

## 9. Euclid's Algorithm

- Euclid's algorithm is a technique for finding the greatest common divisor  $(a, b)$  of two integers or polynomials  $a$  and  $b$ .

- Proposition (2.18, page 48)

Let  $a$  and  $b$  be two positive integers (or polynomials)

Then if  $a = q_1 b + r_1$

for  $0 \leq r_1 < b$  ( $0 \leq \deg(r_1) \leq \deg(b)$ )

One has  $(a, b) = (b, r_1)$

where  $(a, b)$  denotes greatest common divisor.

$$\begin{aligned} b &= q_2 r_1 + r_2 & \Rightarrow & (b, r_1) = (r_1, r_2) \\ & \vdots & & \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n & \Rightarrow & (a, b) = r_n \end{aligned}$$

**Example:**

Suppose  $a = 186$ ,  $b = 66$ ,

then

$$\begin{aligned} 186 &= 66 * 2 + 54 \\ 66 &= 54 * 1 + 12 \\ 54 &= 12 * 4 + 6 \\ 12 &= 6 * 2 + 0 \end{aligned}$$

the greatest common divisor is  $6$ .

▪ **Euclid's Division Algorithm for Polynomials**

**Given two polynomials  $a(x)$  and  $b(x)$**

**Their greatest common divisor can be computed by an iterative application of the division algorithm. If the degree of  $a(x)$  is greater than the degree of  $b(x)$ , the computation of GCD**

**$(a(x), b(x))$  is**

$$a(x) = q_1(x) \cdot b(x) + r_1(x)$$

$$b(x) = q_2(x) \cdot r_1(x) + r_2(x)$$

$$r_1(x) = q_3(x) \cdot r_2(x) + r_3(x)$$

$\vdots$

$$r_{n-1}(x) = q_{n+1}(x) \cdot r_n(x)$$

**where the iterative process stops when a remainder of zero is obtained.**

**Then the greatest common divisor of  $a(x)$  and  $b(x)$  is**

$$r_n(x) = \text{GCD}(a(x), b(x))$$

**Example:**

$$a(x) = x^3 + 1$$

$$b(x) = x^2 + 1$$

$$x^3 + 1 = (x^2 + 1) \cdot x + (x + 1)$$

$$x^2 + 1 = (x + 1) \cdot x$$

**$\therefore$  GCD of  $a(x)$  and  $b(x)$  is  $x + 1$**

## 10. Arithmetic Operations in $\text{GF}(2^m)$

- **Primitive Elements**

Consider the Galois field  $\text{GF}(2^m)$  generated by the primitive polynomial  $p(x) = p_0 + p_1x + p_2x^2 + \cdots + p_{m-1}x^{m-1} + x^m$

**Definition:**

The element  $\alpha$  (a root of  $p(x)$ ) whose powers generate all the non-zero elements of  $\text{GF}(2^m)$  is called a primitive element of  $\text{GF}(2^m)$ .

In fact, any element  $\beta$  in  $\text{GF}(2^m)$  whose powers generate all the nonzero elements of  $\text{GF}(2^m)$  is a primitive element.

**Example:**

$\alpha^4$  and  $\alpha^7$  are also primitive elements of  $\text{GF}(2^4)$ .

▪ **Minimum Polynomial**

- (1) Consider the Galois field  $\text{GF}(2^m)$  generated by a primitive polynomial  $p(x)$  of degree  $m$ . Let  $\beta$  be a non-zero element of  $\text{GF}(2^m)$

Consider the powers

$$\beta, \beta^2, \beta^{2^2}, \dots, \beta^{2^i}, \dots$$

If  $e$  is the smallest nonnegative integer for which

$$\beta^{2^e} = \beta$$

Then the integer “ $e$ ” is called the exponent of  $\beta$ .

- (2) consider the product,

$$\begin{aligned} \varphi(x) &= (x + \beta)(x + \beta^2) \cdots (x + \beta^{2^{e-1}}) \\ &= a_0 + a_1x + a_2x^2 + \cdots + a_{e-1}x^{e-1} + x^e \end{aligned}$$

is a polynomial of  $e$  degree.

We can see that  $\varphi(x)$  is binary and irreducible over  $\text{GF}(2)$ .  $\varphi(x)$  is called the minimal polynomial of the element  $\beta$ .