Division Algorithm

$f(x)$: degree n, $g(x)$: degree $m \le n$, $f(x), g(x) \in F[x]$

(F is a field).

$$f(x) = q(x) \cdot g(x) + r(x),$$

where $\deg q(x) = n - m$

$\deg r(x) \le m-1$

$$r(x) \equiv f(x) \pmod{g(x)},$$

$$r(x) = f(x) \bmod g(x).$$

If there is no remainder ($r(x) = 0$), we say that $g(x)$ divides $f(x)$, $g(x) \mid f(x)$ or $g(x)$ is a <u>factor</u> of $f(x)$.

For our purpose, polynomials over $GF(2)$ are of most interest.

$GF(2)$

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

Ex. $f(x) = x^7 + x^5 + x^4 + x^3 + x + 1$

$g(x) = x^3 + x + 1$, $f(x), g(x) \in GF(2)[x]$.

$$
\begin{array}{r|l}
 & x^4 + 1 \\ \hline
x^3 + x + 1 & x^7 + x^5 + x^4 + x^3 + x + 1 \\
 & x^7 + x^5 + x^4 \\ \hline
 & \qquad\qquad x^3 + x + 1 \\
 & \qquad\qquad x^3 + x + 1 \\ \hline
 & \qquad\qquad\qquad 0.
\end{array}
$$

$\therefore\ g(x) \mid f(x)$

$f(x) = a \cdot \underbrace{a^{-1} f(x)}_{g(x).}$, $\forall a \in F$.

$\boxed{(x^4 - 1) = (x-1)(x^3 + 3x^2 + 3x + 1)}$

Ex. $f(x) = x^4 + 1$

$g(x) = x + 1 \in GF(2)[x]$.

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

$f(x) = a \cdot g(x)$
$a \in F$.
$\deg g = \deg f$.

There are no $u(x)$, $v(x)$ with $\deg u < \deg f$
$\deg v < \deg f$
such that $u(x) v(x) = f(x)$.

$\therefore\ x^4 + 1 = (x+1)(x^3 + x^2 + x + 1)$.

$x^4 + 1$ is reducible.

A polynomial $f(x)$ over a field F is called **irreducible** if and only if $f(x)$ cannot be expressed as a product of two polynomials both of lower degree than $\deg f(x)$.

Finding the GCD (Euclidean Algorithm).

$$\gcd(a,b) = \gcd(b,\ a \bmod b),\quad a,b \in \mathbb{Z}.$$

$$\Rightarrow \gcd(a(x), b(x)) = \gcd(b(x),\ a(x) \bmod b(x)),$$

$$a(x), b(x) \in F[x].$$ verify it

$r_1(x) = a(x) \bmod b(x)$

$r_2(x) = b(x) \bmod r_1(x)$

$r_3(x) = r_1(x) \bmod r_2(x)$

$\vdots$

$r_n(x) = r_{n-2}(x) \bmod r_{n-1}(x)$

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

$= 0.$

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

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

$r_1(x) = q_3(x)\, r_2(x) + r_3(x).$

$\vdots$

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

$r_1(x) = \underline{a(x)} - q_1(x)\, b(x).$

$r_2(x) = b(x) - q_2(x) \cdot \underline{r_1(x)}$

$= a(x) \cdot s_2(x) + b(x) \cdot t_2(x).$

$\vdots$

$d(x) = \gcd(a(x), b(x))$

$= \gcd(b(x), r_1(x))$

$= \cdots$

$= \gcd(r_n(x), 0)$

$= r_n(x).$

$\Rightarrow d(x) = r_n(x) = s_n(x) \cdot a(x) + t_n(x) \cdot b(x)$

Extended Euclidean algorithm

$\exists\ s(x), t(x)$ such that

$$d(x) = a(x) \cdot s(x) + b(x) \cdot t(x)$$

Ex. $a(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ $\quad \in GF(2)[x]$.

$b(x) = x^4 + x^2 + x + 1$

Find $\gcd(a(x), b(x))$.

$$
\begin{array}{r|l}
 & x^2 + x \\
\hline
\underset{b(x)}{x^4 + x^2 + x + 1} & \underset{a(x)}{x^6 + x^5 + x^4 + x^3 + x^2 + x + 1} \\
\hline
 & x^3 + x^2 + 1 \quad r_1(x).
\end{array}
$$

$r_1(x) = a(x) \cdot s(x) + b(x) \cdot t(x)$.

$r_1(x) = a(x) - (x^2 + x)\, b(x)$

$r_2(x) = 0 = b(x) - (x+1)\, r_1(x)$

$$
\begin{array}{r|l}
 & x + 1 \\
\hline
\underset{r_1(x)}{x^3 + x^2 + 1} & \underset{b(x)}{x^4 + x^2 + x + 1} \\
\hline
 & 0 \quad r_2(x)
\end{array}
$$