euclidean algorithm for polynomials (see Appendix B), it is easy to compute $\gcd(f(x), g(x)) = 1 + x + x^3$ and $\gcd(f(x), g(x)+1) = (1+x)(1+x^2+x^3)$, and to check that

$$\begin{aligned} f(x) &= \gcd(f(x), g(x)) \cdot \gcd(f(x), g(x)+1) \\ &= (1+x+x^3)(1+x)(1+x^2+x^3). \end{aligned}$$

We notice in Theorem 5.15 that if $g(x)$ has positive degree, then the factorization of $f(x)$ must be non-trivial. This follows since $\deg(f(x), g(x)-s) < n$ if $g(x)-s \ne 0$.

One question immediately comes to mind. How many polynomials $g(x)$ are there which satisfy $[g(x)]^q \equiv q(x) \pmod{f(x)}$?

Theorem 5.16. Let $f(x)$ be a polynomial over $F = GF(q)$ which has t distinct irreducible factors over F. Then there are exactly q^t polynomials $g(x)$ over F of degree less than n which satisfy $[g(x)]^q \equiv g(x) \pmod{f(x)}$.

Proof.

Let $f(x)$ have degree n, and let $f(x) = \Pi_{i=1}^t p_i^{\alpha_i}(x)$ be the complete factorization of $f(x)$ into powers of irreducible polynomials $p_i(x)$. Consider the simultaneous congruences

$$\begin{aligned} g(x) &\equiv s_1 \pmod{p_1^{\alpha_1}(x)} \\ g(x) &\equiv s_2 \pmod{p_2^{\alpha_2}(x)} \\ &\vdots \\ g(x) &\equiv s_t \pmod{p_t^{\alpha_t}(x)}, \end{aligned} \tag{1}$$

where $s_i \in F$, $1 \le i \le t$. By the *Chinese remainder theorem* (see Appendix C), there exists a unique polynomial $g(x)$ having degree less than n which satisfies this system for any choice of s_i's. Since we can select the s_i's in q^t distinct ways, there are q^t distinct polynomials $g(x)$ satisfying the system. From (1) we get that $f(x)$ divides $\Pi_{i=1}^t(g(x)-s_i)$, for any choice of the s_i, $1 \le i \le t$. Since the $p_i(x)$ are distinct irreducibles and hence coprime, each factor $g(x)-s_k$ in this product is needed at most once in order for $f(x)$ to be a divisor. Hence $f(x)$ divides $\Pi_{s \in F}(g(x)-s)$. But $\Pi_{s \in F}(g(x)-s) = [g(x)]^q - g(x)$. We conclude that

$$[g(x)]^q \equiv g(x) \pmod{f(x)}. \tag{2}$$

(Alternatively, since $g(x) \equiv s_i \pmod{p_i^{\alpha_i}(x)}$, it follows that

$$[g(x)]^q \equiv s_i^q \equiv s_i \equiv g(x) \pmod{p_i^{\alpha_i}(x)}$$

for all i, since $s_i \in F$. Then using the Chinese remainder theorem, (2) follows.)

We have established that there are at least q^t polynomials $g(x)$ with $\deg g(x) < n$ satisfying (2). The above arguments can be reversed to prove that any $g(x)$ satisfying (2) satisfies the system (1) for some choice of $s_1, s_2, \ldots, s_t$. Therefore, there are exactly q^t polynomials of the desired type. □

The set G of all polynomials $g(x)$ such that $g(x)$ satisfies (2) forms a subspace of $V_n(F)$. It follows from the preceding proof that this subspace has dimension t. This leads to the following result.

Theorem 5.17. Let $g_1(x), g_2(x), \ldots, g_t(x)$ be a basis for G. For $p_i^{\alpha_i}(x)$ and $p_j^{\alpha_j}(x)$ with $i \neq j$, there exists some integer k, $1 \le k \le t$, and distinct elements $s, t \in F$, such that $p_i^{\alpha_i}(x)$ divides $g_k(x)-s$ but not $g_k(x)-t$, and $p_j^{\alpha_j}(x)$ divides $g_k(x)-t$ but not $g_k(x)-s$.

Once this is established, we are then assured that application of Theorem 5.15 with $g_k(x)$, $1 \le k \le t$, will result in a complete factorization. This will become more clear with the example below. First, we give a proof of the result.

Proof.

Form the $t \times t$ matrix $M = [m_{ij}]$ where $g_j(x) \equiv m_{ij} \pmod{p_i^{\alpha_i}(x)}$. Theorem 5.15 guarantees that $m_{ij} \in F$. First we show that M is non-singular. Suppose there exist scalars λ_j such that $\sum_{j=1}^{t} \lambda_j m_{ij} = 0$ for each i, $1 \le i \le t$. Then

$$\sum_{j=1}^{t} \lambda_j m_{ij} \equiv \sum_{j=1}^{t} \lambda_j g_j(x) \pmod{p_i^{\alpha_i}(x)},$$

and so $\sum_{j=1}^{t} \lambda_j g_j(x) \equiv 0 \pmod{f(x)}$. But $\deg g_j(x) < \deg f(x)$ for each j, $1 \le j \le t$, and thus $\sum_{j=1}^{t} \lambda_j g_j(x) = 0$. Since the $g_j(x)$'s are linearly independent, it follows that $\lambda_j = 0$, $1 \le j \le t$, and thus the columns of M are linearly independent. In other words, M is non-singular. This implies that no two rows of M are identical. Thus for $i \neq j$, rows i and j differ in some column k, i.e. there is some k such that $m_{ik} \neq m_{jk}$. The result follows. □

Example 28.

Reconsider example 24 where we factor $f(x) = x^{15}-1$ over $GF(q)$ for $q=2$. The cyclotomic cosets are

$$C_0 = \{0\}$$

$$C_1 = \{1,2,4,8\}$$

$$C_3 = \{3,6,9,12\}$$

$$C_7 = \{7,11,13,14\}$$

$$C_5 = \{5,10\}.$$

Each coset corresponds to an irreducible factor of $f(x)$. This tells us that the subspace G contains 2^5 elements. In the special case where $f(x)$ has the form x^n-1, it is easy to find a basis for G. We use the cyclotomic cosets to form polynomials as follows.

$$g_1(x) = 1$$

$$g_2(x) = x^1 + x^2 + x^4 + x^8$$

$$g_3(x) = x^3 + x^6 + x^9 + x^{12}$$

$$g_4(x) = x^7 + x^{11} + x^{13} + x^{14}$$

$$g_5(x) = x^5 + x^{10}.$$

Now it is immediate that $g_i^2(x) \equiv g_i(x) \pmod{f(x)}$, $1 \le i \le 5$, since the powers of x with non-zero coefficients form a cyclotomic coset. It is also easy to see that the vectors associated with the $g_i(x)$'s are linearly independent, since each power of x in $g_i(x)$ is contained in none of the others. Thus we have a basis for G.

With this, we first compute

$$f(x) = \gcd(f(x), g_2(x)) \cdot \gcd(f(x), g_2(x)-1)$$
$$= (1+x+x^3+x^7)(1+x+x^2+x^4+x^8).$$

It suffices to compute $\gcd(f(x), g_2(x))$, since $\gcd(f(x), g_2(x)-1)$ can be found by dividing $f(x)$ by $(f(x), g_2(x))$. Let $a(x) = (1+x+x^3+x^7)$ and $b(x) = 1+x+x^2+x^4+x^8$. We now compute $\gcd(a(x), g_3(x))$ and $\gcd(b(x), g_3(x))$ to refine the factorization.

$$\gcd(a(x), g_3(x)) = 1 + x^3$$

$$\gcd(a(x), g_3(x)-1) = 1 + x + x^4$$

$$\gcd(b(x), g_3(x)) = 1$$

$$\gcd(b(x), g_3(x)-1) = 1 + x + x^2 + x^4 + x^8.$$

Thus

$$f(x) = (1+x^3)(1+x+x^4)(1+x+x^2+x^4+x^8).$$

We could now check $g_4(x)$ with each of these factors. But by inspection we note that $(1+x^3) = (1+x)(1+x+x^2)$ and $(1+x+x^4)$ is irreducible. Let

$$c(x) = 1 + x + x^2 + x^4 + x^8.$$

Then we need only consider $\gcd(c(x), g_4(x))$ and $\gcd(c(x), g_4(x)-1)$.

$$\gcd(c(x), g_4(x)) = 1 + x^3 + x^4$$

$$\gcd(c(x), g_4(x)-1) = 1 + x + x^2 + x^3 + x^4,$$

and we obtain

$$f(x) = (1+x)(1+x+x^2)(1+x^3+x^4)(1+x+x^4)(1+x+x^2+x^3+x^4).$$

Since we now have $f(x)$ as the product of 5 polynomials and we know that $f(x)$ has exactly 5 irreducible factors, we are sure that this is the complete factorization.

The preceding example illustrates a general method for factoring $f(x) = x^n-1$ over $GF(q)$. A basis for the subspace G can always be found from the cyclotomic cosets of q modulo n. Using the basis elements and appropriate gcd operations, the factors of $f(x)$ can be separated.

5.10 Exercises

Cyclic subspaces.

1. Verify that $g(x) = 1 + x^2 + x^3 + x^4$ is a monic divisor of $f(x) = x^7-1$ over $F=Z_2$, and construct the ideal generated by $g(x)$ in $F[x]/(f(x))$.
2. Determine the number of cyclic subspaces in each of the following vector spaces.

   (a) $V_8(Z_2)$ (b) $V_9(Z_2)$ (c) $V_{10}(Z_2)$ (d) $V_{15}(Z_2)$

   (e) $V_{18}(Z_2)$ (f) $V_3(Z_3)$ (g) $V_4(Z_3)$
3. Show that $V_{15}(Z_2)$ contains a cyclic subspace of dimension k for each k, $0 \le k \le 15$.
4. Consider the vector space $V_{17}(Z_2)$.

   (a) Determine the number of cyclic subspaces.

   (b) Determine all values of k, $1 \le k \le 17$, for which a cyclic subspace of dimension k exists.

   (c) Determine the number of these subspaces which have dimension 12.

   (d) Give a generator polynomial for a cyclic subspace of dimension 8, if possible.
5. Determine the number of cyclic subspaces of dimension 9 in $V_{21}(Z_2)$.
6. Determine the number of cyclic subspaces of dimension 5 in $V_8(Z_3)$. Give a generating polynomial for each one.
7. Let $g(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$ be a monic polynomial over F of least degree in some cyclic subspace of $V_n(F)$. Prove that $a_0 \ne 0$.
8. Let $g(x)$ and $h(x)$ be monic divisors of x^n-1 over F. Prove that if $g(x)$ divides $h(x)$, then the cyclic subspace generated by $g(x)$ contains the cyclic subspace generated by $h(x)$.
9. (a) Determine the number of cyclic subspaces in $V_6(Z_3)$.

   (b) Determine the generator polynomial and dimension of the smallest cyclic code containing the vector $\mathbf{v} = (112\ 110)$ in $V_6(Z_3)$.
10. (a) Determine the number of cyclic subspaces in $V_7(Z_2)$.

    (b) Determine the generator polynomial and the dimension of the smallest cyclic code containing each of the following vectors in $V_7(Z_2)$:

    (i) $\mathbf{v}_1 = (1010\ 011)$ (ii) $\mathbf{v}_2 = (0011\ 010)$ (iii) $\mathbf{v}_3 = (0101\ 001)$