$GF(\underbrace{3}_{\mathbb{Z}_3}^{\overbrace{3}^{\text{orde } 3}}) \setminus \{0\}$, 26 elementen

Is $x^3 + 2x + 1$ primitief?

---

groep G, $|G| = q$

$q = \prod_{i=0}^{\infty} p_i^{e_i}$, neem $q_i = q/p^i$

$\forall h \in G$, 'h is een generator' $\leftrightarrow \forall i, (e^i \neq 0 \rightarrow h^{q_i} \neq 1)$

Voorbeeld

$q = 26 = 2 \cdot 13$

$q_0 = 26/2 = 13$

$q_5 = 26/13 = 2$

$\left.\begin{array}{l} \alpha^2 \neq 1 \\ \alpha^{13} \neq 1 \end{array}\right\} \Rightarrow x^3+2x+1$ primitief (want α generator)

Voorbeeld met macht

$q = |GF(3^4) \setminus \{0\}| = 80$

$2^4 \cdot 5 = 80$

$q_0 = 80/2 = 40$

$q_2 = 80/5 = 16$

Specifiek geval

Stel q is priem. Dan zijn alle elementen die ongelijk 1 zijn generator.

$q = p_n$, $q_n = q/p_n = q/q = 1$

h is generator $\Leftrightarrow h^1 \neq 1$

$= h \neq 1$

$GF(3^3)\setminus\{0\}$, 26 elementen

Is x^3+2x+1 primitief?

$\alpha = x \pmod{p}$

$\alpha^2 = x^2 \pmod{p} \quad \neq 1$

$\alpha^3 = x^3 = \cancel{1(x^3+2x+1)} -2x-1$

$= x+2$

$\alpha^4 = x^2+2x$

$\alpha^8 = (x^2+2x)(x^2+2x)$

$= x^4 + \cancel{2x^3} + \cancel{2}x^3 + \cancel{4}x^2$

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

$= 2x^2 + \cancel{3x} + 2$

$\alpha^{12} = (2x^2+2)(x^2+2x)$

$= 2x^4 + 4x^3 + 2x^2 + 4x$

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

$= 2x^2+4x+x+2+2x^2+x$

$= x^2+2$

$\alpha^{13} = x^3+2x$

$= x+2+2x$

$= 2 \quad \neq 1$

$q = 26 = 2\cdot 13$

$q_1 = 26/2 = 13$

$q_2 = 26/13 = 2$

$\Rightarrow$ x^3+2x+1 is primitief