Universiteit van Stellenbosch

Toegepaste Wiskunde 314

Tutoriaal 6: Donderdag 1 April 2004

MEMORANDUM

(1) Die terugvoerpolinoom $f(x) = 1 + p_1x + p_2x^2 + p_3x^3 + p_4x^4$ kan uit die sisteem van vergelykings

$$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \end{bmatrix}$$

bepaal word, deur van (modulêre) Gauss–eliminasie gebruik te maak, of deur die inverse

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

te gebruik. Die oplossing is $f(x) = 1 + x^3 + x^4$.

(2) (a) Ja, $f(x)$ is onreduseerbaar in $(\mathbb{Z}_2[x], +, \times)$; dit het geen faktore in die ring nie.

(b) Ja, $f(x)$ is primitief in $(\mathbb{Z}_2[x], +, \times)$; die eksponent daarvan is maksimaal (naamlik 15), volgens Tabel 3-2.

(3) Die periode van $\underline{s}$ is $p = 15$ (Stelling 3-4).

(4) $\underline{s}_0^{15} = 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0.$

(5) Die kripto–stroom is $\underline{k} = 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1.$

(6) Die kripto–stroom is $\underline{k} = 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0.$

(7) $\underline{s} = 1, 1, 0, 0, 1, 1, \underbrace{1, 1, 0, 0, 1, 1}_{\text{een siklus}}, 1, 1, 0, 0, 1, 1, \ldots$ (Periode: 6)

(8) (a) $1 + x^5 + x^7$ is nie 'n primitiewe polinoom in $\mathbb{Z}_2[x]$ nie, aangesien dit in die ring $(\mathbb{Z}_2[x], +, \times)$ as $(1 + x + x^2)(1 + x + x^3 + x^4 + x^5)$ gefaktoriseer kan word.

(b) $1+x^6+x^7$ het geen faktore in die ring $(\mathbb{Z}_2[x], +, \times)$ nie (m.a.w. is onreduseerbaar in die ring), maar die eksponent daarvan is $e < 2^7 - 1 = 127$; gevolglik is dit nie 'n primitiewe polinoom in $\mathbb{Z}_2[x]$ nie.

(c) $1 + x^4 + x^7$ is wel 'n primitiewe polinoom in $\mathbb{Z}_2[x]$, aangesien dit geen faktore in die ring $(\mathbb{Z}_2[x], +, \times)$ het nie, en 'n eksponent van $e = 2^7 - 1 = 127$ het.

(9) Daar is $\phi(2^{25} - 1)/25 = 1\,296\,000$ primitiewe polinome van graad 25.

(10) Die eerste 8 bisse van die sleutelstroom word gegee deur $\underline{s} = 0, 0, 0, 1, 1, 1, 1, 0, \ldots$ Die ASCII–waarde van die karakter "`z`" is $122 = (01111010)_2$. Deur hierdie 8 bisse (modulo 2) by die eerste 8 bisse van die sleutelstroom te tel, word die binêre stroom $\underline{k} = 0, 1, 1, 0, 0, 1, 0, 0, \ldots$ verkry, en omdat $(01100100)_2 = 100$, is die ooreenstemmende kriptoteks–karakter "d".