other factor by actual division.

$$\begin{array}{r|r}
 & x^5 \qquad -x^3+x^2-x-1 \\
\hline
x^6+x^4-x^3-x^2-x+1 & x^{11} \qquad\qquad\qquad\qquad\qquad -1 \\
 & x^{11}+x^9-x^8-x^7-x^6-x^5 \qquad\qquad\qquad\quad \\
\cline{2-2}
 & -x^9+x^8+x^7+x^6-x^5 \qquad\qquad -1 \\
 & -x^9 \qquad -x^7+x^6+x^5+x^4-x^3 \qquad \\
\cline{2-2}
 & x^8-x^7 \qquad +x^5-x^4+x^3 \qquad -1 \\
 & x^8 \qquad +x^6-x^5-x^4-x^3+x^2 \quad \\
\cline{2-2}
 & -x^7-x^6-x^5 \qquad -x^3-x^2 \quad -1 \\
 & -x^7 \qquad -x^5+x^4+x^3+x^2-x \quad \\
\cline{2-2}
 & -x^6 \qquad -x^4+x^3+x^2+x-1 \\
 & -x^6 \qquad -x^4+x^3+x^2+x-1 \\
\cline{2-2}
 & 0 \\
\cline{2-2}
\end{array}$$

Hence

$$\begin{aligned}
x^{11}-1 &= (x^6+x^4-x^3-x^2-x+1)(x^5-x^3+x^2-x-1) \\
&= (x^6-x^5+x^5-x^4-x^4+x^3+x^3-x^2-x+1) \\
&\quad \times (x^5-x^3+x^2-x-1) \\
&= (x-1)(x^5+x^4-x^3+x^2-1)(x^5-x^3+x^2-x-1)
\end{aligned}$$

As the factorization of $x^{11}-1$ has to have two irreducible factors of degree 5 each, both the above polynomials of degree 5 are indeed irreducible.

Case (iii)

We next consider the factorization of $x^{13}-1$ over GF(3). Here the cyclotomic classes modulo 13 relative to 3 are:

$$C_0=\{0\} \qquad C_1=\{1,3,9\} \qquad C_2=\{2,6,5\} \qquad C_4=\{4,12,10\}$$
$$C_7=\{7,8,11\}$$

Therefore $x^{13}-1$ is a product of $x-1$ and four irreducible polynomials of degree 3 each (by Corollary to Theorem 7.3). The factors are given by the HCF of

$$x^{12}+x^{11}+\cdots+x+1$$

and

$$a+b(x+x^3+x^9)+c(x^2+x^5+x^6)+d(x^4+x^{10}+x^{12})+e(x^7+x^8+x^{11})$$

where a, b, c, d, $e\in\mathrm{GF}(3)$. We find these HCFs by Euclid's algorithm:

$$\begin{array}{r|l}
x^9+x^3+x-1 & x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1\\
& x^{12}+x^6+x^4-x^3\\ \cline{2-2}
& x^{11}+x^{10}+x^9+x^8+x^7+x^5-x^3+x^2+x+1\\
& x^{11}+x^5+x^3-x^2\\ \cline{2-2}
& x^{10}+x^9+x^8+x^7+x^3-x^2+x+1\\
& x^{10}+x^4+x^2-x\\ \cline{2-2}
& x^9+x^8+x^7-x^4+x^3+x^2-x+1\\
& x^9+x^3+x-1\\ \cline{2-2}
& x^8+x^7-x^4+x^2+x-1
\end{array}$$

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

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

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

$$\begin{array}{r l}
x^5 - x^4 + x^3 + x + 1 \big) & \overline{-x^6 \qquad\qquad\qquad + x^2 \quad + 1} \\
 & -x^6 + x^5 - x^4 \qquad - x^2 - x \\ \hline
 & \qquad -x^5 + x^4 \qquad - x^2 + x + 1 \\
 & \qquad -x^5 + x^4 - x^3 \qquad - x - 1 \\ \hline
 & \qquad\qquad\qquad x^3 - x^2 - x - 1 \\ \hline
\end{array}$$

$$\begin{array}{r l}
x^3 - x^2 - x - 1 \big) & \overline{x^5 - x^4 + x^3 \qquad + x + 1} \\
 & x^5 - x^4 - x^3 - x^2 \\ \hline
 & \qquad -x^3 + x^2 + x + 1 \\
 & \qquad -x^3 + x^2 + x + 1 \\ \hline
 & \qquad\qquad\qquad\qquad 0
\end{array}$$

$$\begin{array}{r l}
x^{12} + x^{10} + x^4 - 1 \big) & \overline{x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1} \\
 & x^{12} \qquad + x^{10} \qquad\qquad\qquad\qquad + x^4 \qquad\qquad - 1 \\ \hline
 & \qquad x^{11} \qquad + x^9 + x^8 + x^7 + x^6 + x^5 \qquad + x^3 + x^2 + x - 1
\end{array}$$

$$\begin{array}{r l}
x^{11}+x^9+x^8+x^7+x^6+x^5+x^3+x^2+x-1 \big) & \overline{x^{12}+x^{10} \qquad\qquad\qquad +x^4 \qquad\qquad -1} \\
 & x^{12}+x^{10}+x^9+x^8+x^7+x^6+x^4+x^3+x^2-x \\ \hline
 & \qquad\qquad -x^9-x^8-x^7-x^6 \qquad -x^3-x^2+x-1
\end{array}$$

$$\begin{array}{r l}
-x^9-x^8-x^7-x^6-x^3-x^2+x-1 \big) & \overline{x^{11} \qquad +x^9+x^8+x^7+x^6+x^5 \qquad +x^3+x^2+x-1} \\
 & x^{11}+x^{10}+x^9+x^8 \qquad\qquad +x^5+x^4-x^3+x^2 \\ \hline
 & \quad -x^{10} \qquad\quad +x^7+x^6 \quad -x^4-x^3 \qquad +x-1 \\
 & \quad -x^{10}-x^9-x^8-x^7 \qquad\quad -x^4-x^3+x^2-x \\ \hline
 & \qquad\quad x^9+x^8-x^7+x^6 \qquad\qquad -x^2-x-1 \\
 & \qquad\quad x^9+x^8+x^7+x^6 \qquad\quad +x^3+x^2-x+1 \\ \hline
 & \qquad\qquad\qquad x^7 \qquad\qquad -x^3+x^2 \quad +1
\end{array}$$

$$
\begin{array}{r l}
x^7 - x^3 + x^2 + 1 \big) & \overline{-x^9 - x^8 - x^7 - x^6 \qquad -x^3 - x^2 + x - 1} \\
& -x^9 \qquad\qquad +x^5 - x^4 \quad -x^2 \\
\cline{2-2}
& \quad -x^8 - x^7 - x^6 - x^5 + x^4 - x^3 \quad + x - 1 \\
& \quad -x^8 \qquad\qquad +x^4 - x^3 \quad -x \\
\cline{2-2}
& \qquad -x^7 - x^6 - x^5 \qquad\qquad -x - 1 \\
& \qquad -x^7 \qquad\qquad +x^3 - x^2 \quad -1 \\
\cline{2-2}
& \qquad\quad -x^6 - x^5 \quad -x^3 + x^2 - x
\end{array}
$$

$$
\begin{array}{r l}
-x^6 - x^5 - x^3 + x^2 - x \big) & \overline{x^7 \qquad\qquad -x^3 + x^2 \quad +1} \\
& x^7 + x^6 \quad +x^4 - x^3 + x^2 \\
\cline{2-2}
& \quad -x^6 \quad -x^4 \qquad\qquad +1 \\
& \quad -x^6 - x^5 \quad -x^3 + x^2 - x \\
\cline{2-2}
& \qquad\qquad x^5 - x^4 + x^3 - x^2 + x + 1
\end{array}
$$

$$
\begin{array}{r l}
x^5 - x^4 + x^3 - x^2 + x + 1 \big) & \overline{-x^6 - x^5 \quad -x^3 + x^2 - x} \\
& -x^6 + x^5 - x^4 + x^3 - x^2 - x \\
\cline{2-2}
& \qquad x^5 + x^4 + x^3 - x^2 \\
& \qquad x^5 - x^4 + x^3 - x^2 + x + 1 \\
\cline{2-2}
& \qquad\quad -x^4 \quad -x \quad -1
\end{array}
$$

$$
\begin{array}{r l}
-x^4 - x - 1 \big) & \overline{x^5 - x^4 + x^3 - x^2 + x + 1} \\
& x^5 \qquad\quad +x^2 + x \\
\cline{2-2}
& \quad -x^4 + x^3 + x^2 + 1 \\
& \quad -x^4 \qquad\quad -1 - x \\
\cline{2-2}
& \qquad\qquad x^3 + x^2 + x - 1
\end{array}
$$

$$
\begin{array}{r l}
-x^3 + x^2 + x - 1 \big) & \overline{-x^4 - x - 1} \\
& -x^4 + x - x^3 - x^2 \\
\cline{2-2}
& \quad x^3 + x^2 + x - 1 \\
& \quad x^3 + x^2 + x - 1 \\
\cline{2-2}
& \qquad\quad 0
\end{array}
$$

The two factors of $x^{13}-1$ we have obtained give the factor

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

We divide $x^{12}+x^{11}+\cdots+x+1$ by this factor:

$$\begin{array}{r|l}
 & x^6+x^5-x^4-x^2+x+1\\ \hline
x^6-x^4-x^3-x^2+1 & x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1\\
 & x^{12}\quad -x^{10}-x^9-x^8\quad +x^6\\ \cline{2-2}
 & x^{11}-x^{10}-x^9-x^8+x^7\quad +x^5+x^4+x^3+x^2+x+1\\
 & x^{11}\quad -x^9-x^8-x^7\quad +x^5\\ \cline{2-2}
 & -x^{10}\quad -x^7\quad +x^4+x^3+x^2+x+1\\
 & -x^{10}\quad +x^8+x^7+x^6\quad -x^4\\ \cline{2-2}
 & -x^8+x^7-x^6\quad -x^4+x^3+x^2+x+1\\ \cline{2-2}
 & -x^8+x^7-x^6\quad +x^3+x^2+x+1-x^4\\
 & -x^8\quad +x^6+x^5+x^4\quad -x^2\\ \cline{2-2}
 & x^7+x^6-x^5+x^4+x^3-x^2+x+1\\
 & x^7\quad -x^5-x^4-x^3\quad +x\\ \cline{2-2}
 & x^6\quad -x^4-x^3-x^2\quad +1\\
 & x^6\quad -x^4-x^3-x^2\quad +1\\ \cline{2-2}
 & 0
\end{array}$$

Next consider the case $c=1$, $a=-1$:

$$\begin{array}{r|l}
x^6+x^5+x^2-1 & x^6+x^5-x^4-x^2+x+1\\
 & x^6+x^5\quad +x^2\quad -1\\ \cline{2-2}
 & -x^4+x^2+x-1
\end{array}$$

$$
\begin{array}{r|rrrrrrr}
 & x^6 & +x^5 & & & +x^2 & & -1 \\
\cline{2-8}
-x^4+x^2+x-1 & x^6 & & -x^4 & -x^3 & +x^2 & & \\
\cline{2-8}
 & & x^5 & +x^4 & +x^3 & & & -1 \\
 & & x^5 & & -x^3 & -x^2 & +x & \\
\cline{2-8}
 & & & x^4 & -x^3 & +x^2 & -x & -1 \\
 & & & x^4 & & -x^2 & -x & +1 \\
\cline{2-8}
 & & & & -x^3 & -x^2 & & +1
\end{array}
$$

$$
\begin{array}{r|rrrrr}
 & -x^4 & & +x^2 & +x & -1 \\
\cline{2-6}
-x^3-x^2+1 & -x^4 & -x^3 & & +x & \\
\cline{2-6}
 & & x^3 & +x^2 & & -1 \\
 & & x^3 & +x^2 & & -1 \\
\cline{2-6}
 & & & & & 0 \\
\cline{2-6}
\end{array}
$$

Thus the 3rd irreducible factor of $x^{13}-1$ is x^3+x^2-1. To find the last irreducible factor of $x^{13}-1$, we divide $x^6+x^5-x^4-x^2+x+1$ by x^3+x^2-1:

$$
\begin{array}{r|rrrrrrr}
 & & & & x^3 & & -x & -1 \\
\cline{2-8}
x^3+x^2-1 & x^6 & +x^5 & -x^4 & & -x^2 & +x & +1 \\
 & x^6 & +x^5 & & -x^3 & & & \\
\cline{2-8}
 & & & -x^4 & +x^3 & -x^2 & +x & +1 \\
 & & & -x^4 & -x^3 & & +x & \\
\cline{2-8}
 & & & & -x^3 & -x^2 & & +1 \\
 & & & & -x^3 & -x^2 & & +1 \\
\cline{2-8}
 & & & & & & & 0 \\
\cline{2-8}
\end{array}
$$

Hence

$$x^{13}-1=(x-1)(x^3-x^2-x-1)(x^3+x^2+x-1)(x^3+x^2-1)(x^3-x-1)$$

(Also refer to Case (ii) in Examples 7.2 for an alternative method of factorization of this polynomial.)

We end this section and also the chapter with the following examples which we shall return to in the chapter on quadratic residue codes.

Case (iv)

We consider the polynomial $x^{11}-1$ over the field GF(5) of 5 elements. The cyclotomic cosets relative to 5 modulo 11 are:

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

Therefore $x^{11}-1$ has two irreducible factors of degree 5 each. To find these, we find the HCF of

$$x^9+x^5+x^4+x^3+x+1 \quad \text{and} \quad \sum_{0\le i\le 10} x^i$$

$$
\begin{array}{r}
x^9+x^5+x^4+x^3+x-1\,\big)\,\overline{x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1}\\
x^{10}\qquad\qquad\quad +x^6+x^5+x^4\qquad +x^2-x\quad\\
\hline
x^9+x^8+x^7\qquad\qquad\qquad +x^3\quad +2x+1\\
x^9\qquad\qquad +x^5+x^4+x^3\quad +\ x-1\\
\hline
x^8+x^7\quad -x^5-x^4\qquad\qquad +\ x+2
\end{array}
$$

$$
\begin{array}{r}
x^8+x^7-x^5-x^4+x+2\,\big)\,\overline{x^9+x^5+x^4+x^3+x-1}\\
x^9+x^8\quad -x^6\ \ -x^5+x^2+2x\\
\hline
-x^8\quad +x^6+2x^5+x^4+x^3-x^2-x-1\\
-x^8-x^7\quad +\ x^5+x^4\qquad\qquad -x-2\\
\hline
x^7+x^6+x^5\qquad +x^3-x^2\quad +1
\end{array}
$$

$$
\begin{array}{r}
x^7+x^6+x^5+x^3-x^2+1\,\big)\,\overline{x^8+x^7\quad -x^5-\ x^4\quad +x+2}\\
x^8+x^7+x^6\quad +\ x^4-x^3+x\\
\hline
-x^6-x^5-2x^4+x^3\quad +2
\end{array}
$$

$$
\begin{array}{r}
-x^6-x^5-2x^4+x^3+2\,\big)\,\overline{\ x^7+x^6+x^5+x^3-x^2+1}\\
+x^7+x^6+2x^5-x^4-2x\\
\hline
-x^5+x^4+x^3-x^2+2x+1\\
\hline
\end{array}
$$

$$\begin{array}{r|r} -x^5+x^4+x^3-x^2+2x+1 & -x^6-x^5-2x^4+x^3+2 \\ & -x^6+x^5+\ x^4-x^3+2x^2+x \\ \cline{2-2} & -2x^5-3x^4+2x^3-2x^2-\ \ x+2 \\ & -2x^5+2x^4+2x^3-2x^2+4x+2 \\ \cline{2-2} & 0 \end{array}$$

The HCF $f(x)=x^5-x^4-x^3+x^2-2x-1$ is one of the irreducible factors of degree 5 of $x^{11}-1$. The process of division gives the other factor as

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

Hence

$$x^{11}-1=(x-1)f(x)g(x)$$

Case (v)

We now consider the polynomial $x^{37}-1$ over the field GF(3) of 3 elements.

The cyclotomic cosets relative to 3 modulo 37 are:

$$C_0=\{0\}$$

$$C_1=\{1,3,9,27,7,21,26,4,12,36,34,28,10,30,16,11,33,25\}$$

$$C_2=\{2, 6, 18, 17, 14, 5, 15, 8, 24, 35, 31, 19, 20, 23, 32, 29, 13, 22\}$$

Thus $x^{37}-1$ factors into three irreducible factors one of which is $x-1$ and the other two are of degree 18 each. These factors are obtained as common factors of $x^{37}-1$ with $g(x)-s$ for some $s\in\text{GF}(3)$ where

$$g(x)=\sum_{k\in C_1} x^k \quad \text{or} \quad g(x)=\sum_{k\in C_2} x^k$$

Using Euclid's division algorithm, we obtain these common factors and find that

$$x^{37}-1=(x-1)f(x)g(x)$$

where

$$f(x)=x^{18}+x^{17}-x^{16}-x^{15}+x^{14}-x^{13}-x^{12}-x^{10}-x^9-x^8-x^6$$
$$-x^5+x^4-x^3-x^2+x+1$$

$$g(x)=x^{18}-x^{16}-x^{14}-x^{13}+x^{11}+x^7-x^5-x^4-x^2+1$$

Case (vi)

Again consider the polynomial $x^{61}-1$ over GF(3). The cyclotomic cosets relative to 3 modulo 61 are:

$$\begin{aligned}
C_0 &= \{0\}\\
C_1 &= \{1,3,9,27,20,60,58,52,34,41\}\\
C_2 &= \{2,6,18,54,40,59,55,43,7,21\}\\
C_4 &= \{4,12,36,47,19,57,49,25,14,42\}\\
C_5 &= \{5,15,45,13,39,56,46,16,48,22\}\\
C_8 &= \{8,24,11,33,38,53,37,50,28,23\}\\
C_{10} &= \{10,30,29,26,17,51,31,32,35,44\}
\end{aligned}$$

It follows that $x^{61}-1$ factors as a product of 7 irreducible polynomials over GF(3) one of which is $x-1$ and every other is of degree 10 each.

We use the algorithm of Berlekamp to find the factorization of $x^{61}-1$. Calculating the HCF of

$$1+\sum_{i\in C_8} x^i \quad \text{and} \quad x^{61}-1$$

gives a factor

$$\begin{aligned}
f(x) = x^{20}&-x^{19}-x^{18}+x^{17}-x^{16}+x^{14}-x^{13}-x^{12}+x^{11}\\
&+x^9-x^8-x^7+x^6-x^4+x^3-x^2-x+1
\end{aligned}$$

of $x^{61}-1$. Then finding the HCF of

$$\frac{(x^{61}-1)}{f(x)} \quad \text{and} \quad 1+\sum_{i\in C_{10}} x^i$$

gives another factor of $x^{61}-1$ as:

$$\begin{aligned}
g(x) = x^{20}&+x^{18}+x^{16}+x^{15}+x^{14}-x^{11}-x^{10}-x^9\\
&+x^6+x^5+x^4+x^2+1
\end{aligned}$$

Then the third factor of degree 20 is obtained by actual process of division as

$$\begin{aligned}
h(x) = x^{20}&-x^{19}+x^{17}-x^{15}-x^{14}-x^{13}+x^{12}-x^{11}-x^{10}-x^9+x^8\\
&-x^7-x^6-x^5+x^3-x+1
\end{aligned}$$

We next need to factorize $f(x)$, $g(x)$ and $h(x)$.

To factorize $f(x)$, we have to find a square matrix of order 20 in which the ith row is represented by $x^{3(i-1)}$ reduced modulo $f(x)$. Let this matrix be called

$\mathbf{Q}_1$. Then

$$\mathbf{Q}_1-\mathbf{I}=\left(\begin{array}{cccccccccccccccccccc}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&-1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&-1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&-1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&-1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&-1&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&-1&0&0&0&0&0&0&0&0&0&0&0&1&0\\
-1&0&-1&0&0&1&-1&-1&-1&0&-1&-1&0&-1&0&-1&1&0&0&-1\\
-1&-1&1&-1&1&-1&1&-1&1&-1&0&-1&-1&0&-1&0&1&1&0&1\\
1&0&-1&1&1&1&-1&1&1&-1&-1&1&-1&-1&1&-1&0&-1&-1&0\\
-1&-1&0&-1&-1&1&0&0&1&0&1&0&-1&-1&-1&0&0&-1&1&0\\
0&-1&1&0&1&1&-1&1&-1&1&-1&0&-1&0&1&1&-1&0&-1&1\\
-1&1&0&0&1&0&0&1&1&-1&1&0&1&1&1&0&0&0&0&1\\
-1&-1&1&-1&-1&0&1&0&1&0&-1&1&1&-1&0&-1&1&-1&1&1\\
1&0&0&0&0&-1&1&-1&0&-1&-1&1&0&-1&1&0&1&0&0&1\\
1&1&-1&1&-1&0&-1&1&1&1&-1&0&0&1&1&-1&0&1&-1&0\\
0&1&-1&0&-1&1&1&0&-1&1&-1&1&-1&1&-1&1&0&0&1&-1\\
1&-1&0&0&-1&0&0&1&1&1&-1&1&0&-1&1&1&1&-1&-1&1\\
-1&1&0&1&1&-1&0&0&0&0&-1&-1&-1&-1&1&1&-1&0&-1&1\\
1&1&-1&-1&0&0&0&-1&1&0&0&0&1&1&-1&-1&0&0&0&0
\end{array}\right)$$

If $(g_1 \;\cdots\; g_{20})$ is a row vector over GF(3) which is in the null space of $\mathbf{Q}_1-\mathbf{I}$, we obtain 20 equations in the g_i which finally lead to the relations

$$\begin{aligned}
&g_3=g_4=g_5=g_6=g_7=g_9=g_{10}=g_{13}=g_{14}=g_{17}=0\\
&g_2=-g_8=-g_{11}=g_{12}=g_{15}=g_{16}=-g_{18}=g_{19}=g_{20}
\end{aligned}\qquad(7.6)$$

Calculating the HCF of $f(x)$ and

$$x^{19}+x^{18}-x^{17}+x^{15}+x^{14}+x^{11}-x^{10}-x^7+x$$

gives one irreducible factor of $f(x)$ as

$$f_1(x)=x^{10}+x^9-x^8-x^7-x^6-x^4-x^3-x^2+x+1$$

and by the actual process of division the other factor is

$$f_2(x)=x^{10}+x^9-x^8+x^7-x^6-x^5-x^4+x^3-x^2+x+1$$

If $\mathbf{Q}_2$ denotes the $\mathbf{Q}$-matrix for the factorization of $h(x)$, then

$$\mathbf{Q}_2-\mathbf{I}=\left(\begin{array}{cccccccccccccccccccc}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&-1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&-1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&-1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&-1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&-1&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&-1&0&0&0&0&0&0&0&0&0&0&0&1&0\\
-1&0&1&-1&-1&1&-1&1&0&0&-1&-1&0&0&-1&-1&1&-1&-1&1\\
1&-1&-1&1&0&-1&1&-1&-1&-1&0&0&-1&-1&0&0&1&1&-1&-1\\
1&1&-1&1&1&-1&1&-1&0&0&0&-1&0&0&1&1&-1&0&-1&1\\
0&0&-1&-1&1&1&1&-1&0&-1&0&1&-1&1&1&1&1&-1&1&1\\
-1&-1&1&0&1&-1&-1&-1&0&1&1&0&1&1&0&0&1&1&-1&1\\
-1&1&-1&-1&-1&1&1&0&-1&1&-1&-1&0&0&1&0&-1&0&0&1\\
-1&0&0&-1&0&-1&1&-1&-1&-1&1&-1&-1&-1&0&1&-1&1&-1&-1\\
1&1&-1&-1&-1&0&-1&-1&0&1&0&1&0&1&-1&1&0&0&0&-1\\
1&0&0&1&-1&-1&0&-1&-1&1&1&0&0&-1&0&-1&-1&0&-1&0\\
1&0&-1&-1&1&-1&-1&0&-1&0&0&0&1&1&1&1&0&1&1&1\\
0&1&1&-1&1&1&1&1&-1&1&1&-1&0&-1&1&1&1&1&-1&0\\
-1&-1&-1&-1&-1&-1&-1&1&-1&0&1&-1&-1&0&-1&0&1&0&1&-1\\
-1&0&-1&0&1&1&1&0&1&1&1&0&-1&0&-1&0&0&0&-1&-1
\end{array}\right)$$

Again, if $(g_1 \quad \cdots \quad g_{20})$ is a row vector over GF(3) which is in the null space of $\mathbf{Q}_2 - \mathbf{I}$, we obtain certain equations in the g_i which finally lead to the relations

$$\begin{aligned} g_2 &= -g_3 = -g_5 = -g_6 = -g_7 = g_9 = -g_{11} = -g_{12} \\ &= g_{13} = g_{14} = g_{17} = g_{20} \end{aligned}$$

$$g_4 = g_8 = g_{10} = g_{15} = g_{16} = g_{18} = g_{19} = 0$$

Calculating the HCF of

$$x^{19} + x^{16} + x^{13} + x^{12} - x^{11} - x^{10} + x^8 - x^6 - x^5 - x^4 - x^2 + x + 1$$

and $h(x)$, gives one irreducible factor of $h(x)$ as

$$h_1(x) = x^{10} - x^9 + x^8 - x^7 + x^5 - x^3 + x^2 - x + 1$$

Then, by the process of actual division we obtain the other irreducible factor of $h(x)$ as

$$h_2(x) = x^{10} - x^8 + x^7 - x^6 + x^5 - x^4 + x^3 - x^2 + 1$$

Let

$$F = \mathrm{GF}(3)[x]/\langle h_2(x)\rangle$$

where $\langle h_2(x)\rangle$ denotes the ideal of GF(3)[x] generated by $h_2(x)$. Let

$$\alpha = x + \langle h_2(x)\rangle$$

Then α is a 61st root of unity in F. The elements α, α^4 being in different cyclotomic cosets, these have distinct minimal polynomials. Also α^4 does not satisfy $f_1(x)$, $f_2(x)$ or $h_1(x)$. Therefore, the minimal polynomial of α^4 has to be an irreducible factor of $g(x)$.

Let s_n denote the symmetric polynomial of $\{c^i \mid i \in C_4\}$ taken n elements at a time. We find that $s_1 = s_9$, $s_2 = s_8$, $s_3 = s_7$, $s_4 = s_6$. A process of direct calculations shows that

$$s_1 = s_4 = 0 \qquad s_2 = s_3 = 1$$

and then

$$\alpha^{40} + \alpha^{32} - \alpha^{28} - \alpha^{20} + \alpha^{12} + \alpha^8 + 1 = 0$$

It thus follows that the minimal polynomial of α^4 is

$$g_1(x) = x^{10} + x^8 - x^7 - x^5 - x^3 + x^2 + 1$$

Dividing $g(x)$ by $g_1(x)$ gives the other factor of $g(x)$ as

$$g_2(x) = x^{10} + x^7 + x^6 + x^5 + x^4 + x^3 + 1$$

We have thus obtained the factorization

$$x^{61} - 1 = (x-1)f_1(x)f_2(x)g_1(x)g_2(x)h_1(x)h_2(x)$$

of $x^{61} - 1$ as a product of irreducible factors over GF(3).