Popa Alex Ovidiu
936

PKC Bonus

Berlekamp's Algorithm

(02)

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

Compute $f' = 5x^4 + 4x^3 + 3x^2 - 1$
$= 2x^4 + x^3 + 2 \iff -x^4 + x^3 - 1$ in $\mathbb{Z}_3$

Compute gcd (f, f') :

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

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

$f = x(-x^3 + x^2) - 1 \Rightarrow \gcd(f, f') = 1$

$\Rightarrow f$ is square free

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

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

Consider $V=\mathbb{Z}_3[X]/(f)$ a vector space over $\mathbb{Z}_3$, with a basis $B=(1, X, X^2, X^3, X^4)$. In B, the values of q_{ik} are equal to the coordinates of the vector X^{3k} in the same basis B, for $k=\overline{0,4}$.

1 and X^3 belong to B, and we have:

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

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

The next powers are obtained by computing $X^{3k} \bmod f$.

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

2

$$\frac{x^9}{x^5+x^4+x^3-x-1}$$

$$x^4 - x^3 + x$$

$$x^9$$
$$-x^9 - x^8 - x^7 + x^5 + x^4$$
$$\cancel{-x^8} \cancel{-x^7} + x^5 + x^4$$
$$\cancel{x^8} + \cancel{x^7} + x^6 - \cancel{x^4} - x^3$$
$$\cancel{x^6} + \cancel{x^5} - x^3$$
$$\cancel{-x^6} - \cancel{x^5} - x^4 + x^2 + x$$
$$\boxed{-x^4 - x^3 + x^2 + x}$$

$$\frac{x^{12}}{x^5+x^4+x^3-x-1}$$

$$x^7 - x^6 + x^4 - x^2 + 2$$

$$\cancel{x^{12}}$$
$$\cancel{-x^{12}} - x^{11} - x^{10} + x^8 + x^7$$
$$\cancel{-x^{11}} \cancel{-x^{10}} + x^8 + \cancel{x^7}$$
$$\cancel{x^{11}} + \cancel{x^{10}} + x^9 - \cancel{x^7} - x^6$$
$$\cancel{x^9} + \cancel{x^8} - x^6$$
$$\cancel{-x^9} \cancel{-x^8} - x^7 + x^5 + x^4$$
$$-\cancel{x^7} - \cancel{x^6} + x^5 + x^4$$
$$\cancel{x^7} + \cancel{x^6} + x^5 - x^3 - x^2$$
$$2\cancel{x^5} + x^4 - \cancel{x^3} - x^2$$
$$-2x^5 + x^4 + \cancel{x^3} - x - 1$$
$$\boxed{-x^4 - x^2 - x - 1}$$

-> we add each vector as a column in the matrix Q.

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

Let $\varphi : V \to V$, $\varphi(h) = h^2 - h \pmod{f}$. Then φ is a linear map and $[\varphi]_B = Q - I_5$. Then
$r = \dim \ker \varphi = n - \operatorname{rank}(Q - I_5)$ is the number of irreducible factors of f.

We determine $\operatorname{rank}(Q - I_5)$ using elementary operations to get the echelon form of $Q - I_5$.

$$Q - I_5 = \begin{pmatrix} 0 & 0 & -1 & 0 & -1 \\ 0 & -1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & -1 & 1 \end{pmatrix} \underset{\sim}{R_1 \leftrightarrow R_2} \begin{pmatrix} 0 & -1 & 0 & 1 & -1 \\ 0 & 0 & -1 & 0 & -1 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & -1 & 1 \end{pmatrix}$$

$$\underset{\sim}{R_1 = -R_1} \begin{pmatrix} 0 & 1 & 0 & -1 & 1 \\ 0 & 0 & -1 & 0 & -1 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & -1 & 1 \end{pmatrix} \underset{\sim}{R_4 - R_1} \begin{pmatrix} 0 & 1 & 0 & -1 & 1 \\ 0 & 0 & -1 & 0 & -1 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & -1 & 1 \end{pmatrix}$$

$$\underset{\substack{\sim \\ R_2 = -R_2}}{R_4 + R_2} \begin{pmatrix} 0 & 1 & 0 & -1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -1 & +1 \\ 0 & 0 & 0 & -1 & 1 \end{pmatrix} \underset{\sim}{R_5 = -R_5} \begin{pmatrix} 0 & 1 & 0 & -1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix}$$

$$\overset{R_4-R_3}{\sim}\begin{pmatrix} 0 & 1 & 0 & -1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix} \overset{R_5-R_3}{\sim} \begin{pmatrix} 0 & 1 & 0 & -1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

in row echelon form

$\operatorname{rank}(Q - I_5) = 3$ = nr of non-zero rows in the row echelon form

$r = 5 - 3 = 2$ 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
$$\ker \psi = \{ a \in \mathbb{Z}_3^5 \mid \psi(a) = 0 \}$$

Hence
$$\ker \psi = \{ a = (a_0, \dots, a_4) \in \mathbb{Z}_3^5 \mid (Q - I_5)[a] = [0] \}$$

We have the system:
$$\begin{cases} -a_2 - a_4 = 0 \to \underline{a_2 = -a_4} \\ a_3 - a_4 = 0 \to \underline{a_3 = a_4} \\ -a_1 + a_3 - a_4 = 0 \to \underline{a_1 = 0} \\ a_1 + a_2 + a_3 = 0 \ \text{(true)} \end{cases}$$

$$\Rightarrow \ker \psi = \{ (a_0, 0, -a_4, a_4, a_4) \mid a_0, a_4 \in \mathbb{Z}_3 \}$$
$$= \langle (1,0,0,0,0), (0,0,-1,1,1) \rangle$$

Thus we have a basis of $\ker \psi$, consisting of the two generators. The associated polynomials (forming a basis of $\ker \psi$) are:

$$\begin{cases} h_1 = 1 \\ h_2 = x^4 + x^3 - x^2 \end{cases}$$

We get a factor by computing $(f, h_2 - s)$, for $s \in \mathbb{Z}_3$.

$s = 0 \to (f, h_2) = ?$

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

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

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

$\gcd(f, h_2) = x^2 + x - 1 =$ the first factor of f.

Since we know we have two factors, we can get the second one by dividing f with the first one.

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

is the second factor

$$\Rightarrow \boxed{f = (x^2+x-1)(x^3-x+1)}$$

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

$$= x^5 - x^3 + x^2 + x^4 - x^2 + x - x^3 + x - 1$$

$$= x^5 + x^4 + x^3 - x - 1 \quad (T).$$