Euklidischer Algorithmus & Erweiterung

Bestimmen Sie mit dem erweiterten Euklidischen Algorithmus den ggT von $m := 126$ und $n := 234$ sowie zwei natürliche Zahlen $x, y \in \mathbb{N}$ mit

$ggT(126, 234) \equiv x \cdot 234 \pmod{126}$

$ggT(126, 234) \equiv y \cdot 126 \pmod{234}$

Euklidischer Algorithmus

$234 = 1 \cdot 126 + 108$

$126 = 1 \cdot 108 + 18$

$108 = 6 \cdot 18 + 0$

$\Rightarrow ggT(234, 108) = 18$

$108 : 18 = 6$
108
0

Erweiterung

$108 = 234 - 1 \cdot 126$

$18 = 126 - 1 \cdot 108 = 126 - 1 \cdot (234 - 1 \cdot 126)$

$= 2 \cdot 126 - 1 \cdot 234$

$\Rightarrow ggT(234, 126) \equiv 2 \cdot 126 \pmod{234}$

$ggT(234, 126) \equiv -1 \cdot 234 \pmod{126}$

$\equiv 125 \cdot 234 \pmod{126}$

$x = 125$

$y = 2$

Euklidischer Algorithmus & Erweiterung - GF(16)

$p(x) := x^2 + x \quad i(x) := x^4 + x + 1$

gesucht: $p^{-1}(x) \in GF(16)$ (multiplikativ inverses Polyno

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

$x^2 + x = 0 \cdot (x^3 + x + 1) + x^2 + x$

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

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

$x^2 + x + 1 = (x^2 + x + 1) \cdot 1 + 0$

$\Rightarrow ggT(x^2+x, x^2+x+1) = 1$

Erweiterung

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

$x^2 + x = x^2 + x - 0 \cdot (x^3 + x + 1)$

$= x^2 + x - 0 \cdot (x^4 + x + 1 - x^2 \cdot (x^2 + x))$

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

$= (x^4 + x + 1) + x^2 \cdot (x^2 + x) + x \cdot (x^2 + x)$

$= 1 \cdot (x^4 + x + 1) + (x^2 + x)(x^2 + x)$

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

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

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

$ggT(x^2+x, x^4+x+1) \equiv 1 (x^4 + x + 1) \pmod{(x^2+x)}$

$ggT(x^2+x, x^4+x+1) \equiv (x^2+x+1)(x^2+x) \pmod{(x^4+x+1)}$

$\Rightarrow p^{-1}(x) \equiv x^2 + x + 1$