If $\gcd(m, b) = 1$, then $b^{-1} \pmod m$ exists.

$$1 = \gcd(m, b)$$
$$= m \cdot x + b \cdot y$$
$$\Rightarrow \underbrace{m \cdot x}_{0} + b \cdot y \pmod m = 1 \pmod m$$
$$\Rightarrow b \cdot y = 1 \pmod m$$
$$\Rightarrow \boxed{y = b^{-1} \pmod m}.$$

$f(x) = x^3 + 1$ in $GF(2)$

$Z_2 = \{0, 1\}$

$+_2 = \oplus$

$\cdot_2 = \text{AND}$

$x^2 + x + 1$

$x + 1 \;\big)\; x^3 + 1$

$x^3 + x^2$

$x^2 + 1$

$x^2 + x$

$x + 1$

$x + 1$

0

$x - y \pmod 2 = x \oplus y$

$\therefore f(x) \equiv (x+1)(x^2+x+1)$

$\Rightarrow f(x)$ is reducible.

$GF(p)$ ← Galois field

$GF(p^n)$ ← Extended Galois field

$\{ +_p = \text{addition mod } p,\ \cdot_p = \text{multiplication mod } p \}$

$f(x) = \sum_{i=0}^{n-1} a_i x^i$, a_i's $\in Z_p = \{0, 1, \cdots, p-1\}$

$|GF(p^n)| = |\{ f(x) \mid f(x) = \sum_{i=0}^{n-1} a_i x^i,\ a_i\text{'s} \in Z_p \}| = p^n$.