Universiteit van Stellenbosch

Toegepaste Wiskunde 314

Tutoriaal 6: Donderdag 1 April 2004

Beskou die binêre stroom

$$\underline{s} = 1, 1, 1, 1, 0, 0, 0, 1, \ldots$$

(1) Gestel dit is bekend dat die bogenoemde stroom $\underline{s}$ deur middel van 'n LTSR $\mathcal{F}^4_{f(x)}$ gegenereer is. Bepaal $f(x)$. [Wenk: Die *Mathematica*–opdrag `Inverse[{{a,b,c,d}, {e,f,g,h}, {i,j,k,l}, {m,n,o,p}}, Modulus -> 2]` mag byvoorbeeld handig te pas kom om die inverse van 'n matriks

$$\begin{bmatrix} \texttt{a} & \texttt{b} & \texttt{c} & \texttt{d} \\ \texttt{e} & \texttt{f} & \texttt{g} & \texttt{h} \\ \texttt{i} & \texttt{j} & \texttt{k} & \texttt{l} \\ \texttt{m} & \texttt{n} & \texttt{o} & \texttt{p} \end{bmatrix}$$

in die versameling $\mathcal{Z}_2^{4*}$ te bereken.]

(2) Is die polinoom $f(x)$ in (1)

(a) onreduseerbaar? Motiveer. [Wenk: Die *Mathematica*–opdrag `Factor[f(x), Modulus -> 2]` mag hier handig te pas kom.]

(b) primitief? Motiveer.

(3) Wat is die periode, p, van die stroom $\underline{s}$? Motiveer.

(4) Bereken 'n volle siklus, $\underline{s}_0^p$, van die stroom $\underline{s}$.

(5) Enkripteer die skoonteks `abc` met behulp van 'n gesinkroniseerde stroomsyferstelsel met sleutelstroom $\underline{s}$, soos bo.

(6) Enkripteer die skoonteks `abc` met behulp van 'n self–sinkroniserende stroomsyferstelsel met sleutel–generatorfunksie $s_i = k_{i-1} \oplus k_{i-4} \otimes k_{i-7}$.

(7) Skryf neer die binêre stroom wat met die generator–funksie

$$G(x) = (1 + x + x^4 + x^5)(1 + x^6 + x^{12} + x^{18} + \ldots) = \frac{1 + x + x^4 + x^5}{1 + x^6}$$

ooreenstem.

(8) Watter van die volgende polinome is primitief? Motiveer volledig.

(a) $1 + x^5 + x^7$

(b) $1 + x^6 + x^7$

(c) $1 + x^4 + x^7$

(9) Hoeveel primitiewe polinome is daar van graad 35 in die ring $(\mathbb{Z}_2[x], +, \times)$?

(10) Gebruik die A5–stelsel met sleutel `bcdefghi` om die karakter **`z` met die hand** te enkripteer. Toets die korrektheid van jou antwoord deur middel van die program **EnDeCrypt**. [Wenk: Klik op "Crypto systems" op die **EnDeCrypt** hoofspyskaart, daarna op "Stream ciphers", en daarna op "A5".]

St Elmo's Uitdaging: Ontrafel die betekenis van die kriptoteks

$$1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0$$

wat met behulp van 'n gesinkroniseerde stroomsyferstelel met 'n lineêre terugvoer skuifregister van lengte 6 gevorm is.