We wish to understand when polynomials are coprime without factoring. We begin with an abstract definition and a theorem.

Definition 1. We say that $p(z), q(z) \in \mathbb{F}[z]$ are *coprime* if and only if there exist $a(z), b(z) \in \mathbb{F}[z]$ such that $a(z)p(z) + b(z)q(z) = 1$.

Theorem 1. *Let $p(z), q(z) \in \mathbb{F}[z]$ with $p(z) = \sum_i^m p_i z^i$ and $q(z) = \sum_i^m q_i z^i$. The following are all equaivalent:*

1. *The polynomials are coprime.*
2. *There is a direct sum decomposition*

$$\mathbb{F}_{m+n}[z] = p\mathbb{F}_n[z] \oplus q\mathbb{F}_m[z].$$

3. *The resultant matrix*

$$\mathrm{Res}(p,q) = \begin{pmatrix} p_0 & \cdots & \cdots & \cdots & q_0 & & \\ p_1 & p_0 & \ddots & \vdots & q_1 & & \\ \vdots & p_1 & \ddots & & \vdots & & \\ p_m & \vdots & & & \vdots & \ddots & q_0 \\ & p_{m-1} & \ddots & p_0 & q_n & \ddots & q_1 \\ & p_m & \ddots & p_1 & & & \vdots \\ & & & \vdots & & & \vdots \\ & & & p_{m-1} & & & q_{n-1} \\ & & & p_m & & & q_n \end{pmatrix}$$

   is nonsingular.

4. *The determinant of* $\mathrm{Res}(p,q) \neq 0$.

Examples:

1. Let $p(x) = x^3 + x^2 + x + 1$ and $q(x) = x^2 + 2x + 1$. Then

$$\operatorname{Res}(p, q) = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 2 & 1 & 0 \\ 1 & 1 & 1 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

has determinant zero.

2. Let $p(x) = x^3 - 1$ and $q(x) = x - 1$ with resultant

$$\operatorname{Res}(p, q) = \begin{pmatrix} -1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

has determinant zero.

3. Let $p(x) = x^2 + 1$ and $q(x) = x^3 - x^2 + x - 1$ and consider the resultant

$$\operatorname{Res}(p, q) = \begin{pmatrix} -1 & 0 & 1 & 0 & 0 \\ 1 & -1 & 0 & 1 & 0 \\ -1 & 1 & 1 & 0 & 1 \\ 1 & -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

has determinant zero.

4. Let $p(x) = x^2 + 1$ and $q(x) = x$. The resultant

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

has determinant 1. Hence, $\operatorname{Res}(p, q)$ is nonsingular.

We note that we can write

$$x^2 + 1 - x \cdot x = 1$$

since x and $x^2 + 1$ are coprime.

Calculating the rank of each example:

1. rank 4
2. rank 3
3. rank 3
4. rank 3

From example 4, we can write any degree 2 polynomial as

$$(x^2 + 1)\mathbb{F} \oplus x\mathbb{F}_2[x].$$

For instance,

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