Name: Moldovan Vasilica
Group: 935
mvie2572

Factorization of polynomial using Berlekamp's algorithm

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

We have $g' = 2X^4+2X^3+X+2 = -X^4-X^3+X-1$

To see if g is square-free, we need to compute (g, g'). For this, we will use the Euclidean algorithm.

First, we divide g by g'.

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

Then, we divide g' to the remainder of the division above.

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

$$
\begin{array}{l|l}
X^3+2X+1 & -X^2-2 \\
\hline
-X^3-2X & -X \\
\hline
/ \quad / \quad 1 &
\end{array}
$$

Since the remainder is $1 \Rightarrow (g, g') = 1 \Rightarrow g$ is square-free.

Let $f = g \in \mathbb{Z}_3[X]$.

We need to determine the matrix $Q = (q_{ik}) \in M_5(\mathbb{Z}_3)$, with q_{ik}'s given by:

$$X^{3k} = \sum_{i=0}^{4} q_{ik} X^i \pmod{f}, \quad k = 0, \dots, 4.$$

For $\mathbb{Z}_3$-vector space: $V=\mathbb{Z}_3[X]/(f)=\{a_0+a_1X+a_2X^2+a_3X^3+a_4X^4 \mid a_0,\dots,a_4\in\mathbb{Z}_3\}$

One of its bases is the list of vectors $B=(1,X,\dots,X^4)$.

For $k\in\{0,\dots,4\}$, q_{jk} are the coordinates of the vector X^{3k} in B. Since 1 and X^3 belong to B, we have:

$\cancel{1=1\cdot 0}$

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

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

The next powers are obtained by computing X^{3k} mod f.

$X^{3\cdot 2}=X^6$

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

$X^{3\cdot 3}=X^9$

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

$X^{3\cdot 4}=X^{12}$

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

Then,

$$X^6 = 1-X-X^2-X^3-X^4 \pmod{f}$$

$$X^9 = 2+2X^2+X^4 \overset{(1)}{=} -1-X^2+X^4 \pmod{f}$$

$$\cancel{X^{12} = 2+2X^2+X^4}$$

$$X^{12} = -2-X-X^3 \underset{(2)}{=} 1-X-X^3 \pmod{f}$$

In (1) and (2) we replaced 2 by -1 and -2 by 1, due to the fact that the coefficients are in $\mathbb{Z}_3$.

Hence, we get the matrix:

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

Let $\varphi : V \to V$, $\varphi(h) = h^3 - h \pmod{f}$. Then φ is a linear map and $[\varphi]_B = Q - I_5$. Then, $r = \dim \operatorname{Ker} \varphi = n - \operatorname{rank}(Q - I_5)$ is the number of irreducible factors of f. In order to compute r, we will compute $\operatorname{rank}(Q - I_5)$ from an echelon form of $Q - I_5$.

$$Q - i_5 = \begin{pmatrix} 0 & 0 & 1 & -1 & 1 \\ 0 & -1 & -1 & 0 & -1 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 1 & -1 & -1 & -1 \\ 0 & 0 & -1 & 1 & -1 \end{pmatrix} \underset{R_5 += R_1}{\sim} \begin{pmatrix} 0 & 0 & 1 & -1 & 1 \\ 0 & -1 & -1 & 0 & -1 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 1 & -1 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \underset{R_3 += R_2}{\sim} \begin{pmatrix} 0 & 0 & 1 & -1 & 1 \\ 0 & -1 & -1 & 0 & -1 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & -2 & -1 & -2 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \sim$$

$$\begin{pmatrix} 0 & 0 & 1 & -1 & 1 \\ 0 & -1 & -1 & 0 & -1 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \underset{R_3 += R_1}{\sim} \begin{pmatrix} 0 & 0 & 1 & -1 & 1 \\ 0 & -1 & -1 & 0 & -1 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

We get $\operatorname{rank}(Q - i_5) = 3$ (the number of non-zero rows from an echelon form of the matrix). Hence, f has $r = 3$ irreducible factors.

Since $\dim V = \deg(f) = 5$, we have $V \cong \mathbb{Z}_3^5$. Now we identify φ with $\psi : \mathbb{Z}_3^5 \to \mathbb{Z}_3^5$ and determine a basis of $\operatorname{Ker}\psi = \{a \in \mathbb{Z}_3^5 \mid \psi(a) = 0\}$

$\operatorname{Ker}\psi = \{a = (a_0, a_1, a_2, a_3, a_4) \in \mathbb{Z}_3^5 \mid (Q - i_5)[a] = [0]\}$.

We get the system:

$$\begin{cases} a_2 - a_3 + a_4 = 0 \quad (1) \\ -a_1 - a_2 - a_4 = 0 \\ a_2 - a_3 = 0 \Rightarrow a_2 = a_3 \quad (2) \\ a_1 - a_2 - a_3 - a_4 = 0 \\ -a_2 + a_3 - a_4 = 0 \end{cases}$$

From $(1) + (2) \Rightarrow a_4 = 0$. Replacing $a_4 = 0$ we get:

$$\left.\begin{cases} -a_1 - a_2 = 0 \Rightarrow a_1 = -a_2 \overset{a_1, a_2 \in \mathbb{Z}_3}{=} 2a_2 \\ a_1 - a_2 - a_3 = 0 \end{cases}\right\} \Rightarrow 2a_2 - a_2 - a_3 = 0 \Leftrightarrow a_2 - a_3 = 0 \text{ - True.}$$

Then, the solution of the system is:

$a_1 = -a_2$, $a_2 = a_3$, $a_4 = 0$, $a_0, a_2 \in \mathbb{Z}_3$.

$\operatorname{Ker}\psi = \{(a_0, -a_2, a_2, a_2, 0) \mid a_0, a_2 \in \mathbb{Z}_3\} = \langle (1,0,0,0,0), (0,-1,1,1,0) \rangle = \langle v_1, v_2 \rangle$

A basis of $\operatorname{Ker}\psi$ is ~~(v~~ (v_1, v_2).

The associated polynomials are: $\begin{cases} h_1 = 1 \\ h_2 = -X + X^2 + X^3 \end{cases}$

We compute $(f, h_2 - s)$ where $s \in \mathbb{Z}_3$.
For $s = 0$.

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

$$\begin{array}{l|l}
X^3+X^2-X & X^2+X+2 \\ \cline{2-2}
-X^3-X^2-2X & X \\ \cline{1-1}
/\ \ /\ \ / &
\end{array}$$

$\Rightarrow (f, h_2) = X^2+X+2.$
The second factor is obtained by dividing f by the obtained factor.

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

Therefore,
$$f = (X^2+X+2)(X^3+X^2-X+1).$$