Hoofdvraag G

Algoritme van Berlekamp (even karakteristiek)

input: Een monisch kwadraatvrij polynoom $f \in \mathbb{F}_q[x]$, q oneven, $\deg f = n \geq 1$
output: Een niet triviale factor g van f of "gefaald"

1 Bepaal $\text{rem}(x^q, f)$ in $\mathbb{F}_q[x]$ met behulp van Algoritme 1.5
2 **for** $i = 0, \cdots, n-1$
3 **do** Bepaal $\text{rem}(x^{qi}, f) = \sum_{j=0}^{n-1} q_{ij} x^j$
4 $Q \leftarrow (q_{ij})_{0 \leq i,j < n}$
5 Bepaal een basis voor de kern van $Q - I$, bepaal daarmee $r = \dim \mathcal{B}$, en een basis $\{b_1, \ldots, b_r\}$ voor de Berlekamp deelalgebra met $\deg b_i < n$.
6 Kies onafhankelijke uniform verdeelde random elementen $c_1, \ldots, c_r \in \mathbb{F}_q$
7 $a \leftarrow c_1 b_1 + \cdots + c_r b_r$
8 $g_1 \leftarrow \gcd(a, f)$
9 **if** $g_1 \neq 1$
10 **then return** g_1
11 Bepaal $b = T(a)$ en $\text{rem}(b, f)$ met Algoritme 1.5 en 2.7.
12 $g_2 \leftarrow \gcd(b, f)$
13 **if** $g_2 \neq 1$ en $g_2 \neq f$
14 **then return** g_2
15 **else return** "gefaald"

Zij f een kwadraatvrij polynoom over $\mathbb{F}_q$ ($q = 2^h$). Definieer (zonder details) de Berlekamp deelalgebra en toon aan dit het algoritme van Berlekamp met kans minstens $1/2$ een factor van f vindt als f reduciebel

Bijvraag G

Fast Fourier transformatie (FFT)

input: $n = 2^k$ met $k \in \mathbb{N}$; $f = \sum_{i=0}^{n-1} f_i x^i$; de machten $\omega, \omega^2, \ldots, \omega^{n-1}$ van een primitieve n^{de} eenheidswortel $\omega \in R$.
output: $\text{DFT}_\omega(f) \in R^n$.

1 **if** $n = 1$ **then return** f_0
2 $r \leftarrow \sum_{j=0}^{n/2-1} (f_j + f_{j+n/2}) x^j$, $s \leftarrow \sum_{j=0}^{n/2-1} (f_j - f_{j+n/2}) \omega^j x^j$
3 Evalueer **recursief** de polynomen r en s in de machten van ω^2
4 **return** $\big(r(1), s(1), r(\omega^2), s(\omega^2), \ldots, r(\omega^{n-2}), s(\omega^{n-2})\big)$

Definieer DFT_ω en toon aan dat dit algoritme correct $\text{DFT}_\omega(f)$ berekent.