Berlekamp's algorithm for finding the distinct monic irreducible factor's of a monic polynomial.

$f = X^5 - X^4 + X^3 - X^2 + X + 1 \in \mathbb{Z}_3[X]$

$f' = 5X^4 - 4X^3 + 3X^2 - 2X + 1$

$= 2X^4 - X^3 - 2X + 1$

$= -X^4 - X^3 + X + 1$

We compute $\gcd(f, f')$ in order to check if f is square free

$$
\begin{array}{l|l}
X^5 - X^4 + X^3 - X^2 + X + 1 & -X^4 - X^3 + X + 1 \\
\cline{2-2}
-X^5 - X^4 \qquad + X^2 + X & X + 1 \\
\cline{1-1}
/ \quad X^4 + X^3 \cancel{-X} + 1 & \\
\quad -X^4 - X^3 + X + 1 & \\
\cline{1-1}
\qquad \qquad \boxed{2} &
\end{array}
$$

$\Rightarrow f = f' \cdot (X+1) + 2 \Rightarrow \gcd(f, f') = 1 \Rightarrow$

$\Rightarrow f$ is square free

We compute the matrix $Q = (q_{ik}) \in M_5(\mathbb{Z}_3)$ with elements: $X^{3k} = \sum_{i=0}^{4} q_{ik} X^i \pmod f$, $k = \overline{0,4}$

$V = \mathbb{Z}_3[X]/(f) = \{ a_0 + a_1 X + \dots + a_4 X^4 \mid a_0 .. a_4 \in \mathbb{Z}_3 \}$

$B = (1, X, X^2, X^3, X^4)$ is a basis

$X^{3\cdot 0}, X^{3\cdot 1} \in B$

$$\Rightarrow 1 = 1\cdot 1 + 0\cdot X + 0\cdot X^2 + 0\cdot X^3 + 0\cdot X^4$$
$$X^3 = 0\cdot 1 + 0\cdot X + 0\cdot X^2 + 1\cdot X^3 + 0\cdot X^4$$

The other powers are computed by getting $X^{3k} \bmod f$

$$\begin{array}{l|l}
X^6 & X^5 - X^4 + X^3 - X^2 + X + 1 \\ \hline
-X^6 + X^5 - X^4 + X^3 - X^2 - X & -X - 1 \\ \hline
/\ X^5 - X^4 + X^3 - X^2 - X & \\
-X^5 + X^4 - X^3 + X^2 \cancel{+X} - 1 & \\ \hline
\boxed{-2X - 1} &
\end{array}$$

$$\begin{array}{l|l}
X^9 & X^5 - X^4 + X^3 - X^2 + X + 1 \\ \hline
-X^9 + X^8 - X^7 + X^6 - X^5 - X^4 & -X^4 - X^3 \\ \hline
/\ X^8 - X^7 + X^6 - X^5 - X^4 & \\
-X^8 + X^7 - X^6 - X^5 - X^4 - X^3 & \\ \hline
/\ /\ /\ /\ \boxed{-2X^4 - X^3} &
\end{array}$$

$$X^{12} \quad \Big| \; X^5 - X^4 + X^3 - X^2 + X + 1$$

$$-X^{12} + X^{11} - X^{10} + X^9 - X^8 - X^7 \quad \Big| \; X^7 - X^6 + 2X^2 + 3X + 1$$

$$/ \quad X^{11} - X^{10} + X^9 - X^8 - X^7$$

$$-X^{11} + X^{10} - X^9 + X^8 - X^7 - X^6$$

$$/ \quad / \quad / \quad / \quad -2X^7 - X^6$$

$$2X^7 - 2X^6 + 2X^5 - 2X^4 + 2X^3 + 2X^2$$

$$/ \quad -3X^6 + 2X^5 - 2X^4 + 2X^3 + 2X^2$$

$$3X^6 - 3X^5 + 3X^4 - 3X^3 + 3X^2 + 3X$$

$$/ \quad -X^5 + X^4 - X^3 + 5X^2 + 3X$$

$$X^5 - X^4 + X^3 - X^2 + X + 1$$

$$/ \quad / \quad / \quad \boxed{4X^2 + 4X + 1}$$

So, we have

$X^6 \bmod f = -2X - 1 = X - 1$

$X^9 \bmod f = -2X^4 - X^3 = X^4 - X^3$

$X^{12} \bmod f = 4X^2 + 4X + 1 = X^2 + X + 1$

Now, in order to get Q, we place the coefficents of these as columns in Q.

$$\Rightarrow Q = \begin{pmatrix} 1 & 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Let $\varphi: V \to V$, $\varphi(h) = h^2 - h \pmod f$, so φ is a linear map and $[\varphi]_B = Q - I_5$

The number of irreducible factors of f is

$$r = \dim \ker \varphi = n - \operatorname{rank}(Q - I_5)$$

We compute the rank of an echelon form of $Q - I_5$

$$Q - I_5 = \begin{pmatrix} 0 & 0 & -1 & 0 & 1 \\ 0 & -1 & 1 & 0 & 1 \\ 0 & 0 & -1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix} \overset{r_1 \leftrightarrow r_2}{\sim} \begin{pmatrix} 0 & -1 & 1 & 0 & 1 \\ 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix} \overset{r_1 \cdot (-1)}{\sim} \begin{pmatrix} 0 & 1 & -1 & 0 & -1 \\ 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix} \overset{-r_1+r_4}{\sim}$$

$$\begin{pmatrix} 0 & 1 & -1 & 0 & -1 \\ 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix} \overset{-r_2+r_3}{\sim} \begin{pmatrix} 0 & 1 & -1 & 0 & -1 \\ 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix} \overset{r_2+r_4}{\sim} \begin{pmatrix} 0 & 1 & -1 & 0 & -1 \\ 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix} \overset{r_3 \leftrightarrow r_4}{\sim}$$

$$\begin{pmatrix} 0 & 1 & -1 & 0 & -1 \\ 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix} \overset{-r_2+r_1}{\sim} \begin{pmatrix} 0 & 1 & -1 & 0 & -1 \\ 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \underset{\substack{\shortparallel \\ 0}}{-3} \end{pmatrix} (\mathbb{Z}_3)$$

$\Rightarrow \operatorname{rank}(Q - I_5) = 3$ (non-zero rows)

$\Rightarrow$ The number of factors $r = n - 3 \Leftrightarrow 5 - 3 = 2$ factors

$\dim V = \deg(f) = 5 \Rightarrow V \cong \mathbb{Z}_3^5$

We identify φ with $\psi^n : \mathbb{Z}_3^5 \to \mathbb{Z}_3^5$ and determine a basis of $\ker \psi = \{a \in \mathbb{Z}_3^5 \mid \psi(a) = 0\}$

$\Leftrightarrow \ker \psi = \{a = (a_0, \dots a_n) \in \mathbb{Z}_3^5 \mid (Q - I_5)[a] = [0]\}$

$\Rightarrow$ the system
$$\begin{cases} -a_2 + a_4 = 0 & \Rightarrow a_2 = a_4 \\ -a_1 + a_2 + a_4 = 0 & \Rightarrow a_1 = 2a_2 = -a_2 \\ -a_2 + a_4 = 0 & \Rightarrow a_4 = a_2 \\ a_1 + a_3 = 0 & \Rightarrow a_1 = -a_3 = a_2 \\ a_3 - a_4 = 0 & \Rightarrow a_3 = a_4 \text{ ; } a_0 \in \mathbb{Z}_3 \end{cases}$$
as solution

In other words, we get this system from the rows of $Q - I_5$ and put the row as coefficients for $a_0 \dots a_n$.

$\Rightarrow \ker \psi = \{(a_0, -a_2, a_2, a_2, a_2) \mid a_0, a_2 \in \mathbb{Z}_3\}$
$= \langle (1,0,0,0,0), (0,-1,1,1,1) \rangle$

$\Rightarrow$ We have a basis of two generators with the associated polynomials $\begin{cases} h_1 = 1 \\ h_2 = -X + X^2 + X^3 + X^4 \end{cases}$

To get the non-trivial factor we compute $\gcd(f, h_2)$

$$x^5-x^4+x^3-x^2+x+1 \;\Big|\; \underline{x^4+x^3+x^2-x}$$
$$-x^5-x^4-x^3+x^2 \qquad\qquad -x-1$$
$$\overline{\;/ \quad -2x^4+x+1 \iff}$$
$$\iff x^4+x+1$$
$$-x^4-x^3-x^2+x$$
$$\overline{\;/ \; -x^3-x^2+2x+1 \iff}$$
$$\iff -x^3-x^2-x+1$$

since we are in $\mathbb{Z}_3$ we can write $-2=1$ and $2=-1$

1

$$x^4+x^3+x^2-x \;\Big|\; \underline{-x^3-x^2-x+1}$$
$$-x^4-x^3-x^2+x \qquad\qquad x$$
$$\overline{\;/ \quad / \quad / \quad /\;}$$

$\Rightarrow$ a factor of f is $-x^3-x^2-x+1$

To get the other factor we will just divide f with the first found factor since we only have two factors.

$$x^5-x^4+x^3-x^2+x+1 \;\Big|\; \underline{-x^3-x^2-x+1}$$
$$-x^5-x^4-x^3+x^2 \qquad\qquad x^2+x-1$$
$$\overline{\;/ \; -2x^4+x+1}$$
$$x^4+x+1$$
$$-x^4-x^3-x^2+x$$
$$\overline{-x^3-x^2+2x+1 \iff}$$
$$\iff -x^3-x^2-x+1$$
$$x^3+x^2+x-1$$
$$\overline{\;/ \quad / \quad / \quad /\;}$$

2

$\Rightarrow \boxed{x^2+x-1}$ is the second factor

In conclusion, we have

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